# A STUDY ON MULTIPLE METHODS OF FINGERPRINT HASH CODE GENERATION BASED ON MD5 ALGORITHM USING MODIFIED FILTERING TECHNIQUES AND MINUTIAE DETAILS

**Thesis submitted to Srinivas University in Partial Fulfillment of the requirements for the award of the Degree of**

## DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE

**By**


**Mr. Krishna Prasad K.**

**Reg. No. SUPHDCOMSC2017/02**


**Under the Guidance of**


**Dr. P. Sreeramana Aithal, Ph.D., Post Doc.**

**Professor, College of Computer and Information Sciences,**

**Srinivas University,**

**Mangaluru-575001**




## SRINIVAS UNIVERSITY

**MUKKA, MANGALURU - 574 146 (KARNATAKA STATE), INDIA**

**MARCH- 2018**

# *Certificate*

## RESEARCH SUPERVISOR'S REPORT

This is to certify that Thesis entitled **"A Study on Multiple Methods of Fingerprint Hash Code Generation Based on MD5 Algorithm using Modified Filtering Techniques and Minutiae Details"** Submitted to **Srinivas University, Mukka, Mangaluru, Karnataka State, India**, by **Krishna Prasad K.,** for the award of degree of **Doctor of Philosophy** in **Computer Science** is a record of bonafide research work carried out by him under my supervision. The Thesis has reached the standard of the regulations for the degree and it has not been previously formed the basis for the award of any degree, diploma, associateship, fellowship or any other similar title to the candidate or any other person (s).

Signature of the Research Supervisor

Dr. P. Sreeramana Aithal

Professor, College of Computer and Information Sciences,

Place: Mangaluru City Campus, Pandeshwar-Mangaluru-575001

Date: 20-03-2018 Karnataka State, India

# *Declaration*

## Declaration

I, **Krishna Prasad K.**, hereby declare that the Thesis entitled **"Study on Multiple Methods of Fingerprint Hash Code generation based on MD5 algorithm using Modifying Techniques and Minutiae details"**, submitted to **Srinivas University, Mukka, Mangaluru, Karnataka State, India,** in partial fulfilment of the requirements for the award of the degree of **Doctor of Philosophy** in **Computer Science** is the record of original research work carried out by me during the period from 30-03-2010 to 31-01-2018 under the supervision and guidance of **Dr. P. Sreeramana Aithal**, and has not formed the basis for the award of any degree, diploma, associate-ship, fellowship, or other similar title of any candidate in this or any other university or other similar institutions of higher learning. This Thesis is free from any kind of plagiarism.

Place: Mangaluru

Date: 20-03-2018

Signature of the candidate

Mr. Krishna Prasad K.,

M.Sc (Information Science), M. Phil (CS),

M. Tech (IT).

# *Acknowledgement*

## Acknowledgement

I wish to acknowledge several individuals who provided me with immeasurable help in the completion of this Thesis and degree. First of all, I derive immense pleasure in placing on record my deep sense of appreciation, gratitude and indebtedness to my Thesis supervisor, **Prof. Dr. P. Sreeramana Aithal**, Professor, College of Computer and Information Sciences, Srinivas University, City Campus, Pandeshwar, Mangaluru, for his all-round help in suggesting the problem, sustaining the interest, motivating, inspiring, and extending valuable guidance for the successful completion of the present investigation. Also, numerous discussions I had with him have increased my knowledge.

I am happy for the love and support I have had from **Sumana S.**, my wife and **Abheeshta Krishna**, my son through the years of dreams, and making life truly exciting. I would like to thank my **parents** who have blessed me with great tolerance. I would like to thank my **Father-in-law**, **Mother-in-law**, and **brother-in-law**, for their continuous support and motivation for completing my research work. I would like to thank my **brother** and **his family** for moral support. Without you all, things would have so much harder. I am wholeheartedly grateful to **Sri. CA. A. Raghavendra Rao**, President, A. Shama Rao Foundation, Mangalore and also Chancellor, Srinivas University, Mukka, Mangalore, for encouraging me by providing all facilities to carry out this work. I wish to express my sincere thanks to **Dr. P. Srinivas Rao**, Vice-president, A. Shama Rao Foundation, Mangalore and also Pro-Chancellor, Srinivas University, Mukka, Mangalore, for their support.

I am thankful to **Prof. P. Sridhara Acharya,** Coordinator, BCA Department, College of Computer and Information Sciences, Srinivas University, City Campus, Mangalore, for moral support and encouragement. I also thank all my colleagues at Srinivas College, Pandeshwar, Mangalore, for their kind help and encouragement throughout the period of my research work.

Last but not the least; I thank the **Almighty**, who has made my life blissful. May his name be exalted, honored and glorified.

KRISHNA PRASAD K.

# *Contents*

# CONTENTS

# *List of Figures*

# LIST OF FIGURES

# *List of Tables*

# List of Tables

# *Synopsis*

# SYNOPSIS/ PREPHASE

## A Study on Multiple Methods of Fingerprint Hash Code Generation Based on MD5 Algorithm using Modified Filtering Techniques and Minutiae Details

In this information and communication technology era, human beings are every now and again requested checks of their identity. Regularly, this is done using passwords while seeking activities like public security, access control, surveillance, and application sign on, and so on. In an organization, educational institutions, political and government offices, security has become crucial aspect and more and more research is carried out for the purpose of verification or identification. The issue of normal framework security involves the assurance of framework components. Therefore, this security can be easily breached when a password is divulged, a card is stolen or through social engineering. Besides, a great many people utilize a similar password crosswise over various applications; an impostor, after deciding or accessing a single password, would now be able to get to different applications. Basic passwords can be effortlessly speculated while troublesome passwords might be difficult to review, and passwords can likewise be broken by dictionary attacks. The requirement for solid client validation procedures has expanded in the wake of uplifted worries about security and quick development in systems administration, correspondence, and portability. These constraints related to the utilization of passwords can be improved by the joining of better strategies for client confirmation.

Biometrics innovation has ended up being a precise and proficient response to the security issue. Biometrics is a developing field of research as of late and has been dedicated to the distinguishing proof or authentication of people utilizing one or multiple inherent physical or behavioral characteristics. Among these biometric innovations, hand based biometrics, including unique finger impression or fingerprint, two-dimensional and three-dimensional palm prints, hand geometry or hand shape, hand vein, finger-knuckle print and so forth., are the most mainstream and have the biggest offer in the biometric identification methods. Biometric has increasingly become popular due to its nature of universality and uniqueness in human identification or verification. This is due to the advantages of these traits such as low cost, low-resolution imaging, and stable features. Because of this advancement, a new type of biometric-based verification and identification techniques or methods are developed, which are unique for individuals.

A large portion of the work found in the literature in connection with biometric traits utilizes highlights like iris, face, voice, palm prints, hand geometry, and fingerprints. The biometric fingerprint is one of the most normal and generally utilized biometric attributes throughout the world for recognition purpose.

The recent innovative researchers significantly concentrate on cell phones. Cell phones have turned into a critical gadget of human life. Clients get to their messages, informal organizations, financial balances, and different sites by means of cell phones. Mobile manufacturers or developers and application engineers take an assortment or mixture of safety efforts because of the individual, private as well as the touch sensitive nature of the data put away in cell phones. The utilization of biometric authentication on cell phones began with cameras. From the last few years, cell phone producers have included biometric validation frameworks like the increasingly well known unique fingerprint recognition highlight. This is a more secure and handy answer for recognizable proof on cell phones. The unique fingerprint traits of a man are exceptionally exact and are special to a person. Authentication frameworks in light of unique fingerprints have demonstrated to create low false acceptance rate and false rejection rate, alongside other favorable circumstances like simple and easy usage strategy. Additionally, the unique fingerprint ordinarily stays unaltered from birth until death. Aside from being extraordinary and constant, fingerprints can be accumulated in a non-obtrusive way with no symptom.

The current fingerprint technology is quite mature to identify or verify human using various diverse types of matching or comparing the process with already stored features or templates. One of the potential threats in a biometric framework is the compromise of the biometric template, which may prompt genuine security and protection dangers. The greater part of the fingerprint template protection methods neglects to meet all the coveted necessities of a viable biometric framework like revocability, security, protection, and high coordinating precision. Specifically, ensuring the fingerprint formats has been a troublesome issue because of huge intra-client varieties (e.g., turn, interpretation, nonlinear twisting, and partial fingerprint image). So there is a huge necessity of building a highly secured and not reversible or revocable fingerprint template protection and recognition system, which can serve the need of diverse applications in information, communication, surveillance and security fields. The most alluring properties of high exactness, low error rate and greatest speed or execution time are yet to be accomplished with Automatic Partial Fingerprint Recognition System (APFS). Consequently, the present research means to build up an

Automatic Partial Unique Fingerprint Recognition System, which also takes care of template protection to validate a person.

Fingerprint Hash code is not used for full security or authentication purpose but it can be combined with other security elements like password or OTP in order to enhance security. Fingerprint Hash code acts as a key, which can uniquely identify every person. So it can be replaceable with user-id or username and can work along with text-based or picture based or pattern based passwords. The main objective of this research is;

- To study multiple methods of Fingerprint Hash code generation based on MD5 Algorithm using modified filtering techniques and minutiae details and the extracted feature are unique features of the fingerprint such that there are no collisions in hash code.
- To propose an alternative approach for User Authentication using Multifactor, which includes, Fingerprint Hash code, Password and time synchronized One Time Password (OTP) based on different methods used in this research study.

The sub-objectives of this research work include the study of six methods, which are mentioned below.

- To Study, a Fingerprint Hash code using a different process like Preprocessing, Thinning and Minutiae Extraction, and Minutiae table formation and generating Hash code from these minutiae table (Method-1).
- To Study a Fingerprint Hash code using Gabor filter which includes techniques like Contrast adjustment filtering, Binarisation, Segmentation and generating Hash code from the Gabor filtering details (Method-2).
- To Study a Fingerprint Hash code using Gabor filter with techniques like Binarisation, and Segmentation and without including Contrast adjustment (Method-3).
- To Generate a Fingerprint Hash code as like Method-1 but without storing its location or pixel positions while forming Minutiae Table (Method-4).
- To Produce a Fingerprint Hash code using Freeman chain code and its first difference value for every 8-connected boundary points by making use of different process like enhancement and binarisation (Method-5).
- To Study a Fingerprint Hash code generation using Euclidean distance value by making use of different process like enhancement and binarisation (Method-6).

- To study and analyze Fingerprint Hash code, OTP, and Password-based Multifactor Authentication Model using ABCD Analysis Framework and also compare this new model with existing almost similar systems.

All the six methods of Hash code generation are evaluated using fingerprint recognition performance evaluation matrices. This is to ensure that all these methods generate unique Hash code for even different fingers of the same person using FVC ongoing 2002 benchmark datasets.

The proposed work is implemented using MATLAB2015a. FVC ongoing 2002 benchmark dataset is used for training and test purpose. To develop the proposed fingerprint Hash code matching system based on an MD5 algorithm using modified filtering and Minutiae details various techniques, algorithms, and methodologies are combined. The different Methods for Fingerprint Hash code generation are explained below.

*Method-1:*

This is the main Method of this research work. Other methods are subsidiary methods which are obtained by removing or adding few techniques. The different phases involved in Method-1 are mentioned below.

1. Preprocessing Phase: Raw fingerprint image of FVC ongoing 2002 dataset is input for this phase and initially this input image is filtered using τ-tuning based contrast adjustment method. Filtering is used for removing noise from the input image, whereas enhancement is applied to improve contrast and enhancing fingerprint pattern.
2. Segmentation Phase: Segmentation consists of approaches or algorithms which separates foreground or Region of Interest (ROI) from the background image. ROI is ridge and valley structure of fingerprint or simply real fingerprint structure. For segmentation, in this research work surfeit clipping method is utilized.
3. Skeletonization Phase: This is actually further extension of preprocessing phase. Here the output of the segmented image is converted into fingerprint skeleton using the edge prediction based method. Skeleton image is obtained by doing series of operation, which includes preprocessing, segmentation, and binarization.
4. Minutiae Identification and Extraction Phase: The skeleton image is again processed with the aid of crossing number based method, which considers eight windows of the ridge flow pattern. This processing is done here again on skeleton and minutiae table to remove background region which is located either outside the foreground or within it. Here ridge ending and ridge bifurcation are considered as minutiae. Again after

extracting minutiae it is post-processed to remove spurious minutiae. The minutiae table consists of four columns, which stores ridge ending, ridge bifurcation, and crossing number and some of first three columns. Finally, in this phase feature are extracted in a format which is easily transformable into hash code by adding salt to hash code in order to make hash harder and which is hard to decrypt.

5. Hash code creation Phase: The extracted features are combined and hash code is generated using md5 hashing technique. The MD5 hash algorithm generates 32-bit long hash code. The goal is to perform key for identification by simultaneously hiding or keeping the fingerprint information secretly or noninvertible way. Even though fingerprint is compromised intruder should not get original features of the fingerprint image.
6. Hash Matching Phase: Hash code is stored in the database. Here WampServer is used for database construction. In WampServer MYSQL database package is utilized for creating database and table. Here two process are involved one is training process and test process. For training purpose FVC ongoing 2002 benchmark dataset is considered and trained and finally stored in database table. As a test sample, one fingerprint image is considered and all the six phases are repeated and finally hash code is compared against already stored hashed code of database.

Each of the phases is dealt separately and usually, an output of one phase acts as an input for next phase. The entire approach is tested using different performance evaluation matrices, which includes, False Match Rate (FMR), False Non Match Rate (FNMR), False Match Rate (FMR), Receiver Operating Characteristic (ROC), Equal Error Rate (EER), Failure to Enroll Rate (FTER), Failure to Capture Rate (FTCR) and elapsed time. In this research work, many existing techniques are combined and one alternative approach is proposed for filtering.

There are another five methods are proposed for Fingerprint Hash code generation, which varies in terms of few procedures and methods. But all these methods produce exact matching or similar hash code for static or already taken and preserved fingerprint image. These Hash codes are having applications in authentication as one factor for identity purpose and can be used for authentication or security purpose along with password or OTP.

*Method-2:*

This is almost similar to Method-1 in terms of first few steps, from first step-enhancement to segmentation. Unlike Method-1, here thinning or Skeletonization process is not performed. Instead of that from the Segmentation image fingerprint features are extracted using 64 × 64

sized Gabor filtering techniques by considering variations in frequencies and angle and finally, Hash code is generated using an MD5 hash algorithm like Method-1.

*Method-3:*

This method is exactly similar to Method-2, but here initial Contrast Adjustment filtering and conversion of the image from integer data type to double type is discarded or ruled out. Like Method-2 here also fingerprint features are extracted using Gabor filtering techniques and finally Hash code is generated using an MD5 hash algorithm like Method-2. Due the elimination of two steps compare to Method-2, this will be faster than Method-2. The minutiae features are extracted directly from the segmented image with the help of Gabor filtering technique.

*Method-4:*

This method is almost similar to Method-1. In Method-1 we extract the ridge ending and bifurcation along with its location details. The location details are nothing but pixel position in the pre-processed thinned image. Here we skip post processing because in fingerprint hash code post-processing does not affect performance of matching efficiency

*Method-5:*

Method-5 is based on Freeman chain coding. Freeman chain code extracts all possible boundaries for an image. Which gives starting x and y positions as x0 and y0. This works based on 8 or 4 connected points with respect to a central pixel. The 8 points are represented from 0 to 7 with is a particular format. In order to generate Hash code, we use x0 and y0 position and chain code value for all boundaries of the image. These values are unique to each fingerprint. This method makes use of segmentation process. This method is invariant to translation. If we translate the image also hash code does not change. Initially, the fingerprint is resized to 256 × 256 sized images and then normalized.

*Method-6:*

Method-6 is based on Euclidean distance matrices of a binary image. In this, it calculates the distance from each pixel to its nearest neighbour pixel with value 1 or not equal to zero. The unique distance value, mean and standard deviation are combined to form hash code. This method also makes use of segmentation process.

Euclidean distance is distance as like measured on a scale from every pixel to next nearest neighbor pixel with value 1. It is effectively used in the binary image. The binary image contains only bi values or two-pixel values as 1 or 0. The different processes used in this Method are as follows.

- Fingerprint image enhancement through contrast adjustment with the aid of proposed τ-tuning based Filtering Method
- Binarisation of the fingerprint image
- Euclidean distance for binary image
- Finding unique values of Euclidean distance without any repetition or duplication

**Proposed Multifactor Authentication Model using Fingerprint Hash code, Password, and OTP:**

Based on the six Methods of Fingerprint Hash code generation a simple and fast method is selected for a hash generation, which acts as Identity Key in Multifactor Authentication model. Initially, fingerprint hash code is generated using Gabor filtering techniques and stored in the database along with one password for each registered user. This process is referred as Registration. User personal details are stored in the separate database including a mobile number. In Authentication test stage, the first user loads his fingerprint image to the Multifactor authentication system, which just acts as a key or user identifier just like email-id in an email. On receiving a request from the client, the server sends an OTP to the client registered the mobile phone.

If the user entered and server generated OTP are matched, then OTP verification completes and server again requests for the password. If both Password and Fingerprint Hash code are verified then that user is considered as Authenticated user otherwise as the non-authenticated user.

The thesis consists of seven chapters. The **Chapter 1** is **Introduction to Biometrics & Fingerprint Recognition System**, which consists of elaborative introduction to Biometrics technology, Basic principles of fingerprint technology, Application areas of biometrics, Types of fingerprints, Fingerprint image preprocessing, Fingerprint features- Level 1, Level 2, and Level 3 features, Fingerprint matching algorithms, Template protection, Fingerprint acquisition methods, Performance matrices of fingerprint recognition, Multifactor Authentication, Problem specification, Motivation for the research and Ideal Authentication System. The proposed Ideal Authentication Model Authentication Model consists of different components like Ideal Security, Ideal User-Friendly, Ideal Input, Ideal Process, and Ideal Performance Evaluation Matrices.

An extensive literature survey on Fingerprint biometric recognition is depicted in **Chapter 2** and is **Review of Literature**. This includes a review on Biometric security, Fingerprint recognition system-past to present, Fingerprint sensing technology, Fingerprint filtering,

Fingerprint Enhancement techniques, segmentation techniques, Minutiae based recognition system, hash Functions, MD5 hash algorithm. This chapter also includes Research gap of the existing study.

**Chapter 3** is **Methodology and Fingerprint Image Preprocessing Techniques**, which explains the concept of research objectives, scope, methodologies and fingerprint image preprocessing techniques. Fingerprint image preprocessing techniques consists of Enhancement phase, Segmentation phase, and Skeletonisation phase. Here Segmentation, Filtering algorithm, and Skeletonisation process are discussed including its theory and pseudo-algorithm. In this Chapter Enhancement phase, Segmentation phase, and Skeletonisation phase output are also discussed by considering input from FVC ongoing 2002 benchmark dataset.

**Chapter 4** is **Fingerprint Feature Extraction and Hash Code Creation Phase.** The existing methods or algorithms theoretical aspects are discussed in detail. This covers Minutiae Identification and Extraction Phase, Hash Code creation Phase, and Hash Matching Phase. Workflow for each phase is discussed and flowcharts are drawn if required. The Feature identification and Extraction consist of many sub phases-pre processing skeleton, minutiae identification, and Minutiae table formation, post-processing minutiae table, Final minutiae table formation and feature extraction in the form required for hash function. All these process theories are discussed in detail. If necessary, the workflow for all sub-phases and main phase is discussed and flowcharts are drawn and discussed. Here the necessary output of Skeletonisation and minutiae extraction are discussed by considering input as FVC ongoing 2002 benchmark dataset. This chapter also includes Hash code creation, Database, and hash matching. The theory related to hash code creation using MD5 hash algorithm is also discussed.

**Chapter 5** is **Performance Evaluation of Fingerprint Hash Code Generation Methods**. In this chapter, benchmark dataset and all six methods are discussed and analyzed. Input for the system will be FVC ongoing 2002 benchmark dataset. Here different performance matrices like False Match Rate (FMR), False Non-Match Rate (FNMR), Receiver Operating Characteristic (ROC), Equal Error Rate (EER), Failure to Enroll Rate (FTER), Failure to Capture Rate (FTCR) and elapsed time are discussed and analyzed. Time complexities of all the six methods are discussed and analyzed using asymptotic Big-Oh notation and the result is shown using the graphical image. A Multifactor Authentication Model is proposed based on combined Fingerprint hash code, Password, and OTP. This model is mainly focused on internet-based online transactions and mobile-based safe transactions. This method is not

suitable for ATM machines and Ordinary attendance maintenance system which does not make use of client-server architecture.

**Chapter 6** is **Factors and Elemental Analysis of Multifactor Authentication Model through ABCD Framework.** This chapter discusses ABCD Framework. The new approach of Multifactor Authentication Model using Fingerprint Hash code, OTP and Password are analyzed using ABCD analysis framework. As per ABCD analysis various determinant issues related to Multifactor Authentication Model for Verification/Authentication purpose are (1) Security issues, (2) User-friendly issues, (3) Input issues, (4) Process issues, and (5) Performance Evaluation matrix issues. The new model is compared with already existing almost similar Multifactor Authentication systems.

**Chapter 7** is **Summary, Conclusion, Limitations and Future Scope**. This chapter lists out the summary, conclusion, limitations, and findings of this research work. The future research directions are also identified and discussed.

# CHAPTER ONE

# *Introduction to Biometrics & Fingerprint Recognition System*

**Contents** **Page No**

## 1.1 INTRODUCTION

In this information and communication technology era, human beings are every now and again requested to verify their identity. Regularly, this is done using passwords while seeking activities like public security, access control, surveillance, and application sign on, and so on. In an organization, educational institutions, political and government offices, security has become essential aspect and more and more research is carried out for the purpose of verification or identification (Maltoni, Maio, Jain, & Prabhakar, 2003). The issue of normal framework or traditional security involves the assurance of framework components. Therefore, this security can be easily breached when a password is divulged, a card is stolen or through social engineering (Mitnick & Simon, 2003). Besides, a large group of people utilize a similar password crosswise over various applications; an impostor, after deciding or accessing a single password, would now be able to get to different applications. Basic passwords can be effortlessly speculated while troublesome or rigid passwords might be difficult to review, and passwords can likewise be broken by dictionary attacks. The requirement for solid client validation procedures has expanded in the wake of uplifted worries about security and quick development in systems administration, correspondence, and portability. These constraints related to the utilization of passwords can be improved by the joining or combining of better strategies for client confirmation.

Biometrics innovation has ended up being a precise and proficient response to the security issue. Biometrics is a developing field of research and has been dedicated to the unique proof or authentication of people utilizing one or multiple inherent physical or behavioral characteristics. Among these biometric innovations, hand based biometrics, including unique a finger impression or fingerprint, two-dimensional and three-dimensional palm prints, hand geometry or hand shape, hand vein, finger-knuckle print and so forth., are the most mainstream and have the biggest offer in the biometrics showcase. Biometric has increasingly become popular due to its nature of universality and uniqueness in human identification or verification (Cuntoor, Kale, & Chellappa, 2003). This is due to the advantages of these traits or characterstics such as low cost, low-resolution imaging, and stable features. Because of this advancement, a new type of biometric-based verification and identification techniques or methods are developed, which are unique for individuals (Toledeno et al., 2006).

A large portion of the work found in the literature in connection with biometric traits utilizes iris, face, voice, fingerprints, palm prints, and hand geometry. The biometric fingerprint is

one of the most normal and generally utilized biometric attributes throughout the world for recognition purpose. As a proof for this, Chinese utilized unique mark for marking records since 1000 years (Ali & Hassanien, 2003). As indicated by the examination and study led by BCC Research on biometrics acknowledgment or recognition framework (http://www.bccresearch.com/report/biometrics-technologies-markets-ift042e.html), the overall market for biometric developers totalled $14.9 billion out of 2015 and is depended upon to reach $41.5 billion by 2020 growing at a compound yearly improvement rate (CAGR) of 22.7% from 2015 to 2020. Automatic Fingerprint Identification System (AFIS) and fingerprint system as a section came to $8.8 billion of each 2015 and $24.4 billion by 2020, with a CAGR of 22.8% through the time period. The face, iris, vein, and a voice biometrics trait will increase from $4.2 billion out of 2015 to $11.9 billion by 2020, a CAGR of 22.9% for the season of 2015-2020. These statistical figures point out that the fundamental client authentication of biometric innovation will incorporated by government divisions, legal requirement, and military, transport and aviation management system.

The recent innovative researchers significantly concentrate on cell phones. Cell phones have become important electronic device or equipment in human life. Clients get to their messages, informal organizations, financial balances, and different sites by means of cell phones. Portable equipment makers, working framework and application engineers take an assortment of safety efforts because of the individual, private as well as the touch sensitive nature of the data move away in cell phones. The utilization of biometric authentication on cell phones began with cameras. Initially, cell phone producers have included biometric validation or identification frameworks like the increasingly well known unique fingerprint recognition system. This is a more secure and handy answer for recognizable proof on cell phones. The unique fingerprint traits of a man are exceptionally exact and are special to a person. Authentication frameworks in light of unique fingerprints have demonstrated to create low false acceptance rate and false rejection rate, alongside other favorable circumstances like simple and easy usage strategy. Additionally, the unique fingerprint ordinarily stays unaltered from birth until death (Mahajan et al., 2009). Beside from being extraordinary and constant, fingerprints can be accumulated in a non-obtrusive way with no symptoms (Schmeh, 2003). The current fingerprint technology is quite mature to identify or verify human using various diverse types of matching or comparing the process with already stored features or templates. One of the potential threats in a biometric framework is the

compromise of the biometric template, which may prompt genuine security and protection dangers. The major part of the fingerprint template protection methods does not meet all the desirable necessities of a biometric traits or features like revocability, security, protection, and high matching precision (Jain A.K., et al., 2013). Specifically, high matching accuracy in the fingerprint biometrics has been a difficult issue because of huge intra-client varieties (e.g., turn, interpretation, nonlinear twisting, and fractional prints). So there is a huge necessity of building a highly secured and not reversible or revocable fingerprint template protection and recognition system, which can serve the need of diverse applications in information, communication, surveillance and security fields. The most attractive properties of high exactness, low error rate and greatest speed or execution time are yet to be accomplished with Automatic Partial Fingerprint Recognition System (APFS). Consequently, the present research means to a build up an Automatic Partial Unique Fingerprint Recognition System, which also takes care of template protection to validate a person.

Fingerprint Hash code is not used for full security or authentication purpose but it can be combined with other security elements like password or OTP in order to enhance security. Fingerprint Hash code acts as a key, which can uniquely identify every person. So it can be replaceable with user-id or username and can work along with text-based or picture based or pattern based passwords.

## 1.2 BIOMETRIC TECHNOLOGY

Biometrics is an investigation of checking and setting up the identity of an individual through physiological components or behavioral qualities. Even though biometric technologies differ in complexities, capacities and performance parameters, still all offer a few regular or similar components like biometric sensor module, feature extractor module, a matching module, decision-making module and system database. Biometric frameworks are basically patterned recognition or matching systems. Usually diverse of application areas get benefited by the biometric system which includes login for computer and network, access for physical devices, security in mobile phone devices, government-related identification cards, transport systems, medical records, etc.

Biometric system makes use of different capturing devices with an intention to acquire biometric traits to an automated system. These include camera and scanning devices to capture images, speakers for recording voice, the special type of sensors to capture behavioral

traits, computer hardware, and software to extract, purify or enhance, store and compare the characteristics or features of biometric traits. The biometric sensor module is utilized for acquiring or recognizing data from clients.

The sensor module as a rule embodies or combines a quality check module. Quality estimation is performed to guarantee that the secure biometric can be dependable or adequately handled by a feature extractor. At the point when the information test does not meet the qualification criteria, this module asks for the client to give the biometric input once more.

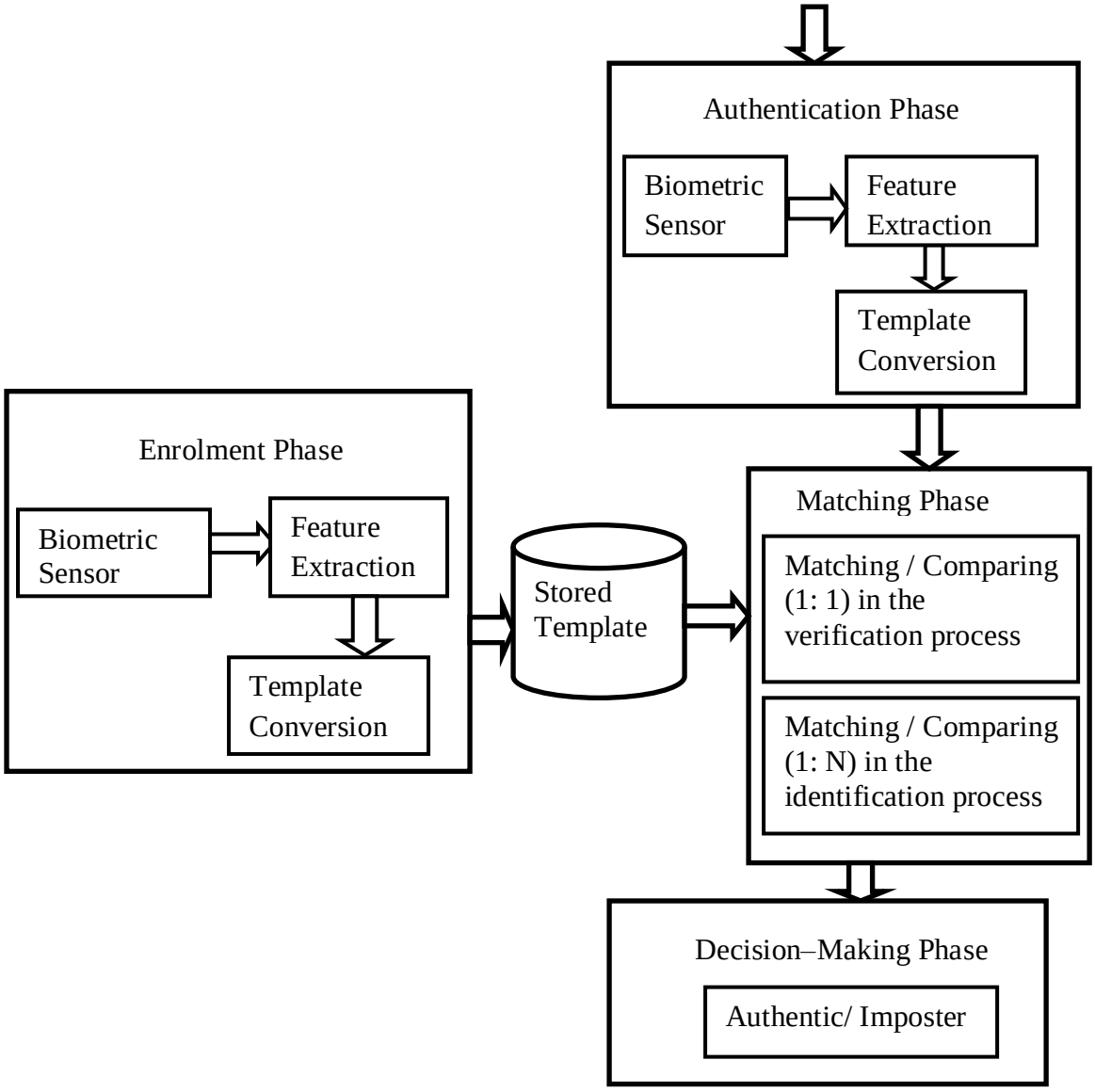



**Figure 1.1:** Biometric Verification or Identification System

The feature extractor module extracts an arrangement of remarkable components or simply features of the secured biometric information. The list of capabilities is another depiction of the first or original biometric information. These features are called as a template and stored in a database or files for future matching or comparing process. A matching module compares the new input biometric features called as a sample with the already existing template. The yield is a coordinating or matching score, which is the level of similarity between the sample and template. Decision-making module is a module that chooses the identity of the client in light of the coordinating or matching score. System database is utilized for storing client templates caught in the course of the enrolment process. The size of the database relies upon the application. Templates are usually stored in remote places or central server or in a local system like mobile device (Vacca, 2007). Biometric recognition is made of two modes, called verification and identification (Maltoni, et al., 2003). Verification can also refer to authentication is used to confirm the person's identity, means grant the system to a person who their claims to be and they are already known to the system.

Identification refers to knowing the person from the group of many suspected members. Verification does one-to-one matching and identification does one-to-many matching or comparisons. In a verification system, after enrolment process enrolled person provides identity through biometric features, which can be any type of biometrics, the systems captures the biometric traits and process it and generates a template, which can be called a test template. The system then compares test template with the already stored template, to determine whether the system template and test template matches or differs. The verification process is frequently referred as 1:1 (balanced) matching. As shown in figure 1.1 biometric verification system consists of four phases of Enrollment phase, Authentication phase, Matching phase, Decision-Making phase. In Enrollment phase, Biometric data are captured using biometric sensors or any other types of capturing devices. These data are processed and features are extracted and which are converted to a unique format called template. This template is stored in the databases or files for future matching or comparison process.

In Authentication phase, the same process of enrolment phase is repeated for one sample biometric data of the enrolled person, except that the template is not stored in the database. In Matching phase, this sample template is compared with the stored template. Based on the matching process score is calculated and a high score reveals that the sample template or biometric data is an authenticate person or else imposter person. The biometric identification

system is similar to a verification system, but here in matching phase instead of 1:1 comparison 1: N comparisons are made in order to identify the person rather than authenticate the person. Unlike verification process, sample template is compared with all reference templates to find a match. The identification process is mainly used to find criminals. Each time a biometric is caught, the template is probably going to be one of a kind or unique. In view of a threshold that sets up the satisfactory level of similitude between the trial and reference template, biometric frameworks can be arranged to make a match or no-coordinate choice. The score representing the level of closeness is produced, and this score is compared with the threshold to make a coordinate or no-coordinate choice. Contingent upon the setting of the threshold in the identification, infrequently a few reference templates can be considered matches to the trial template, with the higher scores relating to best matches.

### 1.2.1 Types of Biometric Technologies

A human body has a few physiological attributes that can fill in as biometric highlights. Additionally, a person builds up a few special behavioral qualities, which can likewise fill in as biometric highlights. A growing number of biometric advancements have been proposed in the course of the last several years, but in an automatic biometric identification system, only a few years back leading biometric came into front line (Adnan et al., 2004). In light of the attributes, biometrics falls into two classes, to be specific, physiological biometrics and behavioral biometrics (Ross, Nandakumar, & Jain, 2006). Any human physiological or behavioral traits can act as biometric characteristics, if and only if it serves some basic properties as universality, distinctiveness, Permanence, and collectability.

Every human being can be recognized through observation of particular characteristics, which mainly involves different types of visual biometrics, chemical biometrics, auditory biometrics, behavioral biometrics, and Olfactory or odor biometrics. Physiological attributes are identified with the state of the body and incorporate unique fingerprint image, face, DNA structure, ear structure, palm print, hand geometry pattern, iris recognition, retina pattern and odor/scent. Behavioral qualities are identified with the conduct of a man like a mark, keystroke dynamics, gait behavior and voice biometrics. A few specialists have begun the term behavior metrics to represent the last class of biometrics.

More conventional methods for access control incorporate token-based or object-based authentication frameworks, for example, a driver's license or passport and knowledge-based

identification frameworks, for example, a password or personal identification number (Jain et al., 2000). Since biometric identifiers are special and unique to people, they are more solid in checking identity than token and information-based strategies. In any case, the gathering of biometric identifiers raises protection about a definitive utilization of this data (Weaver, 2006; Sahoo et al., 2012). Today many biometric technologies such as the face, iris, voice print and hand-based biometrics traits (palm print or fingerprint) can be used to identify persons. Each biometrics has its advantages and defects; no single biometric can effectively meet all requirements like accuracy, practicality, and cost of all applications (Maltoni, Maio, Jain, & Prabhakar, 2003). Some of the most frequently used biometric systems are shown in figure 1.2.

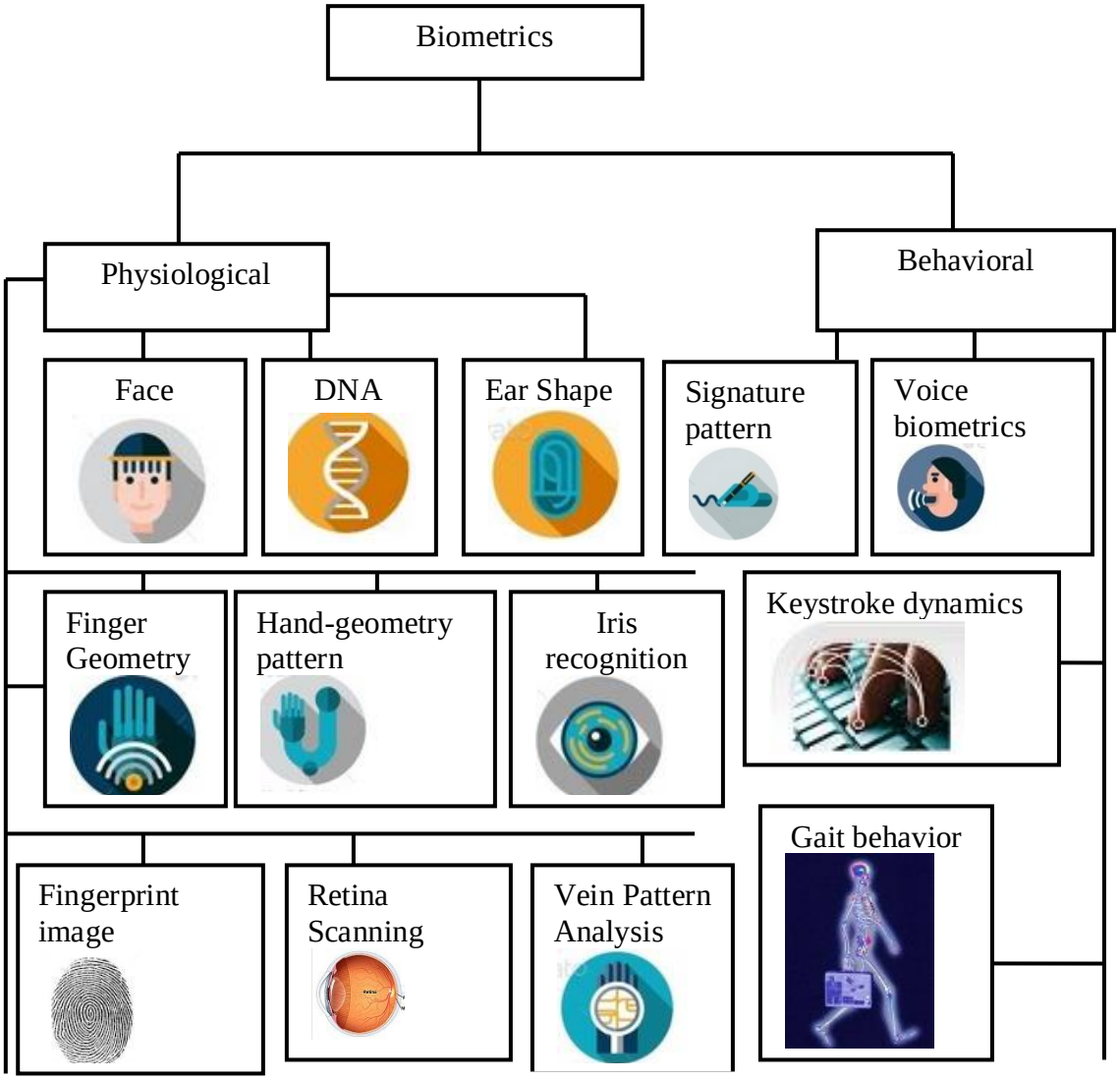



**Figure 1.2:** Examples of Biometrics

Table 1.1 gives comparison of different types of physiological and behavioural biometric based on different factors, which includes (1) Universality, (2) Uniqueness, (3) Permanence, (4) Collectability, (5) Performance, (6) Acceptability, (7) Circumvention, (8) Cost, (9) Size of template, and (10) Security level. In table 1.1, the different abbreviations H, M, L, and S represents High, Medium, Low and Small measures respectively.

Face Recognition (Li and Jain, 2005) identifies user or people by analyzing the unique features of the face, which are not changed during the lifespan of the person unless and until some real wound or damage occurs. The features include the color of the eye, the color of skin, and nose shape and the upper outlines of the eye sockets (K. Krishna Prasad and Aithal P. S., 2017). The primary part of Deoxyribonucleic acid (DNA) molecules is the long-term storage of the information without affecting to its structure or behavior (Arya et al., 2011). DNA structure is extensively used in the forensic lab for crime detection by utilizing DNA found in blood, semen, skin, salivation or hair, which is scientifically referred as DNA matching and it is a solid technique for recognizing or matching DNA.

**Table 1.1:** Comparison of various Biometric Techniques
Source: (Saini & Narinder, 2014; Jain et al., 1997)

| **Biometrics** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
|---|---|---|---|---|---|---|---|---|---|---|
| Fingerprint image | M | H | H | M | H | M | H | L | S | L |
| Face image | H | L | M | H | L | H | L | H | L | L |
| Hand Geometry | M | M | M | H | M | M | M | M | L | M |
| Keystrokes Dynamics | L | L | L | M | L | M | M | M | M | L |
| Dorsal Hand Veins | M | M | M | M | M | M | H | M | M | H |
| Iris recognition | H | H | H | M | H | L | H | H | S | M |
| Retinal | H | H | H | M | H | L | H | H | S | H |
| Signature | L | L | L | H | L | H | L | H | M | M |
| Voice | M | L | L | M | L | H | L | M | S | L |

Human ear structure (Kus, Kacar, Kirci, & Gunes, 2013) do not change radically over time and easily extractable biometric feature, which contains some characteristics like universality, distinctiveness, permanence, and collectability. Palm prints biometrics (Parashar et al., 2008) refers an image captured at palm region of the hand is most promising to identify an individual based on unique palm properties. Iris (Daugman, 2006) is an automatic strategy

for biometric authentication that utilizations numerical or mathematical procedures on video pictures of either of the irises of a person's eyes, whose confounding patterns are exceptional, stable, and can be seen from some separation. Retina (Dowling, 2007) is one of the physiological biometric features which usually never changes and takes into consideration unique patterns in retinal blood vessels and sometimes perplexed with iris biometrics. Out of these iris and retina are more accurate because of some micro unique details.

Hand geometry biometrics (Jain et al., 2008) system can be used for authentication or verification purpose for an individual by measuring nearly 96 measures of the hand like width, height, and length of the fingers, the distance between joints and shape of the knuckles etc.

Usually, natural living beings are made out of concoction components, some special specious produces scent or odor that is a trademark of that life form. Along these lines, the odor can be utilized as a particular trademark crosswise over species (Wongchoosuk et al., 2011). The investigation of odor for human confirmation is under scrutiny both in the scholarly and in the business. Since this is an extremely complex assignment, practical gadgets to capture this are as yet not available.

Signature recognition belongs to behavioral biometrics with two forms as static and dynamic with the signature written on the paper and signature is drawn in the digitized sensor respectively and this sample template is compared with already stored signature template and score is calculated and based on the score level user will be authenticated or rejected (Faundez-Zanuy, 2007). Keystroke progression or dynamics is identified with the way individuals sort characters on consoles. Its consideration as a developing biometric trademark is supported by mental examinations, which exhibited that human dreary or routine activities are unsurprising and understandable and along these lines, an individual could be described by their keystroke flow (Nauman & Ali, 2010). Gait is a budding feature for behavioral biometrics which works based on walking style or habit of the human beings (Ailisto et al., 2005; Mäntyjärvi et al., 2005). Most of the gait recognition approaches are based on machine observation techniques and it’s not well suited for sophisticated or dedicated high-security systems.

Voice biometrics is yet another type of behavioral biometrics which extracts information from the stream of speech signals by measuring its properties pitch, amplitude and frequency (Woodward et al., 2003).

Fingerprint identification is one of the most important biometric technologies compared to other biometrics due to its popularity and widely available technologies since early 1975 (Halici et al., 1999), which has drawn a considerable amount of interest recently. A fingerprint is a physiological feature of an individual that uniquely identifies the person based on fingerprint ridge and valley pattern (Jain and Maltoni, 2003). As fingerprint is the main focus of this research, it is discussed elaborately in following sections.

Although, the entire previously mentioned biometric framework gives off an impression of being the evident innovation for individual verification, it is not yet a perfect method, with the accessibility of reasonable, compact biometric sensors and quick handling processor. Fingerprint identification is ending up progressively obvious that a more extensive utilization of biometric innovation would require better answers for conquering four basic boundaries (Dharchaudhuri, 2010):

I. Security of System: How to ensure that biometric frameworks are definitely not vulnerable to damage or attacks.
II. Privacy concern: How to ensure that the biometric framework is being only utilized for the authentic reason.
III. Identification purpose: How to adequately identify or recognize a user or person with more accuracy (e.g., how to perceive a man with 99.999% precision).
IV. Preserving features: How to effectively store and preserve the biometric template as safe and nonreversible.

This research work endeavors to address these four challenges. With a specific end goal to join biometric framework security (that is, to ensure that fraudsters don't penetrate the framework), protection issues (that is, to ensure that trusted framework managers don't abuse the system), and preserving issues (that is to ensure that the template is revocable) the biometric type chosen must have associated with following qualities.The physical features should not change through the span of the individual's lifetime.

- The physical features must distinguish the distinctive individual exceptionally.
- The information must be effectively checked against the genuine individual in a straightforward, automatic way.
- Enough technologies are required to capture, process, and store.

These attributes are completely upheld by the fingerprint biometric. The fingerprint is one of the most established types of biometrics that has been ended up being exceptionally solid.

The fingerprint of every individual is unique or not changeable and does not change in the course of their lifetime. In addition, the semsor or acquasition devices and programming or technoogy for fingerprint biometrics are progressively getting to be plainly less expensive.

### 1.2.2 Challenges of Biometric System

Despite the fact that biometric methods have been effectively connected in a vast number of true applications, outlining a decent and robust biometric system is still a testing or questionable issue. The four fundamental factors that expansion the many-sided quality furthermore, challenges of system configuration are accuracy, scalability, security, and protection (Nandakumar 2008; Jain et al., 2004).

An ideal or error-free biometric system should make an accurate and correct decision on every test sample regardless of any performance degrading factors like variation or differences in inter-class, similarities in intra-class, different representation for enrolled and sample data, and extreme noise and low sample data quality. Error in different performance evaluation factors of biometrics like false acceptance rate, false rejection rate also influences on the overall performance of biometrics system. Biometrics system precision can be improved by discovering invariance, unambiguous, robust and fault tolerance features or models to extraordinary represent the high biometric quality. Scalability is nothing but the size of the database. In a biometric verification system, it will be small and only a few users' data will be stored in the database and each time in matching process only one sample template is compared with only one reference template. But in a Biometric identification system, a sample template is compared with all stored reference template and also the size of the database is extremely huge. For instance, in an identification system like crime detection, one sample template data may be compared with millions of stored template to identify the crime person. In these scenarios, indexing and filtering techniques (Ratha et al., 2007) can be effectively applied to reduce the burden of searching the large-scale database and the searching process becomes extremely complex and time consuming when the matching template exists as the last record and sequential search is enforced.

The issue of guaranteeing the security and trustworthiness of the biometric information is critical and unsolved. There are two main drawbacks of biometric innovation, which are biometric features are not recoverable. In wrost case, if the user biometric fingerprint has been stolen, it is difficult to replace unlike a stolen smart card, ID, or resetting a password.

Along these lines, building up the credibility and security of biometric information itself turns into a challenging research issue. Biometric information gives uniqueness but does not give full security. A man leaves his fingerprints on each surface he touches and a face image can be watched anyplace by anybody.

As like password based system security threats or attacks, even biometrics system faces security threats, but compare to the password-based system, in biometric-based system more intelligence is required. We can identify nearly 8 basic types of attacks in biometric-based recognition system and these attacks prove that biometric features are also vulnerable to security threats (Ratha et al., 2001). It also depicts to researchers security of biometrics information is new and challenging research problem especially in forensic and defense system and should be emphasized more and more. A few solutions are given by different researchers; few of them are Uludag et al., (2004) and Brin (1998).

### 1.2.3 Vulnerabilities in a Biometric System

Unlike Knowledge-based and token or object-based security system, the biometric system not easily vulnerable to security attacks, but imposter or intruder will try to attack the system by identifying and getting into the root of the weaknesses of biometric systems (Maltoni et al., 2003; Uludag and Jain 2004). Some of the common vulnerabilities of biometric system are listed below;

- Circumvention
- Covert acquisition
- Collusion
- Coercion
- Repudiation
- Denial of service

Circumvention: An impostor will act as legitimate or authenticated user by means of technical measures and will gain access to the protected data of the authenticated user. The examples are access the medical related data, bank account details or any personal details of legitimate user etc.

Covert acquisition: An impostor may surreptitiously acquire the crude biometric information of a client to get to the biometric system. The latent fingerprint of a client or template stored in the database can be used as a source to regenerate legitimate user biometric information

and used for accessing the protected data by the intruder. The intruder will not only access the data but also modify some sensitive data and will end up with the non recoverable loss for the authenticated user.

Collusion: A person with wide user privileges like system administrator or chairman will intentionally modify the system protection parameters and will indirectly invite the intruder to access the secret data of the legitimate user is called Collusion.

Coercion: In coercion, an intruder may constrain the authenticated user to reveal the biometric secret key in an unethical way to access the biometric system (example using gunpoint).

Repudiation: A corrupt user will access the biometric information and uses all facilities of the system and finally denies accessing the system. A bank clerk may modify the financial records of a customer and then deny responsibility by claiming that an intruder could have possibly stolen the biometric data.

Denial of service: An intruder may overpower the system assets or resources to the point where authenticated clients desired access will be denied benefit. This results in slow down or stoppage of the system or simply degrade the system performance. Example for system degrading in automated fingerprint identification system an intruder will enroll many noise samples to test image, which will affect the system capable of recognizing the authenticated user.

Ratha et al., (2001), identified multiple types of attacks that can be initiated against a biometric system is shown in figure 1.3: (a) a fake biometric feature, for example, a false fingerprint image might be introduced at the sensor, (ii) unlawfully trapped information might be resubmitted to the system, (iii) the feature extractor might be replaced by a wrong software or virus program that produces pre programmed traits sets, (iv) Genuine feature sets might be replaced with artificial feature sets, (v) the matcher might be replaced by a predetermined program that dependably yields high scores in this way opposing system security, (vi) the template put away in the database might be adjusted or evacuated, or new template might be presented in the database, (vii) the information in the correspondence channel between different modules of the system might be modified and (viii) an overall result yield by the biometric framework might be superseded or simply altered. In this thesis, template security of the biometric system is considered as cancellable template and templates are even if compromised, the intruder will not get original biometric traits.

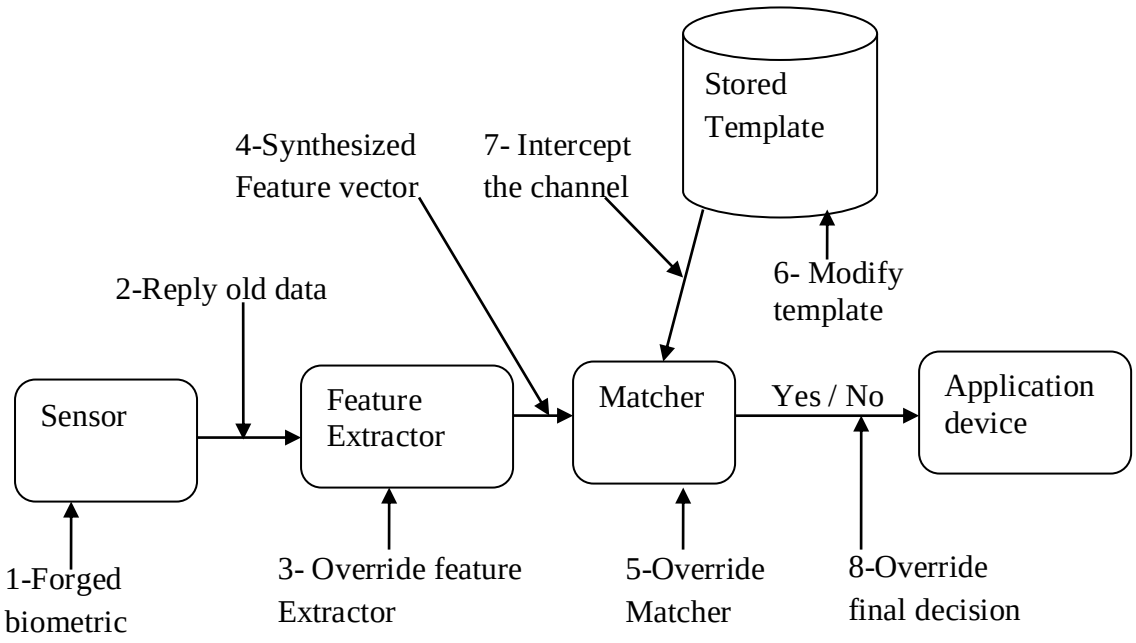



**Figure 1.3:** Vulnerabilities in a Biometric System
(Adopted from Ratha et al., 2001)

## 1.3 FINGERPRINT BIOMETRICS

A fingerprint is an influence or lines of an impression from the friction ridges, from the floor of a fingertip of a person's finger. A friction ridge is a raised part of the epidermis on the fingers and includes one or extra linked ridge units of friction ridge skin. These are every so often regarded as "epidermal ridges", which might be because of the underlying interface between the dermal papillae of the dermis and the inter-papillary (rete) of the epidermis. Those epidermal ridges serve to enlarge the vibrations brought on, for example, at the same time as fingertips brush across a choppy floor, higher transmitting the alerts to sensory nerves concerned in nice texture perception (Kwok, 2009). Those ridges additionally assist in gripping rough surfaces, as well as clean wet surfaces. Impressions of fingerprints may be left behind on a floor with the aid of the herbal secretions of sweat from the eccrine glands which can be present in friction ridge pores and skin, or they will be made via ink or other materials transferred from the peaks of friction ridges at the pores and skin to a pretty easy floor including a fingerprint card (Olsen, 1972). Fingerprint statistics commonly incorporate impressions from the pad at the remaining joint of fingers and thumbs, although fingerprint cards also commonly record portions of lower joint areas of the hands.

The distinctiveness of fingerprint is added forward by using ridge patterns and it has been proved that the information in small regions of friction ridges is in no way repeated. These

friction ridges broaden in a human system all through the fetus level itself (https:// barcode.ro/tutorials/biometrics/fingerprint.html). They are continual for the duration of life and therefore fingerprint-primarily based biometric structures are utilized by more than fifty 52% of the biometric marketplace as an authentication device based totally on biometric trends (Maltoni, Maio, Jain, & Prabhakar, 2003).

The usage of fingerprints for authentication is a universally prevalent solution and a majority of the population has legible fingerprints. This is more than a number of humans who have passports, license and identification cards. It has fairly one of the maximum accurate forms of biometrics available. Apart from the above benefits, the following benefits have additionally been diagnosed.

- The capturing process is simple and requires no training.
- Fingerprint biometrics is a most low-cost biometric user authentication method.
- Fingerprint biometric template occupies very low memory space.
- For capturing processing and matching advanced technologies are readily available

### 1.3.1 Basic principles of Fingerprint Technology

The basic standards of fingerprint generation were scientifically mounted by Sir Francis Galton, a British scientist referred as the father of fingerprint technological advances and are given below.

Permanency or Persistence: This first fundamental principle of fingerprints describes their area of expertise. In keeping with this principle, a fingerprint is a human being feature and no two fingers are observed to have identical ridge styles. This characteristic is valid for even equal twins, who share same genetic code, do not have similar fingerprint ridge pattern. Fingerprints are believed to be formed during the growth of the human embryo and by the point, it is six months old, fingerprints are formed.

Consistent and Constant: This essential property states that a fingerprint, all through the lifetime of an individual, remains unchanged. They may extend with bodily growth, but the patterns remain the equal, just like inflating a balloon doesn't alternate what's revealed on it. This is the most generous characteristic of fingerprints that make them useful for identity management, authentication, and biometric packages. Even the signature of someone, that's taken into consideration a behavioral biometric, may change beyond regular time, but fingerprints remain unchanged throughout someone's lifetime. Fingerprints by no means

change themselves however in some cases, because of wound or harm (as an example, excessive burn or working in positive industries) they will distort or disappear. Being on fingertips, they have usually the first point of physical contact, but, they are no longer broken via superficial injuries. A few clinical conditions also can purpose fingerprints to vanish.

Uniqueness: Two person fingerprints at the outset might look like similar, but every person fingerprint ridge patterns are unique. These ridge patterns can be used for systematic classification in diverse applications.

As a result, it may be understood that fingerprints are perfect in the course of human life and consequently, are most dependable, unchangeable and reliable in setting up the identification of a person.

### 1.3.2 Applications Areas of fingerprint Biometric

Fingerprint biometric has been utilized in numerous areas together with entrance management and door-lock programs, smart cards, vehicle ignition control framework and fingerprint controlled access control system. Because the superior technology allows even extra compact fingerprint sensor size, the variety of application is expanded to the cellular market. Thinking about the developing segment of the existing mobile marketplace, its ability is the best of all utility markets. The fingerprint markets are categorized as given in Figure 1.4.

The fingerprint is one of the most frequent and most dependable assets utilized in criminology to pick out criminals and fraudulent persons. It is also used within the identification of unidentified body wherein fingerprint facts are compared with current databases. They may be an increasing number of users in many crucial carrier oriented industries like banking, licensing and passport, in which usage of fingerprint reduce the incidence of forgery, impersonation, and frauds to a brilliant volume. They have utilized in assets and civil instances in which the usage of historical records of the registration department and on files allows to solve important cases.

Presently, fingerprints captured from newborn toddlers are used in hospitals to avoid oversight of interchangeability in a safe manner to keep the print of mother and toddler together. It is also used by old age pensioners and many commonplace services like railway, electricity board, in which temporary laborers are fingerprinted to keep away from intelligent frauds. Nowadays, fingerprints are used to open computer systems. Software program geared

up locking system is supplied for robust rooms of banks and even doors of houses thereby heading off unauthorized access. Consequently, with its wide usage, fingerprint popularity systems are of excessive demand.

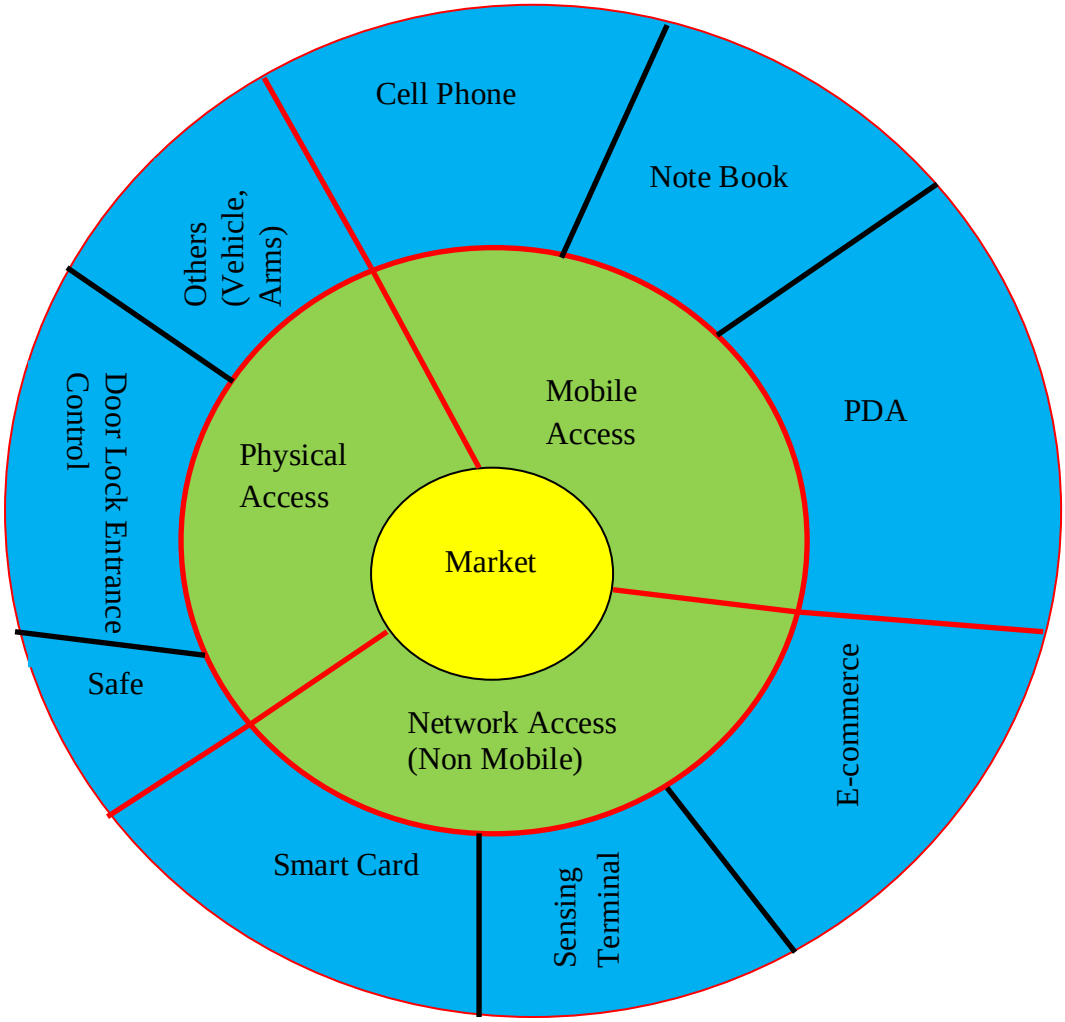



**Figure 1.4:** Application Areas of Fingerprint Biometrics
(Source Maria et al., 2012)

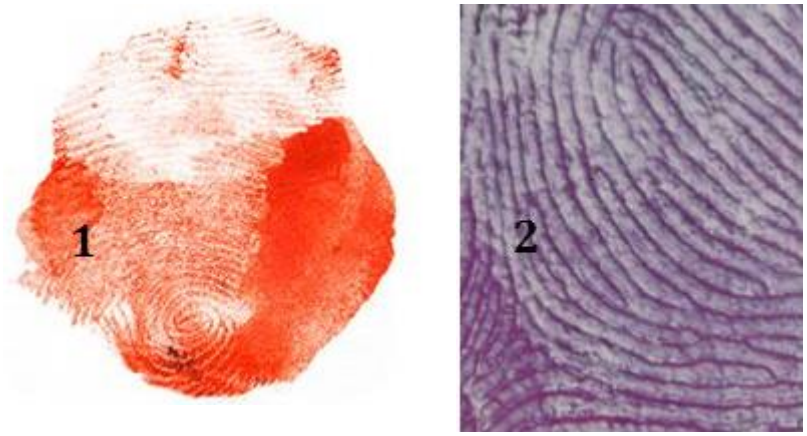
### 1.3. 3 Types of Fingerprints

From olden days, three styles of fingerprints may be obtained, namely, exemplar prints, latent prints and plastic prints. Exemplar prints, or recognized prints, is the name given to fingerprints intentionally accumulated from a topic, whether for functions of enrollment in a system or at the time of arrest for a suspected criminal offense. Exemplar prints may be accumulated the use of stay experiment or by way of using ink on paper cards. An example is shown in Figure 1.5.

Patent prints are friction ridge impressions which might be obvious to the human eye and which have been due to the transfer of remote places material from a finger onto a surface. Some obvious examples might be impressions from floor and moist clay. Due to the reality they're already seen and have no want of enhancement they may be commonly photographed as opposed to being lifted inside the way that latent prints are. Patent prints can be left on a floor by way of using materials consisting of ink, dust, or blood.

**Figure 1.5:** Example of exemplary fingerprint
(Source: http://images.google.com)

Plastic prints are obvious, stimulated prints that happen when a finger touches a delicate, pliable surface bringing about a space. A few surfaces that may contain this kind of unique mark or fingerprint are those that are newly painted or covered, or those that contain wax, gum, blood or whatever other substance that will diminish when hand held and afterward hold the finger edge impressions. These prints require no enhancement with a specific end goal to be viewed, and are effectively noticeable.




(1) Patent print (2) Plastic print

**Figure 1.6:** Example for patent and plastic print
(Source: http://images.google.com)

A plastic print is a grating or harsh edge impression left in a material that holds the state of the edge detail. Although not very many criminals would be reckless enough to leave their prints in a chunk of wet dirt, this would make a great plastic print (Lee, 1973). Regularly experienced illustrations are melted candle wax, putty expelled from the border of window sheets and thick oil stores on auto parts. Such prints areas are already readable and viewable condition and require no enhancement further. Examples for patent and plastic print are shown in figure 1.6.

Irrespective these types, fingerprints are generally classified into three types as rolled, plain and latent fingerprints based on the procedure, how they are captured or collected. In rolled fingerprint image is captured from one end of the finger to another end by rolling and mounting on capturing device in order to obtain complete ridge and valley details of the fingerprint. The plain fingerprint is directly captured using a fingerprint capturing device by pressing a finger tip onto a flat surface. Rolled and plain fingerprints are acquired in a sophisticated attended mode; they will be having good visual quality at the time of training and performance quality at the time of matching one to one or one to many for verification or identification purpose.

Latent prints are unique finger impression buried in a surface and are normally unnoticeable to the naked eye. These prints are the consequence of sweat which is gotten from sweat pores found in the edges of fingers. At the point when fingers touches other body parts, oil or other small particles adhered for example, a light or a film of these substances might be exchanged to that object.

(a) Rolled (b) Plain (c) Latent

**Figure 1.7:** Types of Fingerprints
(Source: http://images.google.com)

The impression left on the particle leaves a particular pattern of the ridges of that finger. These fingerprints must be upgraded upon gathering and, in light of the fact that they fill in as a method for distinguishing the source of the print, they have ended up being to a great degree significant throughout the years in the identification of its source.

## 1.4 FINGERPRINT FEATURES

The fingers are blanketed or covered with a special type of skin which includes minute accelerated traces, known as ‘papillary ridges’ or ‘friction ridges’. The depressions found in between the elevated ridges are called ‘furrows’ or ‘valleys’. Except ridges and furrows, a few white traces, known as, ‘creases’ can also be present. The friction skin region of a finger is not occluded by way of hair or glands. A fingerprint is the reproduction of the friction pores and skin surface of the primary phalange of the finger. In an influence excited by black printers ink, these ridges are represented as ‘black lines’ and the furrows are represented by ‘white strains’. The individuality characteristic of the fingerprint is determined by the local ridge characteristics known as minutiae, which is one of the most important characterstics utilized in fingerprint identification systems (Newham, 1995; Moenssens, 1975). There are more than one hundred fifty minutiae characteristics are diagnosed in literature. These local ridge characteristics aren't similarly distributed. Minutiae are labeled into two forms primarily based on trivialities factors as ridge ending and bifurcation. Ridge ending starts off grow at a point and results in every other point all at once (Lee et al., 2006). Bifurcation is the feature wherein ridge starts from an arbitrary point and actions in a direction and at any other arbitrary point splits into paths or clearly becomes ridge forks. A good exceptional fingerprint picture accommodates the least 50-100 minutiae.

Ridge ending and ridge bifurcation superimposeed in fingerprint image. Computerized fingerprint matching algorithm compares these local ridge traits (minutiae) and their association to achieve rankings on the time of identification and verification process. Yet another trait of minutiae is called delta which is a point on friction ridge, at or nearest to the point of divergence of ridge ending and ridge bifurcation and looks like the shape of delta. From the core ridge ending, ridge pattern, and ridge bifurcation originates.


(a) Ridge ending (b) Bifurcation (c) Short Ridge (d) Delta and Core

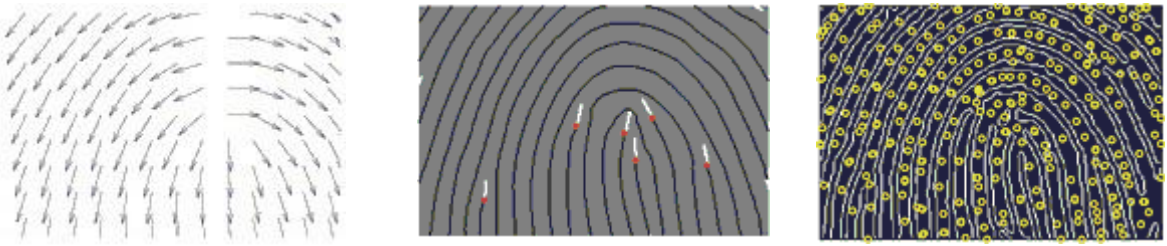
**Figure 1.8:** Basic Fingerprint Features
(Source: http://images.google.com)

The diverse features that may be accumulated from a fingerprint are categorized into 3 groups (Maltoni, et al., 2009), specifically,

Level 1 Features - Includes widespread outlier shape of ridges like ridge flow and ridge pattern configurations (Figure 1.9 (a))

Level 2 Features – Ridge ending and ridge bifurcation or minutiae points (Figure 1.9 (b))

Level 3 Features-Consists of micro details like ridge pore and ridge contours which are usually difficult to extract and process. (Figure 1.9 (c))



(a) Level 1 (b) Level 2 (c) Level 3

**Figure 1.9:** Three Levels Features of Fingerprint
(Source: Krishna Prasad, K., & Aithal P. S. (2017a); http://images.google.com)

### 1.4. 1 Level 1 Features

Level 1 feature incorporates macro information and encompasses the overall ridge flow and pattern configuration. Level 1 feature includes these features. Fingerprint pattern is mainly classified into three as Loop pattern, Whorl Pattern, and Arch pattern deviates. In the loop, pattern ridges starts from either surface of the impression or pattern, re-curves or touch an imaginary line drawn from Delta to the middle and terminates at the equal facet from where it's originated.

In arch pattern ridges start from one side of the fingerprint sample runs to another side without doing backward turn. Whorl pattern includes series of circles which starts from a random point and ends at the same point. Only level 1 feature is not enough to uniquely

identify the fingerprint image, whereas level 1 feature is used for classification or image enhancement purpose. Some examples for the level 1 feature are simple arch, tented arch, left loop, right loop, composite whorl, concentric whorl, Imploding whorl, press whorl, spiral whorl, peacock's- eye whorl, and variant whorl are shown in Figure 1.10.

In arch pattern ridges start from one side of the fingerprint sample runs to another side without doing backward turn. Whorl pattern includes series of circles which starts from a random point and ends at the same point.

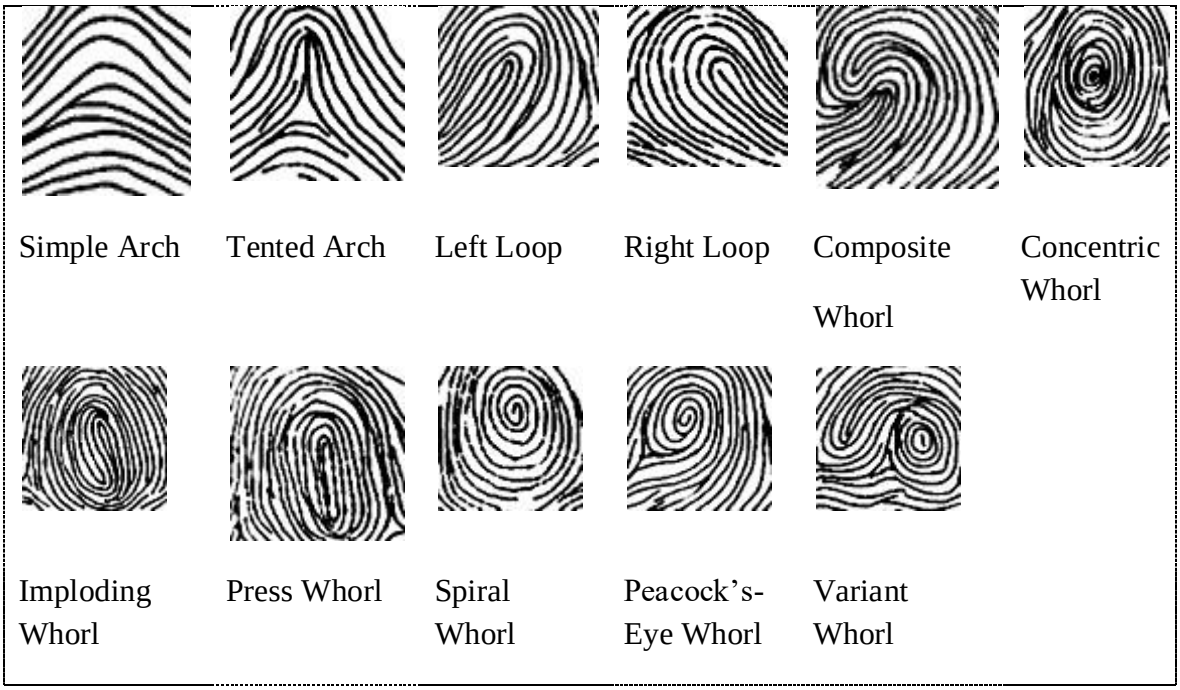



**Figure 1.10:** Examples of Level 1 Features
(Source: http://dermatoglyphics.org)

Only level 1 feature is not enough to uniquely identify the fingerprint image, whereas level 1 feature is used for classification or image enhancement purpose. Some examples for the level 1 feature are simple arch, tented arch, left the loop, right loop, composite whorl, concentric whorl, Imploding Whorl, press whorl, spiral whorl, peacock's- eye whorl, and variant whorl are shown in figure 1.10.

### 1.4. 2 Level 2 Features (Minutiae Based Features)

The evaluation of fingerprints for matching process requires the comparison of several capabilities of the print sample (Pathak, 2010) which consists of patterns that are meticulous exclusive capabilities determined within the fingerprint. A fingerprint has numerous features,

which might be island (a line that runs or flows by itself without touching different strains or regions), dot (an unbiased ridge which looks like a dot and same in duration and width), bridge or crossover (a small ridge which connects parallel ridges), core (center of the fingerprint pattern) and delta (a point from which fingerprint pattern alters or deviates). The exclusive features of a ridge, from which one-of-a-kind pattern occurs, are known as minutiae. Ridge ending or finishing and ridge bifurcation are the two styles of minutiae. A ridge ending is nothing however wherein ridge terminates or discontinue. Ridge bifurcation is a characteristic wherein a ridge splits or diverges, like a fork. From ridge ending and bifurcation, we can outline numerous different functions. The lake or enclosure is a characteristic of this ridge diverges and soon converges and turns into the single ridge. Spur is yet every other function wherein quick ridge branching off a protracted ridge. Still, some other functions like line unit, line fragment, eye, and hook additionally can be extracted and studied, which might be referred as fingerprint low-stage functions. The low-level functions are shown in figure 1.11.


**Figure 1.11:** Low- level Features of Fingerprint image
(Source: http://images.google.com)

Level 2 features display various ways ridge points may be abnormal. Minutiae are most reliable functions, which can be everlasting and unique for each individual except and until some wound or permanent harm happens. The number of minutiae factors collected ought to be extra to get excessive performance. Examples of Level 2 feature are shown in figure 1.12. In this research work Ridge ending and ridge bifurcation or simply Minutiae features or points are used for feature extraction.


**Figure 1.12:** Examples of Level 2 features of fingerprint
(Source: http://images.google.com; Krishna Prasad, K., & Aithal, P. S., 2017a)

### 1.4. 3 Level 3 Features

Level 3 functions are commonly considered as excellent ridge details and include all dimensional attributes of a ridge, along with ridge path divergence, breadth, outline, pores shape, edge outline, just beginning ridges, breaks, creases, scars and other permanent information (Mieloch et al., 2008). Out of the various fingerprint traits, pores and ridge contours are often used level 3 features. Ridge contours also incorporate precious level 3 traits and consist of ridge width and part shape. The shapes and relative role of ridge edges are considered as everlasting and precise. Examples of level 3 feature are shown in figure 1.13.


**Figure 1.13:** Examples of Level 3 Features
(Source: http://images.google.com)

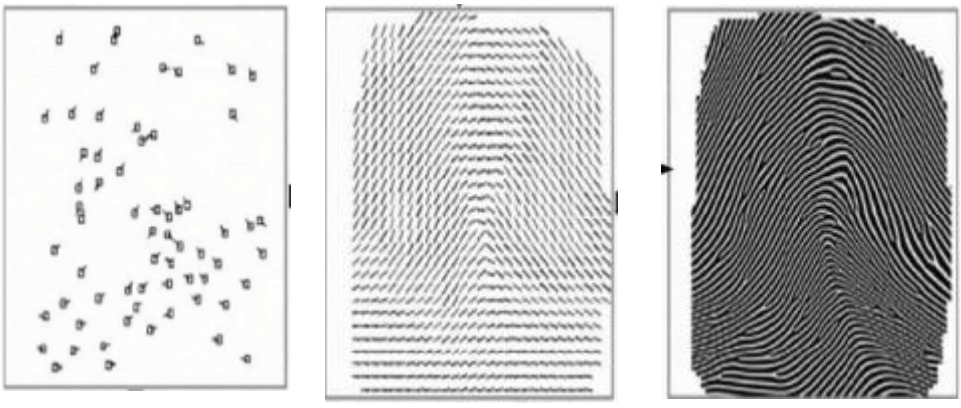
## 1.5 FINGERPRINT TEMPLATE AND PROTECTION

In biometrics, a fingerprint template is a term used to describe a saved document in a fingerprint scanning machine. When a fingerprint is entered into the gadget or sensing or capturing device, only a template of the fingerprint is stored, not an entire image of the fingerprint. A fingerprint template is smaller than the actual fingerprint picture and using the template as opposed to a picture makes for faster processing time. Usually, the fingerprint image is obtained by filtering and preprocessing process. Especially, protecting the fingerprint templates has been a hard hassle due to massive intra-user variations (e.g., rotation, translation, nonlinear deformation, and partial prints). There are two fundamental

challenges in any fingerprint template security scheme (Jain et al., 2013). First, we need to pick the ideal representation scheme that captures a maximum of the biased or discriminatory data's or features but is sufficiently invariant to changes at the time of finger capturing or enrollment process and can be effectively protected or secured with the aid of already available template protection algorithms. Secondly, we need to automatically align or sign in the fingerprints acquired at some stage in enrollment and matching without using any information that might reveal the features, which uniquely signify a fingerprint. The biometric machine can be compromised in many ways. One of the doubtlessly detrimental attacks is the leakage of biometric template statistics. The compromise of this template leads to unauthorized access to data by different people and ends up with nonrecoverable and huge loss of private information. The threat mainly occurs due to following two reasons;

Intrusion Attack: If an intruder accesses the secured fingerprint recognition system's database or template illegally, then intruder can easily reconstruct the original image from the template details. Using reverse engineering from the minutiae details fingerprint image can be reconstructed (Ross et al., 2007; Feng, J., & Jain, A. K. 2009, June; Cappelli et al., 2009). The figure 1.14 shows how fingerprint image can be reconstructed using reverse engineering process from minutiae details.

Function creep: An intruder can make use of the biometric template features for unintended functions (e.g., secretly follow a person throughout diverse applications by matching the templates from the associated databases), compromising the privacy of the person.



Minutiae Orientation filed Fingerprint

**Figure 1.14:** Reconstruction of fingerprint image from the minutiae template (Source: Feng, J., & Jain, A. K. 2009)

A fingerprint template protection schema should focus on following aspects while constructing stringent system (Jin et al., 2006).

*Diversity:* The secured template should not permit matching diverse applications, which allows protecting user private information.

*Revocability:* A new protected template can be regenerated and issued to user instantaneously when it is compromised.

*Noninvertible:* Using reverse engineering or anyway an intruder should not able to get original image from the template image. The intruder will use many strategies or different computational methods, but practically it should become impossible to retrieve original features.

*Performance:* The fingerprint recognition system should able to show good performance in terms of False Acceptance Rate or False Rejection Rate.

## 1.6 STUDIES ON FINGERPRINT SENSING METHODS

Automatic Fingerprint Identification System requires fingerprint image in particular format. Usually, it cannot accept and process the photographic image or image taken from digital camera or mobile camera. There are many unique acquisitions or sensing techniques to gain the fingerprint ridge and valley shape of finger skin or fingerprint (Xia and O'gorman, 2003). Traditionally, in many legal applications fingerprints had been specially obtained offline. Fingerprint acquisition can be mainly categorized into two groups as an offline and live scan. An offline acquisition method gets input through the process of ink spraying on a fingertip and tranferring it into on paper and then digitized with the aid of the paper with an optical scanner or video digital camera. The live acquisition is obtained through the sensor that is having the ability to directly digitize the sensing tip of the finger. As the fingerprint sensing, image processing, signal processing, and communication technology advance more and more new technologies are arriving at the leading edge.

Now, most business-related and forensic related applications or programs directly makes use of live dynamic digital fingerprints acquired by directly sensing the finger surface with a fingerprint sensor using optical, solid-state, ultrasonic, and other fingerprint image acquiring or sensing methods (Krishna Prasad, K., & Aithal, P. S., 2017b). Fingerprint sensors are available numerous sizes and styles but generally fall into two classes; region experiment (or contact) sensor and swipe sensor. With a touch sensor, the user places and holds the finger on

the sensor surface and impact transferred from the pad of the final joint of finger or thumb. Touch sensors are used typically in constant systems because of their size and form (Memon et al., 2008). Usually, touch sensors are square in shape and occupy more space and also weighs more; used in passport or immigration based applications. In swipe sensor, the user glides a finger vertically over the surface. The size and shape of the swipe sensors make it suitable for portable electronic gadgets like laptop computers and mobile phones (Galley et al., 2007; Memon et al., 2008). However, swipe sensor technology intrinsically restricts their appropriateness for a few programs. These sensors require customer education and practice to work consistently and they frequently fail to capture the fingerprint image. However, in each type of sensors, there are some common problems exist, like direct exposure to the surroundings, damage from mechanical results, electrostatic discharge (ESD), thermal surprise, discrimination between liveness and spoof.

### 1.6.1 Fingerprint Acquisition Methods

This section narrates different fingerprint acquisition method, which acts as an input or raw image for Automatic Fingerprint Identification System.

Optical: Optical fingerprint scanners are the oldest technique for capturing and evaluating fingerprints. This technique mainly depends on capturing an optical picture, basically a picture, and the use of algorithms to come across unique patterns on the surface, which include a ridge. Optical sensor comprises of the specialized digital camera, touch surface, the light-emitting phosphor layer, and solid state pixels. The specialized digital camera is used to acquire an image of the fingerprint ridge and valley pattern. A digital camera is located on the sensor and it captures the digital image using visible light. The touch surface is nothing but where the finger is kept, which is situated in the top layer of the sensor. Under the touch surface, where the user keeps his finger is phosphor layer, which emits light. The light emitted from the finger reaches to an array of solid state pixels with the aid of phosphor layer. Wound, scratch and dirty finger will cause a negative effect on the quality of the acquired image. The flaw encountered in this type of sensor is that user finger or skin requires high quality, dry or weather conditions can cause user finger unrecognized.

The disadvantage of this kind of sensor is the reality that the imaging abilities are suffering from the high-quality of skin on the finger. This sensor has a capacity of acquiring only two-dimensional images, synthetic or good quality image can be used to fool this acquisition

device. Live finger detector mechanism should fuse along with this technology to attain more security.

Ultrasonic: Ultrasonic sensor works on the theory of medical ultrasonography with an intention to develop a visual image of the fingerprint. An ultrasonic sensor utilizes sound waves which are having characteristics of high frequency with an intention to enter the inner or layer of the skin. The sound waves are generated with the aid of piezoelectric transducers and also in order to measure reflected energy piezoelectric transducers are used. Image of the fingerprint can be generated by the reflected wave measurement due to reason that dermal skin layers show same features of the fingerprint. Due to this fact even though the skin is damaged and dirty it will exhibit same features of the fingerprint or which will not affect the quality of the input image (Meghdadi and Jalilzadeh 2005, October).

Capacitance: Capacitance sensor utilizes the technology of capacitance to shape fingerprint image. To generate ride and valley structure of the fingerprint capacitance sensor uses electric current. Capacitance sensor comprises a tiny array of cells with one or more semiconductor chips (Setlak, 2005). Every cell includes two conductor plates with parallel plate capacitor and dermal layer and epidermal acts as a dielectric, which is a nonconductor.

Passive Capacitance: This sensor having slight variations from capacitance sensor, in which on the dermal layer of the skin fingerprint image are formed. At every point of the array, the capacitance is measured with the help of sensor pixels. An air gap bridges the volume between the dermal layer and sensing element in valleys, which creates capacitance variance in ridge and valley structure of fingerprint. Two values are already known, which are a dielectric constant of the epidermis and area of the sensing element. Ridge and valley of the fingerprint are differentiated with the help of measured capacitance value (Setlak, 2005).

Active Capacitance: In this type of sensor, initially before measurement of the fingerprint takes place, a voltage is applied to the skin with the help of charging cycle. Effective capacitor charges as an application of voltage. The blueprint of the fingerprint ridge is identified at in the dermal skin through the electric field between finger and sensor. A reference voltage is maintained in discharge cycle in order to calculate the capacitance, by the cross-comparing voltage across the dermal layer and sensing element. Later to form the image of the fingerprint the distance values are mathematically calculated. Like the ultrasonic sensor ridge pattern of the dermal layer are taken into considerations for measurement purpose. So this process overcomes the need for a clean surface and undamaged epidermal

skin of the fingerprint (Setlak, 2005). Table 1.2 shows assessment of optical and nonoptical sensors.

**Table 1.2:** Comparison of optical and nonoptical sensors

| | **Optical** | **Nonoptical** |
|---|---|---|
| Measurements | Light | Pressure, Heat, Capacitance and Ultrasonic wave. |
| Advantages | Specially-strong performance, Physical or electrical durability, Excellent image | Mass production leads to low cost. Compact and low size makes it appropriate in low power applications like mobile phone or laptop computers. |
| Benefits | Oldest and well-known method, Good technology support, Applications in the area of Attendance control, entry control, banking service etc. | Positive competition leads to mass production, which in turn leads to cost reduction. Similar to optical can be used for various applications. |
| Constraints | Difficult to build spoof free or highly secured system | Complex structure, Lack of technical knowledge leads to capture false points of fingerprint. |
| Disadvantages | Reduction in size of the image is too costly, Relatively easy to compromise the security | Performance variations with respect to outer changes in temperature and dryness of a finger |

## 1. 7. MATCHING ALGORITHMS

Fingerprint matching algorithms are used to compare formerly or already stored template of the fingerprints with a reference or sample fingerprint for authentication purpose. For this purpose, either original or initial image should be directly compared with reference fingerprint image or certain features of the fingerprint are extracted and compared. Feature extraction is the just earlier step or process of matching in automatic fingerprint identification system (Subhra & Venkata, 2008). In fingerprint recognition system, there exist two types of matching algorithms one is minutiae based algorithm and another one is non-minutia or pattern based algorithm. Majorities of the research work carried out are based on minutiae points or ridge ending and bifurcations or some low level details of minutiae, these minutia e details are extracted from both sample and template image and are compared and evaluated for better scores.

Pattern-based algorithm focuses on fingerprint primary patterns like Whorl pattern, Arch pattern, and Loop pattern. These patterns are part of Level1 features between a previously

stored template and a candidate or sample fingerprint image. Here alignment of ridge pattern in same orientation is a necessary condition. In order to achieve this central point or core point of the fingerprint pattern is identified and centered on that. Usually, in the pattern based algorithm the type, size, and orientation of the fingerprint pattern will be seeded in the template. The sample fingerprint image is graphically compared with reference image or template using attributes like size, orientation, and type to find the better matching score. The concept of machine learning and neural network are efficiently used in order to learn or train the various features of the enrolled fingerprint. This trained information can be used by the system later to make better decisions for authentication processes or matching process.

**Table 1.3:** Tabular comparison of Fingerprint image Minutiae and Pattern based Matching

| **Minutiae Based Matching** | **Pattern Based Matching** |
|---|---|
| Commonly uses features like Ridge ending, Bifurcation, Hook, Dot, Enclosure, Delta, bridge, Ridge Crossing | simple arch, tented arch, left loop, right loop, composite whorl, concentric whorl, Imploding Whorl, press whorl, spiral whorl, peacock's- eye whorl, and variant whorl |
| Makes use of local features | Makes use of both local and global features. |

## 1.8 PERFORMANCE MATRICES OF FINGERPRINT BIOMETRIC SYSTEM

Every new biometric algorithm has to be tested in order to know efficiency in differentiating decision between authenticated person and imposter. Before implementing the algorithm or new approach in real-time applications, we need to evaluate its performance using different factors (Ross et al., 2006). The performance factors vary from algorithms to algorithm. But the most common or general matrices used to quantify the fingerprint biometric system are;

- False Match Rate (FMR)
- False Non-Match Rate (FNMR)
- Receiver Operating Characteristic (ROC)
- Equal Error Rate (EER)
- Failure to Enroll Rate (FTER)
- Failure to Capture Rate (FTCR)

### False Match Rate (FMR) or False Acceptance Rate (FAR)

FAR is the likelihood of the Automatic Fingerprint Identification System incorrectly suits the input pattern to a non-matching template inside the database. It measures the percentage of

invalid inputs, which might be incorrectly classified. In case of similarity scale, if the individual is an imposter in fact, but the matching score is higher than the threshold, then he/she is treated as authentic. This way it increases the FAR rate and threshold value plays a crucial role in FAR rate. An FMR of 0.001% indicates that on an average of one lakh (100000) fraud or imposter attack one will get access to the system.

**False Rejection Rate (FRR) or False Non-Match Rate (FNMR)**

FRR is the probability that the fingerprint biometric framework unable to identify a match between the authentic person and a coordinating template in the database. An estimation of the percent of substantial valid information sources or valid users are erroneously dismissed, is assessed by this parameter. A 100% FNMR depicts that by and large, 1 in every 100 authentic users is not able to get permission to access the system.

**Receiver Operating Characteristic (ROC)**

The ROC plot is a visual representation of the exchange off between the FAR and the FRR. Normally all matching algorithm makes a decision based on the threshold value. Threshold value indicates how close the difference in score value of the template and sample should be. This threshold sometimes called as sensitivity. When threshold reduces FNMR also reduces but FAR may increase. On the other hand when threshold increases FAR decrease but FRR increases.

**Equal Error Rate (EER)**

EER is the ratio at which both acceptance and rejection mistakes are identical. The value of the EER can be easily generated from the ROC curve. The ERR is a short way to compare the accuracy of the system with exceptional or different ROC curves. An ideal system considers a system with very lowest EER rate.

**Failure to Enroll Rate (FTER)**

FTER is the unsuccessful attempt made to enroll in database or template of an Automatic Fingerprint Identification System by the input. FTER occurs due to low quality or substandard input.

**Failure to Capture Rate (FTCR)**

Inside programmed frameworks or Automatic system, the likelihood that the system neglects or unable to distinguish a biometric input when introduced accurately is referred as Failure to Capture Rate.

**Speed or Response Time**

The speed refers the time taken by the system to enroll as well as authenticate or reject. In technology term, this can be referred as execution time or time utilized by the new algorithm or model in to enroll and match.

## 1.9 DIFFERENT TECHNIQUES USED IN AUTHENTICATION PROCESS

By definition, authentication is using one or multiple mechanisms to show that you are who you claim to be. As soon as the identity of the human or machine is demonstrated, then human or machine is authorized to grant some services. Three worlds wide referred authentication process is as follows

- Token supported authentication
- Biometric supported authentication
- Knowledge supported authentication

Token supported authentication makes use of key cards, bank cards, and smart cards. Token supported authentication system sometimes uses knowledge supported techniques to improve security.

Biometric supported authentication strategies, together with fingerprints, iris scan and facial reputation aren't yet extensively adopted. The essential flaws of this technique are that such systems can be costly, and the identification process may be slow and regularly unreliable. However, this form of technique presents the highest level of protection.

Knowledge supported authentication is most commonly and widely used authentication technique and encompass both text-based and image-based passwords. The image-based techniques can be further subdivided into two classes: recognition-primarily based and recall based graphical techniques. The use of recognition based strategies, a person is provided with a set of images and the user is authenticated through recognizing and identifying the images, which is registered at the time of registration process. In recall based techniques it's essential that user has to reproduce something like a pattern, which is created or drawn at the time of registration process. The two methods of generating One Time Password are Time-Sychronized OTP and Counter-sychronized OTP.

*Time-synchronized OTP:* In time-synchronized OTPs the person has to enter the password within a time frame or within a stipulated time, in other words, OTP having lifespan only for few amount of time after that time it will get expired and another OTP will be generated.

*Counter-synchronized OTP:* In Counter-synchronized OTP, instead of regenerating OTP after the stipulated time, a counter variable is coordinated or synchronized between client device and server.

## 1.10 PROBLEM SPECIFICATION AND MOTIVATION

In this Twenty-first century, especially last four to five years mobile communication technology has undergone drastic changes due to the invention of fast and ubiquitous services and wireless technologies. But still, the mobile system faces, security and authentication challenges. There are wide technology or mechanisms are available in the literature for wireless and mobile devices or internet based applications with the aid of password, one-time password (OTP), and smart cards to provide network and device security or authentication. But these traditional security mechanisms face a lot of shortfalls. Some of the problems of these security systems are as follows.

- Traditional or conventional authentication mechanisms are not always reliable in all circumstances.
- Majority of the template protection strategies unable to accomplish all of the template protection requirements like revocability, protection, privateness and high matching accuracy.
- Drawing shape or pattern on the screen also easily observable or identifiable to imposter using special spy cameras.

A template is a compact representation of the raw input fingerprint image that is usually stored in a database. If the template stored in the database is hacked by the intruder then easily reconstruct original image through physical spoof samples and can get access to diverse applications (Adler 2004, Ross et al., 2007; Feng & Jain, 2009). The stolen template can be used for a variety of applications like unauthorized access to bank details or transactions or illegal access to heath-related information or unauthorized access to intelligence information.

One of the dangerous and vital attacks in the biometric system is an attack towards the biometric templates. Attacks at the templates can cause grave vulnerabilities where a template may be restored with the aid of fraudulent template to gain unlawful access entry to, or a physical spoof may be long-established from the template to obtain unethical access to the system or framework (Alder, 2004; Cappelli et al., 2007). Hence there is a great need and

necessity that biometric data should not be stored in plain text in the database and many foolproof method and technologies are adopted such that not the security of the application but also user privacy and integrity should be maintained or not compromised at any circumstances by the imposter.

Today numerous biometric innovations, for example, fingerprint, face recognition, iris, voice print and hand-based biometrics attributes (palm print or unique finger impression) can be utilized to recognize people.

As mentioned in advance, fingerprint identification technology era has various blessings like imparting excessive protection, much less price and non-invasive manner of acquisition and therefore is one of the maxima frequently used mechanisms. In this research work fingerprint's high individualism and permanent nature motivated us to choose this biometric feature as identity key, which is not fully secured and can be made fully secured by combining with passwords or OTP.

Fingerprint image filtering or pre-processing is one of the crucial factors in deciding or maintaining the quality and efficiency of the Automatic Fingerprint Identification System. Preprocessing involves filtering, segmentation, binarization and thinning or skeleton creation.

Fingerprint segmentation refers to the process of separating the image into two distinct regions as the foreground and background. The foreground is also called as Region of Interest (ROI) because only the region which contains ridge and valley structure is used for processing, while the background contains noisy and irrelevant content and that will be discarded in later enhancement or orientation or classification process. The image has to be converted into binary before extracting features. In order to extract low-quality features or level 2 and level 3 features image has to convert into more specific form is called as skeleton process or thinning.

There are great necessity and requirement for filtering and pre-processing, robust technique otherwise false minutiae are extracted and that leads to incorrect matching and increase in false acceptance rate. So robust pre-processing is especially important for the Latent and partial fingerprint. Template protection is another high demanding requirement for biometric applications in Mobile applications and all other secured applications.

Fingerprint unique Hash code and template protection are motivating force for this research Study. Fingerprint hashing is the new technique which combines biometrics and cryptography. The goal is to perform identification based on fingerprint simultaneously

hiding or keeping the fingerprint information secretly or noninvertible way. Even though fingerprint template is compromised intruder should not get original features of the fingerprint image.

The modern study of fingerprint technology reveals that fingerprint is not so secured like secured passwords which consist of alphanumeric characters, number and special characters. Fingerprints are left at crime places, on materials or at the door which is usually class of latent fingerprints. We cannot keep fingerprint as secure like rigid passwords. Using some modern technology with copper and graphite spray it's easy to mimic fingerprint image. Fingerprints are not fully secret if passwords are leaked or hacked, it easily revocable using another password. But in a biometric security system, which uses only biometric features, is not easy to change fingerprint key or fingerprint are static biometric, which never change much throughout the lifespan. Fingerprints are left at car, door or anyplace where every person goes and places his finger (https://security.stackexchange.com/questions/42384/is-there-any-way-to-cryptographically-hash-a-human-thumbprint).

Fingerprint Hash code is not used for full security or authentication purpose but it can be combined with other security elements like password or OTP in order to enhance security. Fingerprint Hash code acts as a key, which can uniquely identify every person. So it can be replaceable with user-id or username and can work along with text-based or picture based or pattern based passwords. The fingerprint hash code is not constant with biometric sensors or reader (https://hackaday.com/2015/11/10/your-unhashable-fingerprints-secure-nothing/). There are many types of research are carried out translation and rotation invariant fingerprint hash code generation but even small or pixel changes cause a difference in Hash code. So this research does not concentrate on developing fingerprint hash code which is translation and rotation invariant. Keeping all these advantages and flaws of fingerprint biometrics, this study makes use of fingerprint Hash code as a unique key for human identification and can be combined with Password and OTP for authentication or Security purpose.

### 1.11 AN IDEAL AUTHENTICATION SYSTEM

It is well known that we can improve the performance of any system by comparing it with a hypothetical, predicted system of that kind called Ideal system, which is explained by Aithal, P. S., and Aithal, S., (2015), Aithal, P. S., (2015, March), Aithal, P. S. (2015, July), Aithal, P. S. & Aithal, S. (2015, March), and Aithal, S. (2014). The word Ideal system refers to the

system which has utmost characteristics, which cannot be improved further. It is what our mind tells ultimately and which reached the pinnacle of success in the respective field, which can be compared to all other systems of similar type, which lacks in some qualities, explained by Aithal, P. S. (2016a), Aithal, P. S. (2016b), Sridhar Acharya P. and Aithal P. S. (2016), Aithal, S., & Kumar, S. (2016), Aithal P. S. (2016c). The less-efficient system can be converted into the ideal system with the aid of research and continuous innovation in that field. Many objects we can consider as ideals like an ideal gas, ideal fluid, ideal engine, ideal switch, ideal voltage source, ideal current source, ideal semiconductor and ideal communication technology and all of these are considered as standards to improve the quality and performance of similar type, which is explained by Krishna Prasad, K., & Aithal, P. S. (2017c).

**Table 1.4:** List of Ideal components with respect to Authentication System

| Sr. No | Ideal System Components | Definition of Ideal Systems/Components |
|---|---|---|
| 1 | Ideal Speed | The time taken by the Automatic Verification or Authentication System to authenticate the registered user will be very minumum or zero. |
| 2 | Ideal Data Transfer Rate | Any amount of data can be transferred from source to destination without any delay or with in null unit of time duration (In client Server Model) |
| 3 | Ideal Signalling efficiency | The quality of signal is 100% efficient in all aspects. |
| 4 | Ideal Security | 100% protection of Registered user means no intruder can able to break the system anyway. |
| 5 | Ideal Availability | Service can be available any part of the world anytime. |
| 6 | Ideal Bandwidth | The volume of Information per unit of time that a system can handle is unlimited or uncountable. |
| 7 | Ideal False Acceptance Rate | The percentage of system incorrectly classifies the input pattern to an unregistered user is zero. |
| 8 | Ideal False Rejection Rate | The probability that the Authentication framework unable to identify a match between the authentic people is always zero. |
| 9 | Ideal Equal Error Rate | Acceptance and rejection mistakes are identical in the system and which is equal to zero. |
| 10 | Ideal Failure to Enroll Rate | The unsuccessful attempt made to enroll in database or template of an Automatic Fingerprint Identification System by the input is zero. |
| 11 | Ideal Accuracy Rate | Because of False Rejection Rate and False Acceptance Rate is zero, the accuracy of the system becomes high. |

The ideal system of any kind can be placed in mind, while improving the characteristics of practical devices/ systems and reach ideal system or considered to be a pinnacle of success. Some of the ideal systems with respect to Authentication System are listed in Table 1.4.

Ideal Authentication System is a system which has properties like highly user-friendly, ubiquitous services, always available, very cheaper and 100% efficient in all aspects. An ideal or error-free biometric system should make an accurate and correct decision on every test sample regardless of any performance degrading factors like variation or differences in inter-class, similarities in intra-class, different representation for enrolled and sample data, and extreme noise and low sample data quality. As shown in Figure 1.15, we have proposed an Ideal Authentication Model, which consists of different components like Ideal Security, Ideal User-friendly, Ideal Input, Ideal Process, and Ideal Performance Evaluation Matrices.

### 1.11.1 Ideal Security

In Ideal Authentication System, Ideal Security refers a system, which is impossible for an intruder to break the system or impossible for the unregistered user to access the system. Ideal Security model improves or makes the system robust by maintaining security mechanism at various levels like user level, network level, template or database level.

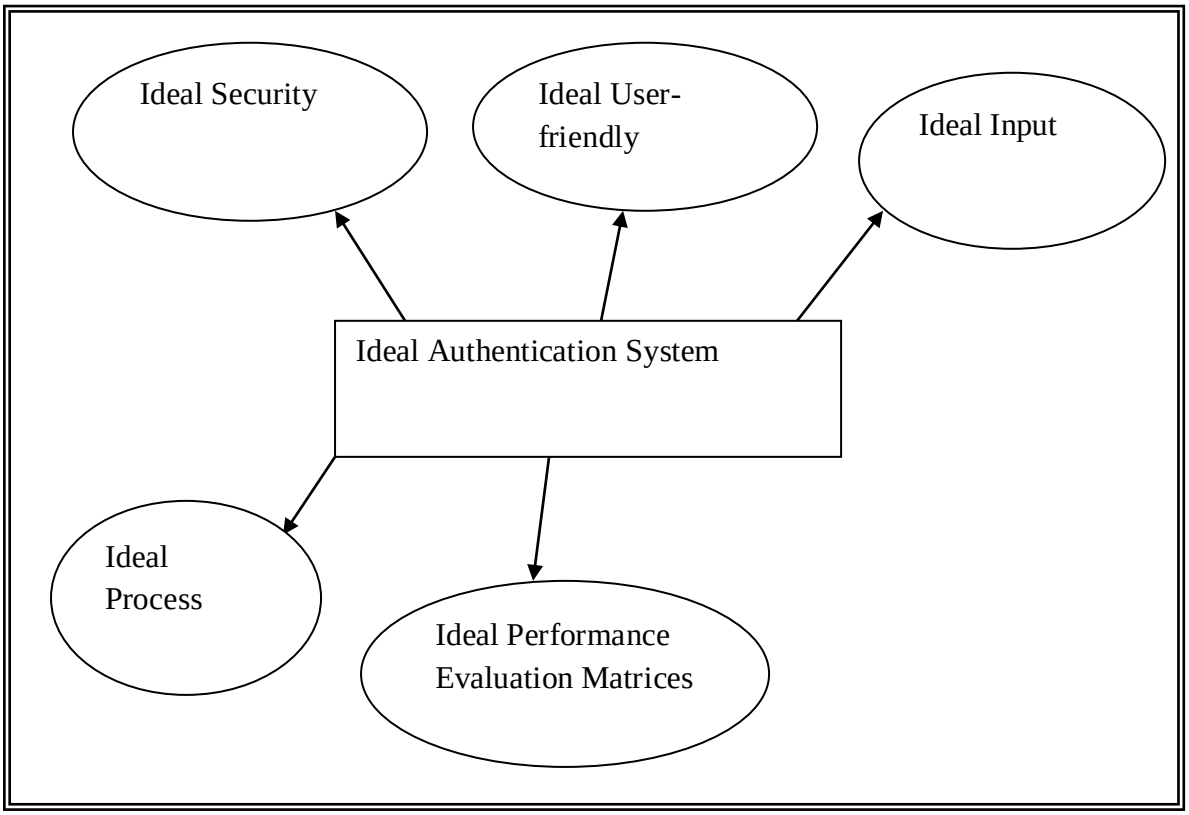



**Figure 1.15:** Ideal Authentication System Model

Security can be enhanced to maximum or optimal level by the use of multifactor authentication model. Table 1.5 shows Ideal security various component's technologies and benefits.

**Table 1.5:** Description of various characteristics of Ideal Security

| Sr. No | Characteristics | Benefits |
|---|---|---|
| 1 | High User level Security | Minimum data is remembered by the user for the authentication process. To realize this use Physiological or Behavioral biometrics |
| 2 | High Network level Security | Difficult to get original data or information.<br>Decrypting of the message by the unknown user becomes impossible. |
| 3 | Ideal Template level or Database level security | Nonrevertible template or impossible to get actual information. |
| 4 | Multifactor Authentication Security | Use more than one factor for authentication like Biometrics, One Time Password (OTP), and Password. |

### 1.11.2 Ideal User-friendly

The goal of the Ideal User-friendly component is that user should able to get access to the system effortless or easily without remembering anything or very minimum amount of data. Ideal user-friendly system should have some characteristics, which are listed in Table 1.6 to call itself as Ideal.

**Table 1.6:** Description of various characteristics of Ideal User-friendly

| Sr. No | Characteristics | Description |
|---|---|---|
| 1 | High Response Time | User should get Authenticated as early as possible or with least amount of time |
| 2 | High Access Time | User should get access to the system with least amount of time |
| 3 | Automatic Process | User should able to get authenticated automatically without entering anything on the screen or just by standing in front of the system |
| 4 | High speed | The execution time for authentication should be very minimum |
| 5 | High Availability | Anytime, Anywhere, Anyplace or simply ubiquitously available |
| 6 | Effort free | User should able to work with the system effortless or freely. |

### 1.11.3 Ideal Input

Ideal Input ensures that registered user should able to get access to the system or authenticated with very less or no input. In an Ideal Authentication system, the Ideal input having different characteristics, which are listed out in Table 1.7.

**Table 1.7:** Description of various characteristics of Ideal Input **[**Source: Aithal, P. S. & Pai T, Vaikunta]

| Sr. No | Characteristics | Description |
|---|---|---|
| 1 | Minimum possessions | Users will be carrying only one data or no data along with them to get authenticated |
| 2 | Least input | The number of data or instruction to the system is as least as possible |
| 3 | Input Selectivity | Select input data rather than remembering and entering |
| 4 | Ubiquitous Data | Any time, Anywhere, and Anyplace able to input or feed data |
| 5 | Reliability | The input should not have any imperfections. It should not fail during execution |
| 6 | Usability | The input should have infinite usability for various applications. |
| 7 | Efficiency | The provided input should have 100% efficiency with an intention to get accurate results. |
| 8 | Input Security | The input should be protected from intruder |
| 9 | Short execution time | The input provided to the system should execute with a minimum amount of time |

### 1.11.4 Ideal Process

In an Ideal Authentication system, Ideal process refers user should able to complete authentication process without any fault, fastly and completely. The different characteristics, of the Ideal process, are listed out in Table 1.8.

**Table 1.8:** Description of various characteristics of Ideal Process

| Sr. No | Characteristics | Description |
|---|---|---|
| 1 | High Atomicity | The Authentication process should complete fast without any errors or should not abort in between if it has started. |
| 2 | Ideal Consistency | After the authentication process system should end up with the consistent state. |
| 3 | Maximum Isolation | The intermediate state of Authentication process should be invisible to other users. |
| 4 | High Availability | Anytime, Anywhere, Anyplace or simply ubiquitously available |
| 5 | Effort free | Authentication process should be effortless. |
| 6 | High durability | After a transaction completes, the changes made should |

| | | |
|---|---|---|
| | | persist even in the case of unexpected system failure.<br>If user credentials like password or biometric are changed, it should persist, if that process completes just before the failure. |

### 1.11.5 Ideal Performance Evaluation Matrices

In Ideal Authentication System, Ideal Performance Evaluation Matrices refers all the performance evaluation matrices normally used for the authentication system. This component is having scope in the biometrics based authentication system. The different characteristics, of Ideal Performance Evaluation Matrices, are listed out in Table 1.9.

**Table 1.9: Description of various characteristics of Ideal Performance Evaluation Matrices**

| Sr. No | Characteristics | Description |
|---|---|---|
| 1 | Ideal False Acceptance Rate | The percentage of system incorrectly classifies the input pattern to an unregistered user is zero. |
| 2 | Ideal False Rejection Rate | The probability that the Authentication framework unable to identify a match between the authentic people is always zero. |
| 3 | Ideal Equal Error Rate | Acceptance and rejection mistakes are identical in the system and which is equal to zero. |
| 4 | Ideal Failure to Enroll Rate | The unsuccessful attempt made to enroll in database or template of an Automatic Fingerprint Identification System by the input is zero. |
| 5 | Ideal Accuracy Rate | Because of False Rejection Rate and False Acceptance Rate is zero, the accuracy of the system becomes high. |
| 6 | Ideal Execution time | Automatic Verification or Authentication process should complete as early as possible for the registered user. |

## 1.12 ORGANIZATION OF THE THESIS

The **Chapter 1** is **Introduction to Biometrics & Fingerprint Recognition System**, which consists of elaborative introduction to Biometrics technology, Basic principles of fingerprint technology, Application areas of biometrics, Types of fingerprints, Fingerprint image preprocessing, Fingerprint features- Level 1, Level 2, and Level 3 features, Fingerprint matching algorithms, Template protection, Fingerprint acquisition methods, Performance matrices of fingerprint recognition, Multifactor Authentication, Problem specification, Motivation for the research and Ideal Authentication System. The proposed Ideal

Authentication Model consists of different components like Ideal Security, Ideal User-Friendly, Ideal Input, Ideal Process, and Ideal Performance Evaluation Matrices.

An extensive literature survey on Fingerprint biometric recognition is depicted in **Chapter 2** and is **Review of Literature**. This includes a review on Biometric security, Fingerprint recognition system-past to present, Fingerprint sensing technology, Fingerprint filtering, Fingerprint Enhancement techniques, segmentation techniques, Minutiae based recognition system, hash Functions, MD5 hash algorithm. This chapter also includes Research gap of the existing study.

**Chapter 3** is **Methodology and Fingerprint Image Preprocessing Techniques**, which explains the concept of research objectives, scope, methodologies and fingerprint image preprocessing techniques. Fingerprint image preprocessing techniques consists of Enhancement phase, Segmentation phase, and Skeletonisation phase. Here Segmentation, Filtering algorithm, and Skeletonisation process are discussed including its theory and pseudo-algorithm. In this Chapter Enhancement phase, Segmentation phase, and Skeletonisation phase output are also discussed by considering input from FVC ongoing 2002 benchmark dataset.

**Chapter 4** is **Fingerprint Feature Extraction and Hash Code Creation Phase**. The existing methods or algorithms theoretical aspects are discussed in detail. This covers Minutiae Identification and Extraction Phase, Hash Code creation Phase, and Hash Matching Phase. Workflow for each phase is discussed and flowcharts are drawn, if required. The Feature identification and Extraction consist of many sub phases-pre processing skeleton, minutiae identification, and Minutiae table formation, post-processing minutiae table, Final minutiae table formation and feature extraction in the form required for hash function. All these process theories are discussed in detail. If necessary, the workflow for all sub-phases and main phase is discussed and flowcharts are drawn and discussed. Here the necessary output of Skeletonisation and minutiae extraction are discussed by considering input as FVC ongoing 2002 benchmark dataset. This chapter also includes Hash code creation, Database, and hash matching. The theory related to hash code creation using MD5 hash algorithm is also discussed.

**Chapter 5** is **Performance Evaluation of Fingerprint Hash Code Generation Methods**. In this chapter, benchmark dataset and all six methods are discussed and analyzed. Input for the system will be FVC ongoing 2002 benchmark dataset. Here different performance matrices

like False Match Rate (FMR), False Non Match Rate (FNMR), Receiver Operating Characteristic (ROC), Equal Error Rate (EER), Failure to Enroll Rate (FTER), Failure to Capture Rate (FTCR) and elapsed time are discussed and analyzed. Time complexities of all the six methods are discussed and analyzed using asymptotic Big-Oh notation and the result is shown using the graphical image. A Multifactor Authentication Model is proposed based on combined Fingerprint hash code, Password, and OTP. This model is mainly focused on internet-based online transactions and mobile-based safe transactions. This method is not suitable for ATM machines and Ordinary attendance maintenance system which does not make use of client-server architecture.

**Chapter 6** is **Factors and Elemental Analysis of Multifactor Authentication Model through ABCD Framework.** This chapter discusses ABCD Framework. The new approach of Multifactor Authentication Model using Fingerprint Hash code, OTP and Password are analyzed using ABCD analysis framework. As per ABCD analysis various determinant issues related to Multifactor Authentication Model for Verification/Authentication purpose are (1) Security issues, (2) User-friendly issues, (3) Input issues, (4) Process issues, and (5) Performance Evaluation matrix issues. The new model is compared with already existing almost similar Multifactor Authentication systems.

**Chapter 7** is **Summary, Conclusion, Limitations and Future Scope**. This chapter lists out the summary, conclusion, limitations, and findings of this research work. The future research directions are also identified and discussed.

## 1.13 CHAPTER SUMMARY

In this chapter, all the introductory theories related to Biometric system, its principles, application, fingerprint technology, biometric template protection, fingerprint sensing technologies and Ideal Authentication System are discussed. The detailed theories and research contribution made by other researchers to the different phases mentioned in this research framework like image filtering, enhancement, segmentation, Skeletonisation, minutiae identification, extraction and hash functions and, OTP are discussed under the title Review of Literature in the next chapter.

**********

# CHAPTER TWO

# *Review of Literature*

**Contents** **Page No.**

## 2.1 INTRODUCTION

The drastic changes in mobile and wireless based technologies and increasing number of applications and users demanded high security concern, which leads to research on biometrics with a purpose to increase the security aspects and to minimize security threats. The current global security threat has prejudiced people and their administration to take some special actions and extra precaution in safety or security threats. The security or protection is important not only for the nation but also for individual persons, their property, surroundings, and belongings and for all assets. Due to this reason every now and then new advents are invented in biometrics with an ultimate aim of improving security. In biometrics, new technologies are introduced. But out of which fingerprint identification biometrics technique considered to be the most effective approach for utmost security authentication.

As industrial incentives boom, various new devices for user identification or verification are being highly developed, each with its very own benefits and constraints. Even though biometric systems are not so easily vulnerable to security threats but some intelligent intruder can compromise the system using the information of biometric templates. So it's essential and necessary to develop noninvertible, revocable and highly robust biometric templates. Advances in cryptographic and hashing techniques can be efficiently used to make the biometric system more secure and robust. In this chapter already conducted researches and some important theory related to the biometric system are discussed under the title as a review of the literature with special reference to fingerprint biometrics.

## 2.2 REVIEWS ON BIOMETRIC TECHNOLOGY AND SECURITY

The term biometrics is formed initially using two words as bio means life and metrics means to measure, which is taken from Greek language (Rood and Hornak, 2008). Automated biometric systems, which is processed and decided by the computer, have best turn out to be available over the previous decades due to drastic development in diverse applications and fields. Although Automated Biometric identification System is having only 50-75 years of history, the history of biometric systems is thousands of years back. The face is one of the simple examples of a biometric characteristic used for recognition. Since from the civilization, people have used faces to discover recognized and unknown (unfamiliar) people. This simple undertaking became more and more challenging as populations improved and as more convenient methods of journey delivered many new individuals into- as soon as small communities. The idea of human-to-human reputation is also visible in behavioral-most

important biometrics which includes a speaker and gains popularity. Individuals use those characteristics, truly unconsciously, to recognize acknowledged people on a day-to-day basis. The role of Egyptians and Chinese are very crucial in the history of biometrics system. Today, biometric face recognition, iris recognition, retina recognition and many more new biometrics technologies are used for the security purpose. This section gives a brief history of biometric security and fingerprint recognition.

The William Herschel hand printed on the back of each worker with an intention to make a differentiation between worker and employee. Late 1858 only the organized imprison of hand and fingerprint are used for identification and verification purpose and same is inspired by the William Herschel and made him develop handprint technology (Komarinski, 2004). At some stage later in 1870, Alphonse Bertillon generated a method to figure out individual persons based on précis information of their bodily descriptions and snapshots and are usually termed as bertillonage or anthropometrics and this has become outdated in 1903 for the reasons that some bodily measurements are not unique. In 1892, Sir Francis Galton proposed a new type of fingerprint biometrics based on the usage of minutiae characteristics and is used by many scientific and research communities even today. Later in 1896, Sir Edward Henry, contributed new principles or methods to the success of fingerprint popularity with the aid of Galton's theory to find out prisoners with the help of their fingerprint impressions. He adopted classification system that bifurcated plenty of fingerprints of mankind easily and also helped in searching the prisoners. He assisted and guided for the establishment of fingerprint bureau in the year 1986 and the new method got good popularity for crime detection all over the world.

In the beginning, the concept of the usage of iris styles or patterns for user identification was at the start proposed in 1936 by ophthalmologist Frank Burch (Iradian Technologies, 2017). In 1987 two other ophthalmologists, Aran Safir and Leonard Flom patented this concept, and in 1989 they requested John Daugman to try and create actual algorithms for iris popularity. But now, this technology is additionally being used in numerous different applications such as entry control system for high safety installations, credit score card usage verification, and employee identification (Medien & Burghardt, 2002). Woodrow w. Bledsoe used biometrics traits like eyes, ears, nostril, and mouth for human recognition at around 1960 and this was considered as the first step for the initial partial automatic and partial face recognition system. Gunnar Fan, a Swedish professor, produced a replica of speech recognition in around 1960

(Woodward et al., 2003). This invention has become the foundation of real automated speech recognition system at a later stage.

Initially, automatic signature verification system-a digital form of the signature having the ability to identify the person uniquely is developed by North American aviation at some point of 1965 (Mauceri, 1965). The investigation team of the federal bureau (FBI) used the same approach by changing a little bit to investigate the extensive man-hours invested for the purpose of analysis in 1969. In 1970 authentication system based on face recognition are just initiated. Goldstein et al. (1971) used 21 precise markers of human organs like hair coloration, the thickness of lip to computerize the recognition process. The main flaws of such a machine or system were that all those features have been not computed automatically and which are done manually.

In around 1970, Dr. Joseph Perkell introduced the speech recognition based on behavioral components of speech (Woodward et al, 2003). The year 1974 witnessed initial hand geometry framework for controlling some applications like entry control system, schedule and attendance management system and user identification system. The success of this first biometric automatic system, inspired the numerous investment businesses for the improvement of hand scanner and feature extraction technique-the unique features of the hand geometry (Ratha & Bolle, 2004), with an ultimate goal to improve or build an excellent human recognizer. The result of the above system influenced the initial model of speaker reputation system in 1976. In 1996, the hand geometry changed into applied correctly on the Olympic Games and the machine-implemented became capable of cope with the registration of over 65,000 human beings.

In the year 1988, the primary semi-automatic facial recognition system was developed by Lakewood-section of Loss Angele's country sheriffs department for finding out thief's or suspects. The facial recognition or identification system was further studied and analyzed by several series of discoveries by a panel of researchers, they are Sirovich and Kirby (1989), Turk and Pentland (1991), Philipis et al. (2000).

The capacity of the human ear for personal identity turned into diagnosed and encouraged as early as 1890 via the French criminologist Alphonse Bertillon. Bertillon made use of the outline and a few measurements of the ear as a part of the bertillonage system that changed into used to perceive recidivists. One of the first ear reputation systems is Iannarelli's system which becomes at first advanced in 1949 (Iannarelli 1989). This is a manual machine based on 12 measurements of the ear. Vertical, horizontal, diagonal, and anti-diagonal strains are

drawn from that center point to intersect, the internal and external curves on the exterior of the pinna. The 12 measurements are derived from these intersections and used to represent the ear. Fields et al. (1960) made an endeavor to recognize infant babies in hospitals. They visually measured 206 units of ear snapshots and concluded that the morphological fidelity of the ear can be used to set up the identity of the newborn.

Hand geometry is an authentication generation with a prolonged history of use. Historic paintings in Chauvet Cavern have been carbon dated to be 31,000 years vintage. A few say that the handprints left with those artworks are the artist's particular signature. The first industrial hand geometry scanner changed into the Identimat introduced via Identimation in the early 1970's. This device used a 1,000 watt light bulb to spark off mechanically scanned photocells for measuring the hand form. Within the mid-1960's Robert Miller of New Jersey became analyzing a navy clothing procurement report wherein he came upon the remark that hand sizes have been so various that they might be used to pick out people. This led this avid inventor to develop the primary automatic hand geometry identity device.

Of all of the biometric identity structures, DNA affords the most reliable form of identification. DNA is intrinsically digital and unchangeable during a human's existence or even after demise. DNA differs from other normal biometrics patterns in several aspects as DNA calls for a tangible bodily pattern rather than an impression, image, or recording. DNA matching isn't always carried out in actual-time, and presently now not all stages of contrast are automated. DNA matching does not rent templates or feature extraction but instead represents the contrast of actual samples.

The human genome incorporates only 20,000-25,000 genes (Collins et al., 2004; Lander et al., 2001; Venter et al., 2001). Consequently, most of the genome, approximately 75%, is extragenic. These regions are called junk or less emphasis DNA.

The research into keystroke dynamics as an authentication technique is predicated on growing a method that is sturdy, inexpensive, and has the capability to be obvious to the person. It was researched as early as 1975 (Spillane, 1975) and has been the concern of numerous patents (Brown, & Rogers, 1996; Garcia, 1996; Young, 1989). keystroke dynamics are not expected to be specific to every man or woman seeing that there are probably to be similarities among individuals' typing style, particularly on cellular gadgets, but it is recognized to be sufficiently one of a kind among users to be useful as a method of verifying a person's identification. Gafurov & Snekkenes (2009) studied gait behavior, which is gathered from the acceleration signals collected from sensors attached to the man or woman's

leg. This gait record is used to understand or recognize persons. It has been shown that impostors who know their closest man or woman in the database or the genders of the users can be a threat to gait primarily based authentication.

The succeeding level in fingerprint computerization happened at the give up of 1994 with the included Automatic Fingerprint Identification System (AFIS) competition. The competition found three principal challenges as (1) digital fingerprint possession (2) local ridge characteristic or feature extraction and (3) ridge characteristic prototype matching (David et al., 2005).

The primary Automatic Fingerprint Identification System (AFIS) changed into advanced through palm machine in 1993. For the duration of 1995, the irises biometric become formally launched as a business authentication device by way of defense nuclear corporation and iris scan. The year 2000 visualized face recognition dealer take a look at (FRVT 2000) subsidized by means of the US authorities organization and at the same year vascular pattern is initiated for recognition system (Im et al., 2001). In the around the year 2003, ICAO (International Civil Aviation Organization) used biometric identification/verification information into different travel document verification like passport and which is readable by a machine (MRTDs). In 2004, US started first statewide palm print database and in the same year, face recognition system also tried to improve the recognition difficulties. In 2005, iris biometric identification system just evolved and iris snapshot is collected from individuals taking walks through a portal.

In the year 1998 only, biometric system stepped into mobile applications but faced a lot of challenges and which resulted in significant adoption rates. Yıldırım, N., & Varol, A. (2015, May) explained the importance of fingerprint security and stages of their fingerprint web login authentication. They developed authentication application using fingerprint security feature for Samsung device. The proposed system consists of two stages of the framework, in 1st web service based authentication and 2nd stage is developed in the Android application side, which generates a random password. Authors used only the predefined fingerprint SDK for fingerprint registration and verification. They used the mobile IMEI number for secondary registration and verification for mobile. Moreover, this paper proposed two levels of authentication using finger and IMEI number, but here not exactly meet the function procedures of fingerprint recognition. It is still questionable lack of accuracy and complexity in authentication.

## 2.3 REVIEWS ON FINGERPRINT RECOGNITION SYSTEM

Fingerprint image and identification technology have been in life for hundreds of years. Archaeologists have exposed proof suggesting that interest in fingerprint dates to prehistory.

In Nova Scotia Petroglyphs-from the time of pre-historic native people, displaying a hand with exaggerated ridge patterns has been discovered. In historic Babylon and China, the fingerprint has been impressed on clay pills and seals. Using fingerprint is a completely unique human identifier dates returned to 2nd century B.C. China, where the identity of the sender of a critical report will be validated by way of his fingerprint influence within the wax seal. In fourteenth-century Persia fingerprints have been inspired by numerous professional papers. At that point, a governmental legitimate located that no fingerprints have been exactly alike (Malathi, 2012).

By means of the recently invented microscope, Professor Marcello Malpighi at the college of bologna cited ridges at the surface of palms in 1686. He defined them as loops and spirals, however, did no longer note their fee as a way of personal identification. Later, in 1823 professor John Evangelist Purkinje posted his thesis presenting a device type based on nine distinctive fingerprint patterns at Breslau University. This was the first step closer to the current study of fingerprints. Hermann Welcker an anthropologist of the college of Halle from German, analyzed friction of ridge pores and skin permanence-which is considered in the present study as features of fingerprints, by printing his private hand in 1856 and once more in 1897, then written and published a book in 1898.

The primary, modern, and current use of fingerprints happen in 1856 while Sir William Herschel, the leader magistrate from India, had a nearby businessman, Rajyadhar Konai; provoke his handprint at the back. Later, the right index and center palms were printed next to the signature on all contracts made with the locals. The reason was to frighten the signer of repudiating the agreement because the locals believed that non-public contact with the file made it greater binding. As his collection of fingerprint grew, Sir Herschel started out to realize that fingerprints could prove or disprove identification. No matter his lack of medical know-how in fingerprinting he turned into satisfied that fingerprints are unique and everlasting at some point of lifestyles.

In 1863 professor Paul-Jean Coulier, of Val-de-grace from Paris, published his observational study that fingerprints may be advanced on paper through iodine fuming, explaining the way to maintain (restore) such evolved impressions and mentioning the capability for figuring out suspects' fingerprints with the help of use of a expand or magnify glass. In modern fingerprint

recognition system, these types of fingerprints are called as Latent fingerprints. Adding more information to latent fingerprints, in 1877, American microscopist Thomas Taylor found that unknowingly left prints of finger or palm item might be used to resolve crimes.

The Alphonse Bertillon, a French anthropologist, devised the primary widely customary medical technique of biometric identification in 1870. The Bertillon machine, bertillonage, or anthropometry became not primarily based on fingerprinting however relied on a systematic mixture of bodily measurements. Bertillon's gadget included measurements inclusive of the head period, head width, duration of the middle finger, the left foot's period; and the forearm period from the elbow to the end of the center finger. Bertillon in 1888 changed into the made leader of the newly created branch of judicial identification where he utilized anthropometry as the good method of identity. He later added fingerprints image but demoted them to a less important function within the class of unique marks. Through grouping, the statistics of any single individual will be located into one in every of 243 distinct classes. For the next thirty years, bertillonage becomes the number one method of biometric identification (Malathi, 2012).

In the 1870s, Dr. Henry Faulds, health care provider-superintendent of Tsukiji sanatorium in Tokyo, Japan, who has received the examination of skin-furrows and after becoming aware of finger grades on a sample of prehistoric pottery. Dr. Faulds, now not most effective diagnosed the significance of fingerprints as a way of identity, however, devised a method of a class as well. In 1880, Faulds forwarded an evidence of his class machine and designed a pattern for recording inked impressions. Apart from that in the year 1880, Dr. Henry Faulds posted a piece of writing in the clinical magazine. He stated fingerprints as a way of personal identity and using printers ink as a technique for obtaining such fingerprints. He is likewise credited with the number one fingerprint identity of a greasy fingerprint left on an alcohol bottle. The method of classification proposed by way of Dr. Faulds is known as Henry type classification and is primarily based on patterns together with loops and whorls, which is still used nowadays to arrange fingerprint card files.

In 1882, Gilbert Thompson, worn his personal thumbprint on a file to assist prevent forgery, which is considered as the first identified application of fingerprints image in the U.S.A. Continuing the research contribution work of Dr. Faulds, Sir William Herschel and Sir Francis Galton set up the uniqueness and solidity of fingerprints. This e-book, fingerprints from 1892, includes the first fingerprint class gadget containing three fundamental sample types: loop, arch, and whorl. The system changed into based on the distribution of the sample

sorts on the ten fingers. The machine worked, but there was a necessity to be progressed with a type that changed into simpler to administer. Sir Galton diagnosed the traits used for user identification, the specific ridge traits called minutiae, which are frequently called "Galton's information".

In 1892, Juan Vecetich, an Argentine police respectable, made the first crook fingerprint identification. He became capable of identifying a female, who had assassinated her two sons and tried to suicide in an attempt to avoid blame. The bloody print remained on a doorpost, provided her identity for the assassin.

On 12 June 1897, an authority and committee in India approved a committee record that fingerprints ought to be used for the type of criminal statistics by a body headed by a governor. Later anthropometric bureaus situated in Kolkata of India have become the sector's first fingerprint bureau in the same year. Haque and Bose followed the Henry machine of fingerprint classification from India and became very successful. The Henry category device continues to be used in English-speaking international locations like England. Table 2.1 explains the summary of literature survey with Author name, Year and their findings/inventions/Results.

**Table 2.1:** Fingerprint recognition system Milestone from 1800-1899

| Sr. No | Authors | Year | Inventions/Findings/Results |
|---|---|---|---|
| 1 | Professor Marcello Malpighi | 1686 | Cited ridges at the surface of palms. |
| 2 | Professor John Evangelist Purkinje | 1823 | Analyzed nine distinctive fingerprint patterns. |
| 3 | Hermann Welcker | 1856 | Studied friction ridge pores and skin permanence. |
| 4 | Sir William Herschel | 1856 | That fingerprints could prove or disprove identification. |
| 5 | Professor Paul-Jean Coulier | 1863 | Fingerprints may be advanced on paper through iodine fuming, explaining the way to maintain (restore) such evolved impressions and mentioning the capability for figuring out suspects' fingerprints with external apparatus to view the image like magnifying capability glass. |
| 6 | Thomas Taylor | 1877 | Found that palm prints and fingerprints exist on any item might be used to resolve crimes. |
| 7 | Alphonse Bertillon | 1870 | Devised the primary widely customary medical technique of biometric identification. Bertillon's gadget included measurements inclusive of the head period, |

| | | | |
|---|---|---|---|
| | | | head width, duration of the middle finger, small portion of the left foot etc. |
| 8 | Dr. Henry Faulds | 1870 | Examined skin-furrows after become aware of finger grades on a sample of prehistoric pottery. Even though not effectively diagnosed the significance of fingerprints as a way of identity, but planed a method of a class as well. |
| 9 | Gilbert Thompson | 1882 | Used his personal thumbprint on a file to assist prevent forgery, which is considered as the first identified real application of fingerprints in the U.S.A region. |
| 10 | Juan Vecetich | 1892 | Made a real attempt for a crook or criminal fingerprint identification. |

### 2.3.1 Henry Classification era of Fingerprint Recognition

Throughout the 1890's, Sir Edward Richard Henry, a British reputable in Bengal believed that a fingerprinting system changed into the solution to his hassle of verifying the identity of criminals. He studied the works of Sir Galton and Sir Henry and proved that they might be used to produce 1,024 primary classifications, which was instituted in Bengal in 1897. The system is described in his e-book, which includes applications of fingerprint images. In June 1897, bertillonage was changed and the Henry type device became the official approach to figuring out criminals in British India. In 1903, the Henry category machines become used to distinguish prisoners who had been equal twins. The Bertillon machine changed into now not able to make out the difference between equal twins and therefore Henry type device turned into in addition strengthened (Malathi, 2012).

Juan Vucetich additionally Laboured on a category system based totally on the findings of Sir Galton and used in fingerprint forensics. His systems become posted in his e-book, named as Dactiloscopía Comparada (comparative fingerprinting) in 1904. His gadget, the Vucetich machine, continues to be utilized in maximum Spanish-speaking international locations.

Throughout the first 25 years of the 1900s, an increasing number of companies within the U.S. began to send copies of their fingerprint cards to the national bureau of criminal identity. These files fashioned the nucleus of the FBI fingerprint files even as the detection division of the FBI become hooked up to 1924. By 1946, the FBI had processed more than 100 million fingerprint cards in manually maintained documents. By 1971, this variety had elevated to two hundred million playing cards. The primary United States to adopt a national computerized form of fingerprint imaging turned into Australia in 1986, which applied fingerprint imaging era into its regulation enforcement gadget.

On the worldwide symposium on latent fingerprint detection and identification, performed by way of the Israeli countrywide police organization, at Neurim, Israel, June 1995, the Neurim declaration become issued. No clinical basis exists for requiring that a pre-determined minimum number of friction ridge functions need to be resent in two affects in order to set up a fantastic identity. The assertion has unanimously accredited all present, and later, signed through 28 individuals from the subsequent eleven nations: Australia, Canada, France, Holland, Hungary, Israel, New Zealand, Sweden, Switzerland, UK, and United States.

With the creation of AFIS era (Automatic Fingerprint Identification System), the documents have been breaking up into automatic crook documents and manually maintained civil documents. Many files had been found to be duplicated and the information truly represented somewhere between 25 and 30 million criminals and an unknown quantity of individuals within the civil documents.

In 2012 INTERPOL's Automatic Fingerprint Identity System repository exceeds one lakh and fifty thousand of fingerprints for vital international criminal statistics from one hundred ninety member countries. Over 170 international locations have 24 x 7 interface ability with INTERPOL expert fingerprint offerings.

The most important AFIS repository in America is operated via the Department of Homeland security's US visit program, containing over one hundred twenty million men and women' fingerprints, many inside the form of -finger records. The US visit program has been migrating from flat (not rolled) fingerprints to ten flat fingerprints considering that 2007. Speedy capture generation currently enables recording of ten simultaneous fingerprint impressions in as low as 15 seconds according to man or woman. The largest criminal fingerprint AFIS repository in the USA is the FBI's subsequent technology identification (NGI) in Clarksburg, WV. NGI has extra than 60 million person automatic fingerprint records (both crook and civil applicant records). NGI is the FBI's maximum treasured provider to American regulation enforcement, providing accurate and fast fingerprint identification offerings.

The Unique Identity Authority of India is the world's biggest fingerprint (and largest multi-modal biometric) machine the use of fingerprint, face and iris biometric records. India's unique identity task is likewise referred to as AADHAAR, a word meaning the foundation in several Indian languages. AADHAAR is voluntary software, with the purpose of finally offering dependable national id documents to most of estimated India's 1.25 billion residents. With a biometric database many times large than every other within the global, AADHAAR's

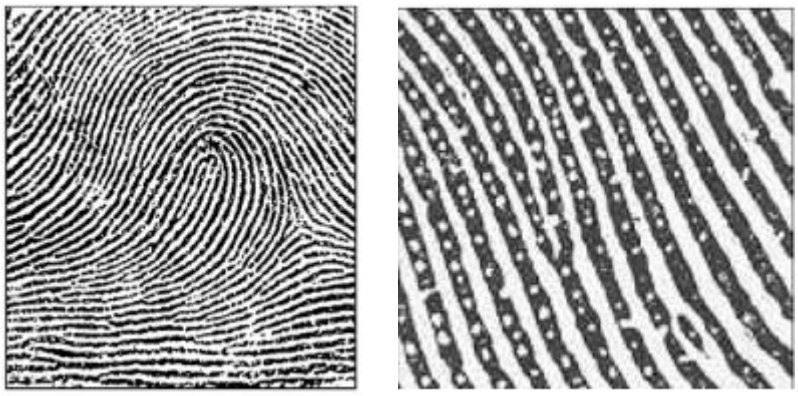
capacity to leverage computerized fingerprint and iris modalities (and probably automatic face recognition) allows fast and dependable computerized looking and identification not possible to perform with fingerprint technology alone, in particular, while looking kids and aged citizens' fingerprints. As of January 2017, the authority has issued more than 1.11 billion (more than 111 crores) AADHAAR numbers.

## 2.4 BASIC STRUCTURE OF FINGERPRINT

The skin at the palm and palms of the human hand along with the skin on the sole and feet of the foot has the precise and unique belongings of being ridged by way of a pattern of slender or narrow ridges and valleys, additionally called furrows or ravines (Cummins, 1961). These skin ridges have several useful functions. For instance, they enhance the friction between the pores and skin and different surfaces, thereby lowering slipping. Because of this the pores and skin is often known as friction skin. Because of the huge kind of ridge orientations on the surface, the ridges are capable of increase the drag in all guidelines.

The friction additionally blessings the experience of contact by means of increasing sensitivity and helping to differentiate extraordinary texture. The ridges on human pores and skin become elevated for the duration of fetal improvement with the help of across the eighteenth week of being pregnant, and the sample of ridges remains unchanged throughout an individual's existence. This is called permanence. The overall pattern of ridges and valleys is essentially decided by genetic elements. But, in the course of their formation minor developmental disturbances create neighbourhood ridge irregularities. Those disturbances are effects of the fetus unique improvement environment in the womb, so all ridge valley styles are particular while examined sufficiently closely. That is even real for twins who share the exact same DNA. The worldwide ridge patterns for twins are regularly very similar, but minute irregularities may be used to differentiate the individuals (Jain et al., 2002). Figure 2.1a suggests a sample fingerprint and Figure 2.1b includes a magnified view of the ridges and valleys from a small location of a fingerprint. Due to the permanence or never changing or unique traits mentioned above, fingerprints may be used to uniquely become aware of individuals during their existence. There are 3 levels of shape or features in a fingerprint. The first level of structure is the global pattern of ridges and valleys. As an example, some of the ridges in Figure 2.1 (a) input from the lowest-left of the photo, loop around a not unusual or same centre point, and go out on the left. That is the global pattern of the fingerprint ridges, and maximum fingerprints fall sincerely into one in all numerous sample or pattern

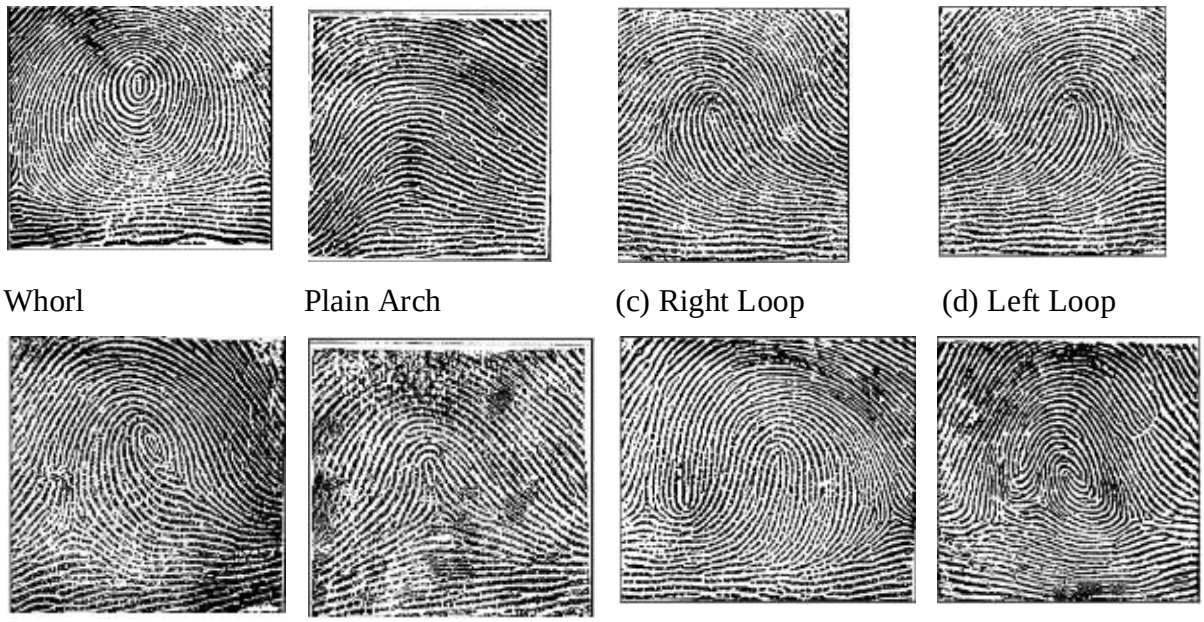
classes. The most common class scheme is known as Henry's classification (Henry, 1900) and is shown in Figure 2.2.



(a) A Fingerprint image (b) A magnified image of fingerprint ridge and valley

**Figure 2.1:** Fingerprint image with its ridge and valley

Henry's classifications (and others primarily based on it) are known as exclusive due to the fact they partition fingerprints based on mutually exclusive property. The most important application of fingerprint classification is indexing. The distribution of fingerprint classes in nature isn't always uniform. Central pockets, Twin loops and Accidentals are very exceptional so they may be regularly unobserved for type purposes.



Whorl Plain Arch (c) Right Loop (d) Left Loop

(e) Central Pocket (f) Tented Arch (g) Twin Loop (h) Accidental

**Figure 2.2:** Henry's Fingerprint Classes

The probabilities of the remaining class types are approximately 0.037 (arch), 0.338 (left loop), 0.317 (right loop), 0.029 (tented arch) and 0.279 (whorls) (Wilson, 1994). Observe that left loops, right loops and whorls are the most commonplace, making up 93.4% of all

fingerprints. Consequently, fingerprint instructions have a totally limited capability to distinguish individual prints from each other. The second level structure or Level 2 happens in neighbourhood or local fingerprint regions. In Figure 2.1 (b) one of the ridges splits into two awesome ridges. Also in same Figure, word that close to the bottom right of the image there is a totally brief ridge. These neighbourhood ridge discontinuities, called minutiae (or minutia inside the less commonplace singular form), shown in Figure 2.3, have little impact on the global ridge-valley pattern. But, it's being and locations of those minutiae that encompass a good deal of a fingerprint's individuality. For this reason, they are the essential and common discriminating feature utilized by human experts. There are fundamental varieties of minutiae: ridge termination and bifurcations. Ridge endings are locations in which ridges terminate and bifurcations are places wherein a single ridge separates into two ridges. There are other types of minutiae, but they're combos of ridge termination and bifurcations. A typical fingerprint carries as much as 80 minutiae; however, far fewer might be present in a latent print or a print captured from a small scanner.

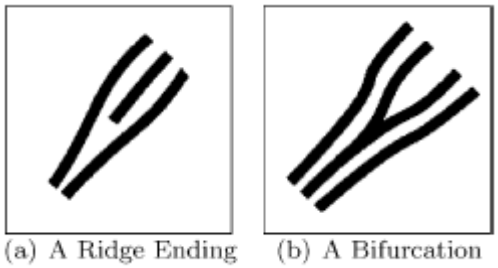



**Figure 2.3:** Fingerprint Minutiae
(Source: Yager and Amin, 2004)

The Level 3 structure or type of fingerprint consists of low level capabilities or features inclusive of sweat pore and ridge shapes. However, they're rarely used in automatic structures because they require very excessive decision scans or high quality for dependable feature extraction. Singularities are every other important fingerprint shape which has each global and local characteristic. Globally, a singularity is a location of a fingerprint wherein the ridge pattern makes it visually outstanding. In literature two types fingerprint singularities are available: cores and deltas. Locally, a core is the turning point of an internal-most ridge and a delta is a place where in two ridges are running side by side or parallel diverge and then run for a while as if single ridge. Singularities are helpful for determining fingerprint's class. The singularities with core and delta is shown in Figure 2.4.

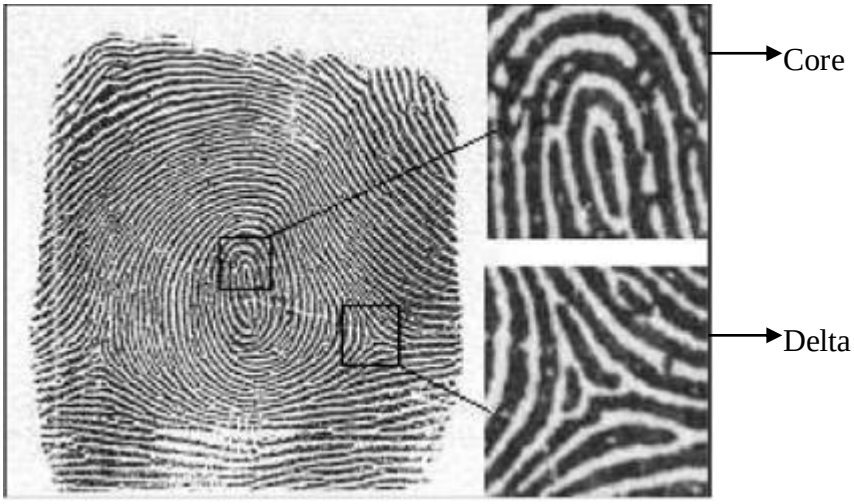



**Figure 2.4:** Fingerprint singularities with core and delta (Yager and Amin, 2004)

Pankanti et al., (2002) have conducted a study on the uniqueness of fingerprints based on minutiae features. They presented a model of fingerprint individuality that is particularly suitable for computerized matching as it takes under consideration some of the challenges faced through matching algorithms. Pankanti et al., (2002) presented a variety of results based on the number of minutiae features present in a fingerprint and the wide variety of correspondences required to consider two fingerprint matching or similarities. As an example, a framework whose prints include 36 minutiae on an average should have the ability to differentiate about sixteen million fingerprints primarily based on 12 corresponding minutiae pairs.

The first Research work on the Automation of Fingerprint matching seemed in 1963 (Trauring, 1963). From there next subsequent four decades there has been a huge attempt by using regulation enforcement, private, and academic institutions to expand green AFISs.

## 2.5 FINGERPRINT INDIVIDUALITY PROBABILITY MODELS

The early fingerprint individuality research usually targeted on minutiae-based representations; a few studies explicitly factored in fingerprint class which includes right loop, loop at left, whorl structure, arch pattern, tented arch pattern, and so forth statistics. The kind, direction, and region of minutiae were the maximum normally used features in those individuality researches. The sort of minutiae used varies from one examine to different: a few research used two minutia varieties as ending and bifurcation. Whereas others used as many as, 13 types of occasions (Osterburg et al., 1977). Later models taken into consideration

additional capabilities like ridge counts sweat pores to decide the chance of incidence of a specific fingerprint configuration (Stoney & Thornton, 1986; Roddy & Stosz, 1997). Ridge ending and ridge bifurcation features are collectively called as minutiae features.

The fingerprint individuality problem turned into first addressed by Galton in 1892 (Galton, 1892) who taken into consideration a square place spanning six-ridges in a given fingerprint. He assumed that, on an average, a complete fingerprint may be blanketed by 24 such six-ridge huge independent rectangular areas. Galton estimated that he have to effectively reconstruct any of the areas with a probability of ½ looking at the encompassing ridges. As a consequence, the chance of a specific fingerprint configuration, given the surrounding ridges is$(1/2)^{24}$. He accelerated this conditional (on surrounding ridges) possibility with the probability of finding the surrounding ridges to acquire the possibility of the prevalence of a fingerprint as (1/16) x (1/16) x $(1/2)^{24}$ = 1.45 x $10^{-11}$ (i.e., 1 in 68 billion). Where in 1/16 is the chance of prevalence of a specific fingerprint type (consisting of arch style, tented arch style, left loop style, right loop pattern, double loop pattern, whorl pattern, and so on.) and 1/ 256 is the possibility of prevalence of an appropriate number of ridges getting into and exiting every of the 24 regions.

The Henry model (1900) the 2$^{nd}$ version, proposed by Sir Edward Henry, turned into a drastic deviation from Galton's method. Henry proposed that each minutia was an unbiased, identically distributed event (every occurrence of minutia has the equal possibility and is not established or prompted by means of every other minutia). The chance of a minutia occurrence was 1/4 (.25). The possibility of locating 12 matching minutiae was then (1/4)12 = 6 x $10^{-8}$ (i.e., about 1 in 17 million). To account for pattern type, consistent with Henry's model, sample kind became deemed equal to two more minutiae (multiplying the preceding results for minutiae by 1/sixteen). As a result, if given a whorl print with 12 minutiae, the possibility of finding a whorl print with 12 matching minutiae is (1/4)14 = 4 x $10^{-9}$ (i.e., approximately 1 in 270 million).

The Balthazard model (1911), which is the usage of Henry's method, Dr. Victor Balthazard also used the probability of a minutia event same to 1/4, however at the same time as Henry's became arbitrary, Balthazard primarily based his use of 1/4 on whether or not a bifurcation or ridge finishing pointed to the left or to the proper. He proposed that each of those four opportunities (bifurcation left or right, ridge finishing left or right) is equally possible to arise, and thus he arrived at a chance of 1/4 for a minutia event. His model did no longer include a thing for pattern type. His version founded 17 matching minutiae had a probability of (1/4)17

= $6x10^{-11}$. He then reasoned that, in order for his model to meet the expectation of best one person on the earth to have a matching configuration to the print, 17 minutiae in the agreement would want to be located (i.e., 1 in 17 billion). He additionally conceded that if one was certain the donor turned into confined to a certain geographical place, then an advantageous identification can be set up with a decreased variety of minutiae (e.g., 10 to 12 minutiae). In effect, Balthazard proposed the primary minimum factor threshold.

The Bose model (1917) used the Henry version and also used a chance of 1/4 for a minutia event; but, he actually did so with a bad assumption. He chose 1/4 as a chance on the basis of his contention that there are 4 kinds of minutiae events, all equally probably to arise: a dot, bifurcation, finishing ridge, or non-stop ridge. Surely, there are many more continuous ridge occasions than trivialities and surely more ridge endings and bifurcations than dots disbursed in a normal fingerprint.

The wilder and Wentworth model (1918) used the Henry version as well, however in preference to an assumed possibility of minutia incidence of 1/4, they used 1/50. They haven't any definite statistics for understanding the in step with the percentage of occurrence of minutiae and they took as small as a ratio of 4 to one, for the percentage of prevalence of any one of these details; it would be rather 1 in 50 or 1 in a hundred. The Pearson Model (1930) did not create a separate fingerprint model. The Pearson model (1930) did no longer create a separate fingerprint version. Pearson advised that an extra suitable estimate of the possibility of a minutia event was 1/36, in place of 1/2 as Galton had used.

The Roxburgh model (1933) integrated several modern standards. First, it blanketed an aspect for the number of intervening ridges from a minutia to the starting place, the use of a polar coordinate framework. All preceding models used rectangular areas or Cartesian coordinate structures. Second, Roxburgh protected a clarity thing, recognizing that clarity can be low because of smearing or bluring and every now and then the kind of trivialities found in a print may be ambiguous. The element, termed “Q” for superiority, allowed for the adjustment of chances based totally on the high-quality of a minutia. The Roxburgh model also incorporated elements for sample or pattern kind and minutiae kind.

The Cummins and Midlo model (1943) is identical to the wilder and Wentworth model, with the exception of a factor for sample or pattern type. They reasoned that the probability of acquiring the maximum common fingerprint sample (an Ulnar loop) with comparable ridge counts (based totally on 11 ridges) was 1/31. Consequently, as a top sure, this issue is improved with the probability of a minutia arrangement.

The Amy model (1948) included two essential factors of individuality: the wide variety and count and location of minutiae. Amy first derived facts for the variety of minutiae from gazing frequencies of occurrence in a hundred fingerprints. All preceding fashions either arbitrarily assigned frequencies or assumed same frequencies. Amy used the Balthazard standards of bifurcation to the left or right and ridge ending but observed that these minutiae types have been no longer uniformly distributed. From these distributions, Amy calculated a component for trivialities type (which includes orientation). Amy then calculated the whole range of viable minutiae preparations, given some of the minutiae. He did so the use of a binomial distribution. This type of probability distribution and modelling might be comparable to calculating how many distinct methods you could arrange a positive wide variety of motors in a parking lot with a set quantity of areas, in which each automobile would be parked in an area, however no longer all areas packed full, and sooner or later, the lot itself having a fixed, given length.

Kingston's (1964) model, which is very much like Amy's model, computes the possibility of a fingerprint configuration based totally at the probabilities of the located wide variety of minutiae, observed positions of minutiae, and determined minutiae kinds.

Gupta (1968) anticipated the probability of P (fingerprint configuration probability) as 1/10 for bifurcation and endings, and 1/100 for the less commonly taking place minutiae kinds, primarily based on 1,000 fingerprints. He extensively utilized a fingerprint-kind-factor of 1/10 and correspondence-in-ridge-count number-aspect of 1/10.

Osterburg et al. (1980) divided fingerprints into discrete cells of size 1mm x 1mm. They computed the frequencies of 13 forms of trivialities activities (together with an empty cell) from 39 fingerprints (8591 cells) and estimated the chance that 12 ridge endings will in shape between two fingerprints based totally on a median fingerprint area of 72 mm2 as 1.25 x 10-20.

Trauring (1963) become the first to pay attention explicitly on measuring the quantity of element needed to establish a correspondence between two prints from the identical finger (intra-class variant) the usage of an AFIS and determined that corresponding fingerprint capabilities in impressions of the same finger can be displaced from every different by as a great deal as 1:5 times the inter-ridge distance. He similarly assumed that (i) Minutiae are allotted randomly, (ii) There are most effective kinds of minutiae (ending and bifurcation), (iii) The two sorts of minutiae are similarly in all likelihood, (iv) The two viable orientations

of minutiae are equally in all likelihood, and (v) Minutiae type, orientation, and position are impartial variables.

Stoney et al. (1986) severely reviewed earlier fingerprint individuality fashions and proposed a detailed set of fingerprint features that should be considered. These capabilities covered ridge shape and description of minutiae area, ridge counts between pairs of minutiae, description of minutiae distribution, orientation of minutiae, variation in minutiae type, variation among fingerprints from the identical supply, number of positions (distinctive translations and rotations of the input fingerprint to fit with the template), and wide variety of comparisons finished with different fingerprints for identity. Table 2.2 shows tabular comparisons of the features used in fingerprint individuality models by different authors.

**Table 2.2:** Fingerprint features used in different individuality Models

(Source: Pankanti et al., 2002)

| **Author** | **Fingerprint Features** |
|---|---|
| Galton (1892) | ridges, minutiae types |
| Pearson (1930) | ridges, minutiae types |
| Henry (1900) | minutiae locations, types, core-to-delta ridge count |
| Balthazard (1911) | minutiae locations, two types, and two directions |
| Bose (1917) | minutiae locations and three types |
| Wentworth & Wilder (1918) | minutiae locations |
| Cummins & Midlo (1943) | minutiae locations and types, core-to-delta ridge count |
| Gupta (1968) | minutiae locations and types, fingerprint types, ridge count |
| Roxburgh (1933) | minutiae locations, two minutiae types, two orientations, fingerprint and core types, number of possible positioning, area, fingerprint quality |
| Amy (1948) | minutiae locations, number, types, and orientation |
| Trauring (1963) | minutiae locations, two types, and two orientations |
| Kingston (1964) | minutiae locations, number, and types |
| Osterburg et al. (1980) | minutiae locations and types |
| Stoney et al. (1986) | minutiae locations, distribution, orientation, and types, variation among prints from the same source, ridge counts, and number of alignments |

## 2.6 FINGERPRINT ENHANCEMENT TECHNIQUES

In fingerprint recognition system the quality of the image acts an extremely significant role while matching two fingerprints. Most of the fingerprint recognition systems result in poor matching due to impurity or noisy images (Krishna Prasad, K., & Aithal, P. S., 2007d). So there is high necessity and scope for image preprocessing and enhancement techniques with the purpose of enhancing or improving the superiority of fingerprint image and to obtain high accuracy in the matching process. The best fingerprint input is decided by using many elements, which sometimes can be difficult to manipulate; consequently a fingerprint machine has to be able to handle additionally the image input of medium and occasional high-quality (recoverable). In some cases, it's far feasible to enhance considerably the image best by way of making use of a few image enhancement techniques. The primary reason for such system is to develop the image by way of improving the clarity of ridge shape or growing the consistency of the ridge orientation. In noisy areas, it's very difficult to define a common or similar orientation of the ridges. The technique of improving the image before the feature or characteristics extraction is likewise called pre-processing. The reason for degradation lies inside the reality that image received from sensors or different media aren't constantly assured of ideal pleasant. The primary purposes of fingerprint image preprocessing operations are noise reduction and evaluation enhancement which complements the contrast between darker and brighter curves in a fingerprint image. There are many filtering techniques and enhancement methods are available in the literature, which is examined in this part.

Hong et al. (1998) proposed a rapid fingerprint enhancement or improvement algorithm, which depended on ridge orientation pattern and frequency pattern and through that, they can able to obtain more clear ridge and valley structure of the initial fingerprint image. They have evaluated the performance of fingerprint enhancement algorithm using goodness index and found that incorporating enhancement algorithm improves verification accuracy. Chikkerur et al. (2005) anticipated a new concept for fingerprint improvement based on Short Time Fourier Transform (STFT) Analysis, mainly used for non-stationary properties. The algorithm evaluated all inherent features of the fingerprint image and found that performance of the algorithm improved slightly better. The Three inherent features are foreground or interested region mask, local ridge orientation pattern, and local frequency orientation structures. Sepasian et al. (2008) proposed an algorithm for fingerprint minutiae based on CLAHE (usually referred as Contrast Limited Adaptive Histogram Equalization). Their

primary intention was to know the performance of combining Clip Limit, standard deviation, and sliding neighborhood, three techniques for the fingerprint enhancement. Through a simulated investigation, paper stimulates developing thinning process and enhancement of the image.

Greenberg et al. (2000) compare the detection and analysis of minutiae through fingerprint image binarization and direct extraction of minutiae from grayscale fingerprint images. They used Histogram equalization concept, Wiener filtering method, and image binarization as first method and unique anisotropic method of filtering for direct grayscale enhancement or improvement as the second method in order to compare binarisation and direct extraction of minutiae from grayscale image techniques with an ultimate goal to achieve image enhancement. They found that both methods show significant improvements in terms of efficiency and execution time.

He et al. (2003) studied, analyzed and proposed a new algorithm based on orientation fields for image enhancement. In order to reduce noise and to obtain a high-quality image and to obtain better matching results, image enhancement and minutiae matching are two important steps in auto computer-assisted fingerprint recognition system. Misra et al. (2012) developed a method for fingerprint image enhancement based on Fourier cosine transform and matching of fingerprint image based on region and line structure that live between minutiae pairs.

Yang et al. (2002) improved the existing algorithm for fingerprint feature extraction by extracting minutiae directly from an original gray level image without undergoing steps of binarization and thinning and obtained considerable better performance efficiency. Yang et al. (2003) introduced novel filter design method for fingerprint image enhancement using Traditional Gabor Filter (TGF) of the invention to overcome drawbacks in image-dependent parameter selection strategy. They have modified existing Traditional Gabor Filter as Modified Gabor Filter (MGF). Their algorithm achieved a remarkable advantage in preserving fingerprint image structure and in image enhancement consistency.

Lee et al. (2006) studied recognition of fingerprint image captured by a mobile camera. They proposed a robust regression method to overcome the drawbacks of gradient-based filtering inability to remove outliers. In the pre-processing stage, they divided the fingerprint images into small blocks and verified blocks quality using good or bad quality regions. Their pre-processing algorithm and experimental results showed good performance compared to conventional ones.

The accuracy of the test datasets image directly depends on the quality of the image in training dataset. Because of this purpose, the good quality image is an essential and basic requirement for the improved results of matching. But this is not so easy or possible to obtain a good quality image almost all the time due to skin problems, scars on fingers. These wounds or cuts may end up with false minutiae results even in the good quality image. The error or noisy fingerprint image cannot able to provide all features at the time of feature extraction, either it may give wrong data or may not give required features only. Looking into all these aspects, fingerprint image pre-processing or enhancement becomes necessary and essential. There are many fingerprint enhancing techniques are available in the literature, overviews of these few techniques are explained below (Saini, 2012).

**2.6.1 Contrast Adjustment:** It is part of the noise filtering or smoothing process, which is essential in automatic identification or recognition systems like a fingerprint or any other biometric-based recognition systems to get higher efficiency.

**2.6.1.1 Histogram Modelling:** The histogram of the fingerprint image represents, how often or number of times a gray level occurs in a group of total gray levels of the image. The output image produced by the histogram contains noisy in terms of intensity levels (Gonzalez, 2002; Jain, A. K., 1989; Zimmerman *et al.*, 1988; Kim, Y. T., 1997

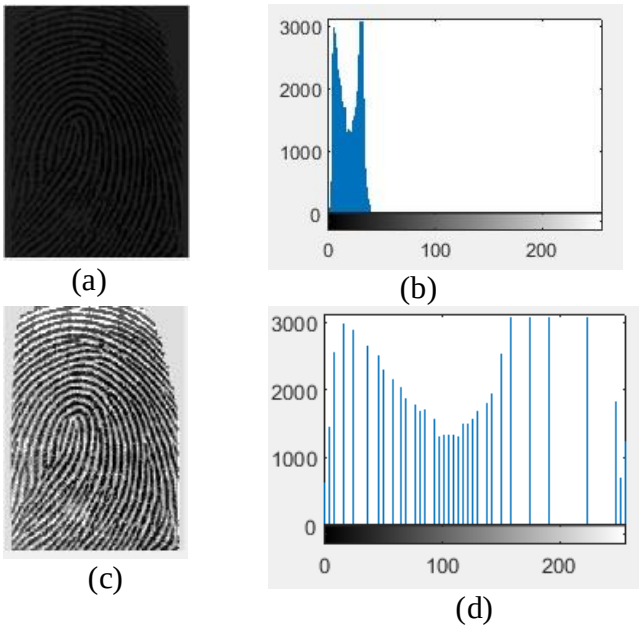



**Figure 2.5:** Fingerprint Image and its Histogram (a) Original image (b) Histogram of original image (c) Histogram equalized image (d) Histogram of equalized image (Krishna Prasad, K., & Aithal, P. S., 2007)

Histogram equalization is a special technique to adjust intensity or brightness and to enhance the contrast (range of value between dark black to heavy white) of the image pixels. By using histogram equalization, we can get a uniform or identical histogram for the output image. This technique is mainly used for improvement in contrast of an image by adjusting the individual gray level of the image. There are many variations of Histogram equalization by modifying the logic of Histogram equalization. The results of the histogram are shown in Figure 2.5.

**2.6.2 Filtering Methods**

In fingerprint image recognition system, many filtering methods are available in the literature. These filtering methods ultimate purpose is to remove all types of error encountered in input or initial image and to improve the image recognition capacity in all aspects. Few methods are discussed below;

**2.6.2.1 Median Filtering:** Median filtering considers statistical median of the pixels contained in a window around the pixel and it is a nonlinear filtering process used to remove impulsive noise and to improve the fingerprint image excellence (Cao et al., 2010). Median is calculated as follows

$V(m, n) = \text{median} \{y (m-k, n-1), (k,1) \epsilon W\}$

Where W is the chosen Window. As like statistical figures, median filtering requires pixel values of the window should be arranged in order.

**2.6.2.2 High Pass filtering:** High pass filtering is basically used to extract edges of the images (O'Gorman and Nickerson, 1989). High pass filter helps to enhance the superiority of the image by sharpening the edges of the fingerprint image. Due to this reason its always good practice to do High passes filtering for the original image. The high pass filtering simply removes or the blurred image from the original image.

**2.6.2.3 Weiner Filtering:** Weiner filtering produces a good quality image by removing additive noises even when the image is having blur or low intensity (Greenberg et al., 2000). It minimizes maximum error in the process of noise smoothing, to enhance the superiority of the image.

**2.6.2.4 Gabor Filtering:** Gabor channel is a linear channel whose impulse reaction is characterized by a harmonic function and the result is multiplied by a Gaussian function (Hong et al., 1998). Gabor filter ideally catches both local orientation pattern and frequency details from a fingerprint image. Once the ridge orientation and ridge frequency are calculated, at that point they are utilized to build the Gabor filter. In fingerprint enhancement,

Gabor filter can be aligned to a particular frequency and orientation values. Gabor filter can improve the ridges towards local orientation.

**2.6.3 Binarisation and Thinning:** Binarisation is one of the preprocessing stages in automatic fingerprint recognition systems. If the input image is a color image, first it should be converted into a grayscale image (V. Espinosa, 2002). From the grayscale image, a binary image is obtained by considering only two states as zero for ridges, which are represented by black color and one for the valley, which is represented by white color. In binarisation, we present some threshold for pixels and pixel which is lower and higher than is threshold is represented by white and black color respectively. Thinning is a special process that consecutively wears away the foreground pixels and finally produces lines that are the almost one-pixel width (Ahmed & Ward, 2002; Patil et al., 2005). The first and foremost condition for thinning is input image should be a binary image and produces output as a binary image. Thinning is a final prior step to minutiae extraction in automatic fingerprint recognition system. Thinning is not achieved in a single step but it achieved through an iterative process. The connectivity of ridges and bifurcation can be reproduced from the thinning, means it preserves the basic structure of the image without affecting its original structure.

## 2.7 FINGERPRINT SEGMENTATION TECHNIQUES

An essential and important step in order to obtain high quality and performance rate at all types of image is through accurate segmentation. Fingerprint segmentation is the one of the main process involved in fingerprint pre-processing and it refers to the process of dividing or separating the image into two disjoint regions as the foreground and background. The foreground also called as Region of Interest (ROI) because only the region which contains ridge and valley structure is used for processing, while the background contains noisy and irrelevant content and that will be discarded in later enhancement or orientation or classification process.

In literature, a good number of papers are available for fingerprint segmentation, which can be roughly categorized under two classifications as block-wise methods and pixel-wise methods (Krishna Prasad, K., & Aithal, P. S., 2017e). In the block-wise method, the fingerprint images are classified into different equal sized nonoverlapping blocks and further organize blocks into foreground and background region based on the extracted block-wise features. On the other hand, pixel-wise methods emphasis on pixel and classifies the fingerprint image based on pixel-wise features of the image. The most common types of

features used in segmentation algorithms are gray-level features, orientation features, ridge pattern and ridge frequency features, ridge intensity features, and frequency domain features.

Some of the most common types of segmentation algorithms are, TV-L1 based Adaptive Total Variation Model (Zhang, Lai, & Kuo, 2012a), TV-L2 based Directional Total Variation Model (Zhang, Lai, & Kuo, 2012b), Method based on a combination of ridge orientation and ridge frequency characteristics using orientation tensor approach (Choi, Boaventura, Boaventura, & Jain, 2012), Orientation field is combined with the statistical characteristics of the gray to form new method (Xue, & Li, 2012), Ridge orientation Method based on Ridge Temple using correlation with a sinusoid (Short, Hsiao, Abbott, & Fox, 2011), and the coherence, the mean, the variance as three pixel features method (Bazen & Gerez, 2001).

Jain & Dubes (1988), explains the algorithm for clustering in his book, these early approaches for clustering can be used for segmentation, which acts as the basis for many new methods including boundary based segmentation such as Canny edge detection Canny, 1986. In this method, researcher defines a comprehensive set of goals for the computation of edge detection points. Adams and Bishof (1994) proposed segmentation algorithm for images, which are intensity images with certain characteristics like robust, rapid, and free of tuning parameters. This algorithm can take input as either individual pixels or regions and points these inputs to some region formed by the algorithm. The algorithms explain two methods in which input corresponds to the region, either by using manual seed or by an automated procedure. Chakraborty et al. (1996), proposed a method which combines region based segmentation and boundary finding to form new method which is more vigorous to error or noise and high performance. The literature covered above is some general segmentation algorithms which will apply to any types of images.

In literature, there are many studies available, which mainly focus on fingerprint image segmentation. Most of the segmentation algorithm does classification of the image based on either supervised learning or unsupervised learning. When a class label is not known or unknown, means of unsupervised learning, classification is significantly and very difficult. Researchers, Mehtre, et al. (1989) classified the image into blocks, which is administrative specific and the size was 16 × 16 pixels. Based on the gradient distribution, each block was classified. This method is best suited for simple fingerprint images which contain only background and foreground. Later Researchers Mehtre and Chatterjee (1989) extended this work by leaving the grayscale variance, which will usually be lower than some threshold value. Researchers Ratha et al. (1995) proposed 16 × 16 blocks of classes and each one was

developed based on the gray scale variance in the direction opposite to the orientation of ridges.

The authors Jain and Ratha (1997), concentrated for the detection of objects located in complex backgrounds. The given object is first applied to a bank of even-symmetric Gabor filters. The output image received from the Gabor filter is subjected to a sigmoid function transformation. The yield image of the Gabor filter is applied as an input to the clustering algorithm, which develops spatially compact clusters. Sun and Ai (1996) pre-processed initially fingerprint image by converting it into a binary image with the help of dynamic threshold value (T). Moayer and Fu (1975) used sampling squares, which are obtained from the subdivision of fingerprint images for the ultimate goal of feature extraction. They used dynamic threshold value (T) to convert the initial image to a binary image. In order to determine the local threshold value, researchers used neighbor pixels by group $5 \times 5$ pixels.

Bazen and Gerez (2000) used coherence and morphology of fingerprint image with an intention to obtain a smooth image by filtering different types of noises. The same author Bazen and Gerez (2001) improved their work by adding two more statistical features as the mean and variance for their previous work. Here classification is done with the aid of optimal linear classifiers, which acts as a trainer for classification. With a goal to find compact cluster and reducing, classification error for post-processing morphology is applied.

Naji et al. (2002) developed a segmentation algorithm, which computerized or automated the method of selecting a threshold value at the time of segmentation with the aid of histogram equalizer. Segmentation algorithm generally falls under two categories of machine learning techniques as supervised learning and unsupervised learning. Unsupervised learning uses threshold decided on detecting features to cluster the image. Supervised learning uses a simple linear classifier to classify features as a region of interest (ROI) or background and foreground. As a part of supervised methods, Alonso-Fernandez et al. (2005) used a Gabor filter to filter the input image and to obtain a smooth image. The neural network can also be used in the segmentation process to reduce the noise or to enhance the image quality.

Barreto et al. (2005) used a neural network to train the fingerprint image data sets using Fourier spectrum and obtained a segmentation of fingerprint images. Zhu et al. (2006) also used neural network concepts in order to train the fingerprint data set, but they used the gradient of the fingerprint orientation to segment the images. Wu et al. (2007) proposed a new method for segmentation; in their method, they used the strength of Harries corner function to extract the background from foreground or to extract a region of interest. In order

to separate region of interest from the background image, they used corner strength measures. Tiwari, K., & Gupta, P. (2015) proposed a new method for extracting a single fingerprint image from the slap fingerprint scanner, which simultaneously scans four fingerprints of a person in a single image. While extracting the single fingerprint image the image is also required to be segmented. They used a novel technique to extract solitary (single) fingerprint image based on force field and heuristics using divide and conquer strategy and is tested in IITK-4slap-Rural and IITK-4slap-student database.

Thai, Huckemann, and Gottschlich (2016) proposed the new approach for fingerprint segmentation in three folds, firstly used factorized directional bandpass (FDB) and directional Hilbert transform originated from Butterworth bandpass (DHBB) filter combined with soft-thresholding for texture extraction. Secondly, as an evaluation benchmark with 10560 images marked manually for ground truth segmentation. Thirdly they have compared systematically factored directional filtering with other similar fingerprint segmentation approach and obtained comparatively good performance.

## 2.8 FINGERPRINT MATCHING ALGORITHMS

Fingerprint corresponding refers to deciding the similarity among given fingerprint snapshots. The alternative of the matching algorithm relies upon on which fingerprint illustration is getting used. Typically, a matching set of rules first tries to get better the interpretation, noise filtering, rotation and bending parameters between the specified image sets and then decides the likeness between the images. Fingerprint matching is taken into consideration a challenging problem due to the noise in the fingerprint image, massive intra-magnificence variant and small interclass variations between different impressions of the similar finger. As each authentication system has special overall performance requirement, there is a scope to always improve the matching overall performance of the cutting-edge systems. These sections depict a number of the existing matching algorithms in literature and there are primarily grouped into five categories.

- Minutiae Based Matching
- Non-minutiae Based Matching
- Correlation Based Matching
- Ridge Feature Based Matching
- Hybrid Methods

### 2.8. 1 Minutiae based Fingerprint Matching

Minutiae-based matching is the maximum broadly used the method of fingerprint illustration and its configuration is incredibly exclusive (Nanni and Lumini, 2008). Non-minutia feature primarily based strategies (Jain et al., 2000; Zhang and Wang, 2002), include that usage of image depth values, orientation fields, cores, and so on. A minutiae-based method far more correct or accurate in comparison to other correlation primarily based structures and the template size are smaller in minutiae-based fingerprint illustration. In this system, fingerprints match if their minutiae point match while comparing two fingerprints. Minutiae-based fingerprint technique is the backbone of maximum presently available fingerprint popularity matching techniques. Compared to other fingerprint characteristics, the minutia point characteristics having corresponding orientation maps are sufficient to distinguish between fingerprints robustly. Fingerprint illustration the usage of minutiae properties reduces the complicated trouble of fingerprint reputation to a problem of point pattern matching. Since the unique fingerprint image can't be reconstructed using most effective the minutiae information, the minutiae-based fingerprint identification systems also can help privateness problems and the minutiae are sincerely enough sufficient to show fingerprint individuality. In phrases of evaluation, intensity decision and global distortion the minutiae are more solid and study in relation to different fingerprint matching schemes. But, the primary mission lies in extracting the minutiae from a low-quality image.

An remarkable quality of fingerprint image is truly critical for minutiae extraction. However, every so often the image quality might be poor due to diverse reasons and therefore it becomes essential to enhance or remove the noise and improve the contrast of the fingerprint image earlier than minutiae matching of fingerprints. The minutiae extraction techniques are categorized into two classes as grayscaled fingerprint image and binarized fingerprint image. Figure 2.6 shows the minutiae extraction classification techniques.

#### 2.8. 1.1 Binarised Image Minutiae Identification Techniques

A number of binary images primarily based strategies exist in the literatures which recognize minutiae through analyzing the localized pixel pattern or styles. These methods are classified into two types as skeletonized image and those which work on non-skeletonised fingerprint image.

### 2.8. 1.1.1 Non-Skeletonised Binary Image

Maximum fingerprint minutia extraction techniques are thinning-based wherein the skeletonization manner converts each ridge to one pixel length. Minutia factors are detected through finding the endpoints and bifurcation factors on the thinned or skeletonized ridge primarily based on the wide variety of neighboring pixels. The end factors are selected in the event that they have a single neighbor and the bifurcation points are decided on in the event that they have greater than two neighbors. However, techniques based totally on thinning are sensitive to noise and the skeleton shape does no longer conform to intuitive expectation. This category makes a specialty of a binary image based totally technique of minutiae extraction without a thinning technique. The principle problem within the minutiae extraction technique the use of thinning processes comes from the reality that minutiae within the skeleton image do not usually correspond to true minutiae inside the fingerprint image. In fact, quite a few spurious minutiae are determined because of undesired spikes, breaks, and holes. Consequently, put up processing is usually followed to keep away from spurious minutiae, which are based on each statistical and structural fact after characteristic or feature detection. Non skeletonised fingerprint is classified into three types as Chaincode representation (Shi & Govindaraju, 2006), run length encoding representation (Di et al., 1996; Shin et al., 2006), and Ridge flow and local pixel analysis representation (Gamassi et al., 2005; Alibeigi et al., 2009; Maddala et al., 2010).

#### 2.8.1.1.1.1 Chaincode Processing Method

Chain code processing approach is primarily based on the Chaincode illustration of object contours and the pixel image may be recovered completely from the Chaincode of its contour. On this technique, the changeover from whitish background condition to blackish forefront or foreground condition are identified with the help of tracing the image from up to down and right region to left region. A chain code based fingerprint feature extraction method considers ridge contours. The authentic gray-scale image is more suitable the use of an active noise removal or filter design that considers benefits of the forecasted directional flow of the contours. Image characteristics or minutiae are produced by the convention of ridge contour following (Govindaraju et al., 2003; Shi & Govindaraju, 2006). Each contour detail depicts smallest portion-pixel on the contour. It consists of fields for the x-axis, and y-axis positions of the pixel, the incline of the contour to the pixel, and supplementary statistics including curvature. In a binarized image of a fingerprint, ridge lines are a couple of pixel

huge usually without covering in one pixel wide. Tracing a line of ridge alongside its boundary in a counterclockwise direction, a termination or closing minutia (ridge ending) is observed when the outline makes an enormous left turn. Similarly, a split or fork minutia is detected when the outline or trace makes a vast proper flip or simply right turn.

**2.8.1.1.1.2 Run Length Encoding Method**

Run length encoding technique is based totally on the horizontal and vertical run-length encoding from binary fingerprint images. This method effects in speedy minutiae extraction without requiring a computationally costly thinning system (Di et al., 1996; Shin et al., 2006).

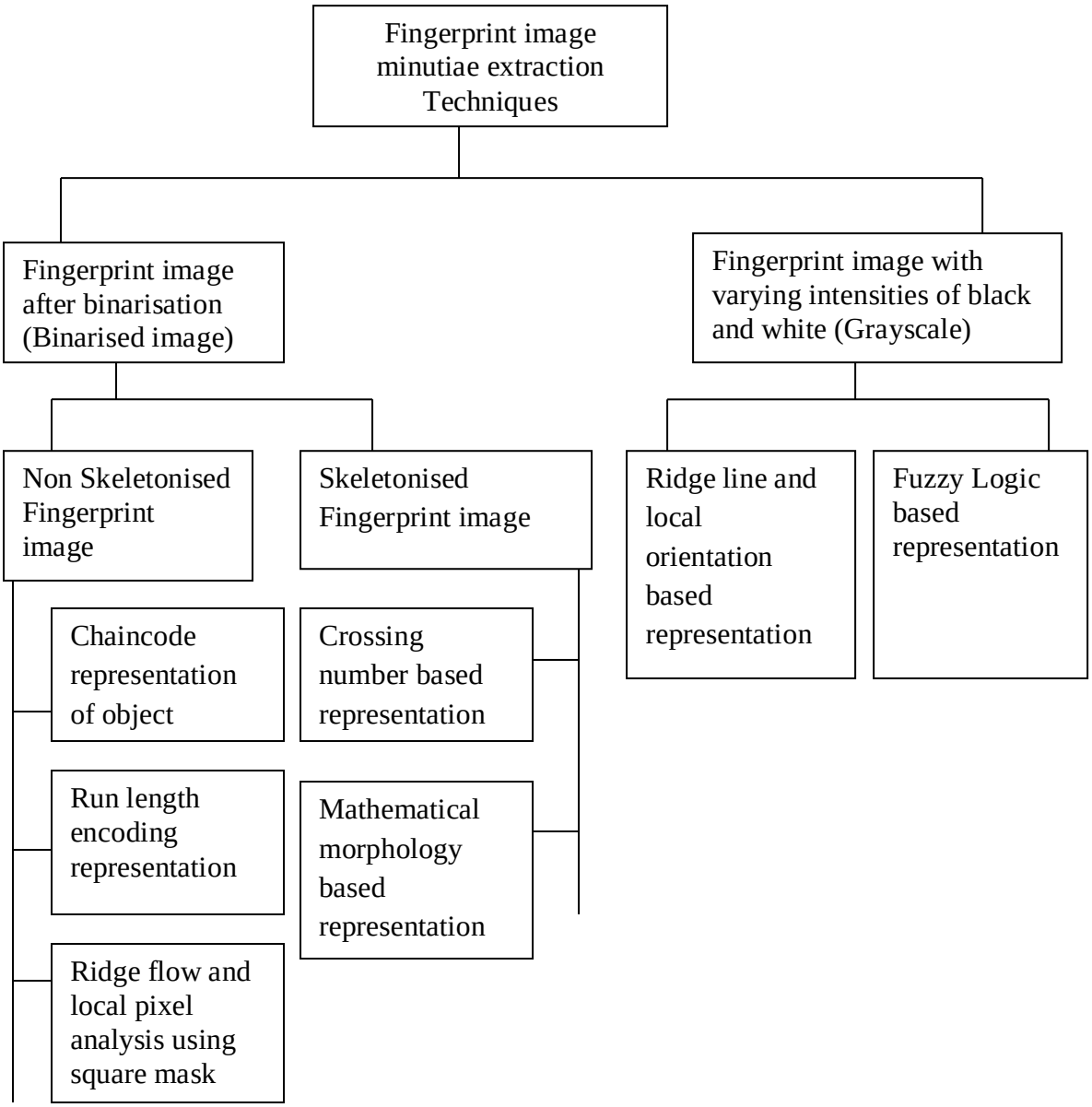



**Figure 2.6:** Minutiae Extraction Classification Techniques

This permits one to build a graph representation for some of the computing duties like component labeling, computations of Euler quantity, diameter, and convex hull, and a couple of points (Di et al., 1996). After run-length encoding, then runs' adjacency is checked and properties of runs are detected. But all feature runs cannot be proper minutiae. So, a few geometric constraints are brought for checking the validity of feature runs. As depicted in Figure 2.7 the image is preprocessed for enhancement, that's primarily based on the complexity of the image with Gabor filters adjusted to the neighborhood ridge orientation and frequency.

Initially, the picture is segmented (Klein et al., 2002; Chen et al., 2004; Alonso et al., 2005) to extract foreground region from the background region. Next, the task is normalization so that it has a contrast adjusted and equally distributed intensity levels. After finding the local orientation and frequency of ridge pattern around each pixel, the Gabor filter is implemented to every pixel location of the image. As an end result, the filtering process improves the ridges orientated within the route or direction of local orientation. Hence the filter out will increase the contrast between the region of actual and noisy image ridges, while correctly decreasing noise to set the parameters with admire to the orientation and the frequency, respectively. Subsequently, the image is binarized. The most effective way to apply binarisation is to choose a threshold value, and classify all pixels with values above this threshold as white, and all other pixels as black. The difficulty is the way to select the ideal threshold. In many cases, locating one threshold compatible to the entire image is very hard, and in lots of instances even impossible. Consequently, adaptive image binarization is having a scope where an ideal threshold is chosen for every image place (Zhang & Xiao, 2006; Otsu 1979). A run-length encoding is an efficient coding scheme for binary or labeled image as it efficiently utilizes memory space and also speeds up image processing time. In the context of the binary image, successive black pixels along the test line are defined as a run. Normally, a run-length encoding of a binary image is a listing of contiguous horizontal runs of black-pixels. For each run a locality of the beginning pixel of a run and either its length or the location of its ending pixel should be recorded.

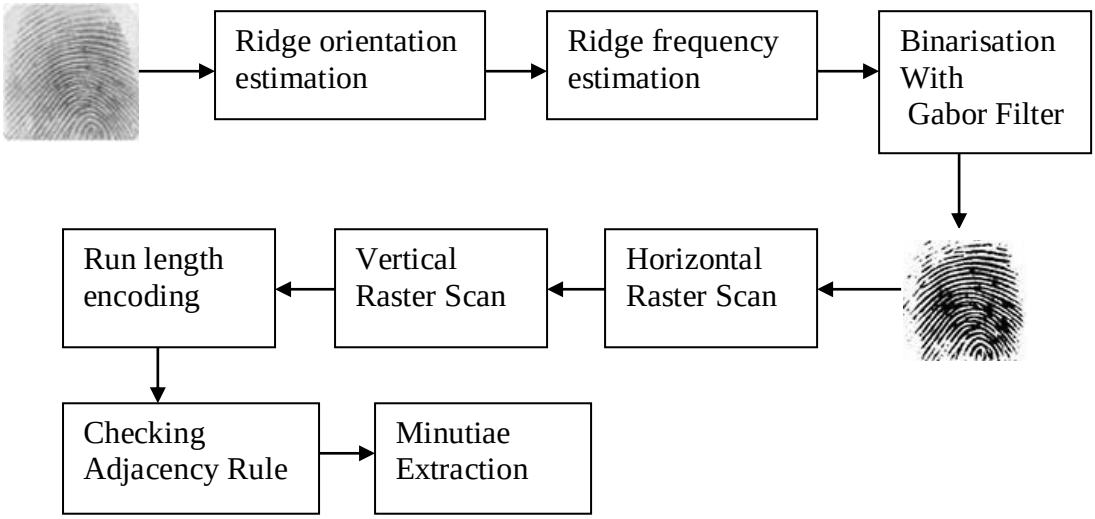



**Figure 2.7:** Block diagram of minutiae extraction technique using run length encoding

#### 2.6.1.1.1.3 Ridge Flow and Local pixel variation Analysis

Ridge flow and local pixel variation is a rectangular based technique to extract minutiae from non-skeletonised binarised image in which a 3×3 rectangular mask is created around each pixel inside the fingerprint image and the common of pixels is computed (Jain et al., 2000; Alibeigi et al., 2009; Maddala et al., 2010). The pixel is handled as a ridge termination minutia if the average value is less than 0.25 and bifurcation minutiae if the average is more than 0.75. Gamassi & Scotti (2005) developed a fingerprint minutiae extraction based on the examination of the local properties. In this paper, the fingerprint image minutiae are diagnosed by way of analyzing the intensity depth alongside squared paths in the image. It achieves good accuracy and it may be an amazing candidate to be carried out on easy hardware architectures, as an instance of biometric structures embedded in moveable or portable applications like cell phones. Alibeigi et al., (2009) further used this method and proposed a hardware scheme primarily based on the pipelined architecture for the identical work mentioned by Gamassi & Scotti (2005). Maddala et al., (2010) defined the implementation and assessment of an existing fingerprint identification device advanced by means of the National level wide institute with standards Technology usually abbreviated as NIST. The fingerprints are first contrast adjusted or filtered and enhanced and binarized. The binarized image is then scanned both horizontally and vertically the usage of a 2x3 pixel window size to identify ridge endings or terminations and bifurcations. A post-processing stage is used to decrease the number of fake minutiae.

#### 2.8.1.1. 2 Skeletonisation based Minutiae Extraction Method

Skeletonised technique of minutiae extraction is likewise called Skeletonisation-based minutiae extraction. Here again, pre-processing strategies are carried out to enhance or remove noise, the fingerprint image is segmented and binarized. The binarized image is then thinned using a set of rules that removes pixels from ridges until the ridges are one-pixel length (V. Espinosa, 2002). There are many methods available in the literature for skeletonization or thinning process (Ahmed & Ward, 2002; Patil et al., 2005; X. You, 2005). After extracting the minutiae from the improved, binarized and thinned image some post-processing is carried out on this final fingerprint image to take away any spurious minutiae. The techniques on this class are of types–crossing number based and morphology-based totally.

#### 2.8.1.1. 2.1 Crossing Number Based Thinned Minutiae Extraction Method

Crossing number wide variety based, which is the most extensively used technique of minutiae extraction inside the skeletonized binary image class. This method is ideal for different methods due to its computational performance and intrinsic simplicity. In this method, a skeleton image is used in which the ridge run pattern is considered as a window with a size of eight-connected. The nearby pixel of every ridge pixel in the image has scanned the usage of a 3×3 window from which the minutiae are extracted as shown in Figure 2.8. The crossing number may be used to categorize a ridge pixel as a finishing, bifurcation or non-minutiae point. As an example, a ridge pixel with a crossing-number of zero will correspond to an isolated factor and a crossing number of 4 correspond to a crossing factor..

| | | |
|---|---|---|
| P4 | P3 | P2 |
| P5 | P | P1 |
| P6 | P7 | P8 |

**Figure 2.8:** 3 × 3 neighborhood-crossing number

Jain et al., (1997) have additionally performed minutiae extraction with the need of the skeleton image. Their approach entails the usage of a 3x3 window to verify the nearby area of each ridge pixel within the image. A pixel is then categorized as a ridge finishing if it has most effective one neighboring ridge pixel within the image, and categorized as a bifurcation if it has 3 neighboring ridge pixels. Therefore, it can be seen that this approach is very much

like the crossing number technique. Properties of crossing number of skeletonisation are shown in Table 2.3.

**Table 2.3:** Properties of crossing number of Skeletonisation
(Source: Bansal et al., 2011)

| Crossing number | Property |
|---|---|
| 0 | Isolated point |
| 1 | Ridge ending point |
| 2 | Continuing ridge point |
| 3 | Bifurcation point |
| 4 | Crossing point |

Fake or false minutiae may be added to the image because of elements including noisy image, and image artifacts created by the thinning or Skeletonisation process. Subsequently, after the minutiae are extracted, it's far essential to do post-processing which will validate the minutiae. Few examples of false minutiae structures include the spur, hollow, triangle and spike systems (Xiao & Raafat, 1991). It could be seen that the spur shape generates false ridge endings; whereas both the hollow and triangle systems generate false bifurcations. The spike structure creates a fake bifurcation and a fake ridge finishing point.

The majority of the proposed work for image post processing-processing after thinning, in the literature (Xiao & Raafat, 1991; Zhao & Tang, 2007; Akram et al., 2008) are based on a series of structural policies used to discard spurious minutiae. For example, a ridge ending factor that is linked to a bifurcation point, and is below a sure or convinced threshold distance is removed. But, alternatively, then using a unique set of heuristics every time to do away with a unique kind of fake minutia, some processes include the validation of different varieties of minutiae right into a single algorithm. They verified the validity of each minutiae point by way of scanning the skeleton image and analyzing the local neighborhood across the minutiae. The algorithm is then able to cancel out fake or false minutiae primarily based on the configuration of the ridge pixels connected to the minutiae point.

Amengual et al., (1997) considered low-level features or minutiae points in order to extract features of the fingerprint image. For the description and retrieval of minutiae, they used already available varieties of minutiae extraction method or techniques by modifying a little bit. Farina et al., (1999) proposed set of algorithms for minutiae extraction from the fingerprint image.

Gnanasivam & Muttan (2010) proposed preprocessing techniques for filtering and noise removal of the image before extracting features from the image. The preprocessing is done to

acquire the vertical orientated fingerprint image followed through the center point of fingerprint pattern detection-core point and region of interest choice. Then characteristics extraction is performed in the extracted area of concern image.

Leung et al., (1991) proposed a neural network primarily based approach to minutiae extraction where preprocessing strategies are first carried out to clean or remove the noises and then binary ridge pattern is thinned or skeletonized. Before applying neural network approach skeleton is ready for feature extraction. In a later stage, a multilayer perceptron concept of three layers is trained to extract the minutiae from the skeletonized image of the fingerprint.

#### 2.8.1.1. 2.2 Morphology based Minutiae Extraction Method

The morphology-based minutiae extraction strategies are based on mathematical morphology (Humbe et al., 2007; Bansal et al., 2010) in which the image is pre-processed with a goal to reduce the overhead of post-processing filtering. The image is pre-processed with morphological operators to do away with spurs, bridges and so on (Bansal et al., 2010). After which the authentic minutiae are extracted through the morphological hit or miss rework to extract original minutiae. The morphological operators are forming operators which permit the manipulation of shapes for identity and also the composition of objects and item capabilities. Morphological operators are basic operators and their composition permits the natural manipulation of shapes for the identity and the composition of objects and object capabilities. The approach develops structuring factors for exceptional forms of minutiae found in a fingerprint image to be utilized by the HMT to extract legitimate minutiae. Ridge endings are those pixels in an image which have only one nearby point in a 3x3 neighborly located pixels or points.

#### 2.8.1.2 Minutiae Extraction from Greyscale images Method

Minutiae extraction from a directly grayscale image without converting to a binary image, even though continues to be being researched, there are some of the techniques to extract minutiae from grey scale fingerprint image without binarisation and Skeletonisation. This extraction method becoming important and popular due to following reasons

- An extremely good deal of statistics might be misplaced at some point of the binarization method.
- Binarisation and Skeletonisation are time ingesting procedures.
- Binarisation and Skeletonisation operations introduce a lot of spurious minutiae.

- The binarization techniques do no longer show to be mainly useful while implemented to low resolution or quality images.

**2.8.1.2.1 Minutiae Extraction by subsequent ridge flow lines**

Maio and Maltoni (1997, 1998 ) proposed methods on this technique is to without delay extract the minutiae from the grayscale image through following the ridge running lines with the assist of nearby orientation discipline. This method tries to locate a local or restricted maximum comparative to the cross-section orthogonal in the path of the ridge. Consider any one initial point as $Point_s(a_c, b_c)$ with local direction $\Phi_c$ with in the fingerprint image, another novel candidate point $Point_n(a_n, b_n)$ achieved by following the ridge flow along the $\Phi_c$ with already decided steps Ψ pixels from $Point_s(a_c, b_c)$. A novel section £ having the $Point_n(a_n, b_n)$ is orthogonal to $\Phi_c$ . The gray level intensity value of $\Phi_c$ becomes $Point_s(a_c, b_c)$ to start another following step. This method is iterated till all the minutiae are located. The surest value for the tracing or following step Ψ and phase period σ is chosen primarily based on the average width of ridge traces. Jiang et al., (2001) enhanced the method of Maio and Maltoni by preferring live tracing or following step Ψ with respect to modification ridge contrast and bending degree. A large step Ψ is utilized when the bending degree of the local ridge is minimal and intensity changes along the ridge path are small. Instead of following one ridge, liu et al. (2000) proposed following a central ridge and the two adjacent valleys simultaneously. In every section £ a central maximum and adjoining minima are positioned at every step, and the ridge following step Ψ is lively decided based on the distance among the lateral minima from the central most. Linear symmetry method is utilized to extract the fingerprint minutiae based on the notion that minutiae are confined discontinuities of the LS vector (Nilsson and Bigun (2001); Fronthaler et al (2005). Two varieties of symmetries - parabolic symmetry and linear symmetry are adapted to model and find the factors within the grey-scale image where there's loss of symmetry. Here 9 x 9 size window is used to find the symmetry noise filter response.

Gao et al proposed a minutia extraction method based totally on Gabor segment. Differing from most present strategies, the technique works in the transform area of the fingerprint image where, the picture is convolved by a Gabor filter out, resulting in a complicated image. It is then converted into the amplitude and phase part. A minutiae extractor then extracts minutiae immediately from the Gabor segment area. Ratha et al (1995) proposed a minutiae extraction algorithm in which the flow path of ridges is computed through viewing the

fingerprint image as a directional textured image. A ridge segmentation set of rules based on a waveform projection is then used to correctly locate the ridges and a thinned ridge image is obtained and smoothed the usage of morphological operators. Finally, the minutiae are extracted from the thinned ridges based on the range of crossings and a post-processing step implemented to take away spurious minutia.

#### 2.8.1.2.2 Fuzzy Techniques for minutiae extraction from a grayscale image

Some fuzzy strategies have also been recommended in literature to extract minutiae from grayscale images immediately. Sagar et al (1995, 1999) proposed that a grayscale picture consists of two, levels of gray pixels. The darker pixels constitute the ridges from one such stage. The lighter pixels, constituting the valleys and furrows form another such level. The usage of human linguistics, these stages of gray can be described as darkish and vivid levels correspondingly. With the help of using fuzzy logic, these two tiers are modeled and used together with suitable fuzzy policies to extract minutiae accurately. For this motive, rough line thinned structures for both ridges and valleys are obtained. Seeing that bifurcations may be visible as valley endings, the identical set of rules that determined ridge endings will be applied to decide valley endings. A 5x5 pixel check window is positioned at each factor of the road thinned shape. The average value of the 25 pixels is received.

### 2.8.2 Non-minutiae Based Matching

The non-minutiae based matching is classified as

- Global and local texture features of fingerprint
- Level 3 features of fingerprint

Global and local texture features are vital alternatives to minutiae-based matching. Textures are defined via spatial repetition of the basic factors and are characterized by way of properties inclusive of scale, orientation, frequency, symmetry. Fingerprint ridge strains are mainly described but smooth ridge orientation and frequency, besides at singular areas. Those singular areas are discontinuities in an essentially regular pattern and encompass the loops and deltas at a coarse resolution and the minutiae feature at a higher level. Global texture analysis fuses contributions from exclusive feature areas into a Global measurement and as a result, most of the available spatial statistics are lost. Local texture evaluation has proved to be extra powerful than international characteristic analysis (Jain et al., 1999).

Fusion methods that merge texture and minutiae characteristics have also been proposed (Nanni and Lumini, 2008). This method used nearby binary styles or Local Binary Pattern

(LBP) as fingerprint descriptors. In this device, two fingerprints to be matched are first aligned with the use of their minutiae, then the image decomposed in several overlapping sub-windows, each sub-window is convolved with a depository of Gabor filtering techniques and, eventually, the invariant nearby binary patterns histograms are extracted from the convolved image.

Nikam and Agarwal (2008) also used LBP functions along with wavelets for fingerprint detection. Neighbourhood binary sample (LBP) histograms are used to capture that textural information. Wavelet strength functions, characterizing ridge frequency and orientation records, are also used for improving the efficiency of the proposed technique. Dimensionalities of the function sets are decreased via going for walks sequential feature floating selection (SFFS).

Existing matching algorithms can be labeled into two categories, Global and Local feature-based totally algorithms. Global characteristics-based algorithms purpose at spotting an item as an entire. This class of a set of rules or heuristics is appropriate for the popularity of homogeneous (textureless) objects, which can be without difficulty segmented from the background image. Examples encompass Hu moments (Vuppala et al., 2007) and the eigenvectors of the covariance matrix of the segmented object (Lee et al., 2005). Global capabilities based totally recognizers are simple and rapid however there are obstacles in the reliability of object reputation under changes. In evaluation to this, local capabilities based algorithms are extraordinary suitable for textured objects and are more suitable with respect to changes. The benefits of local over global capabilities are demonstrated by means of Ke et al. (2004).

Neighbourhood features based algorithms cognizance mainly at the so-known as key points. On this context, the general scheme for object recognition generally involves three crucial stages: The primary one is the extraction of salient feature factors or characteristics (for instance corners) from both the test and model item mechanisms that purpose to keep the region characteristics insensitive to perspective and illumination changes. The final level is the matching between check (test) and model images, totally based on the extracted features.

The improvement of image matching by the usage of a fixed of local key points can be traced back to the work of Moravec (1977). He described the idea of point or region of interest as being distinct regions in pictures that can be used to locate matching regions in consecutive photo frames. The Moravec operator became in addition advanced by Harris and Stephens (1998) who made it more repeatable within small image dissimilarity and near edges. Their

new method is shown to outperform in natural or realistic images. Schmid and Mohr (1997) used Harris corners to reveal that invariant nearby capabilities matching can be prolonged to the general image popularity problem. They used a rotationally invariant descriptor for the local image regions to be able to allow characteristic matching below random orientation variations. Although it is rotational invariant, the Harris corner detector is but very responsive to modifications in image scale, and therefore, does not provide a terrific basis for matching images of different sizes.

### 2.8.3 Correlation based Matching

The correlation-based matching for healthy two fingerprints takes into account that the fingerprints are aligned and the correlation is computed for every corresponding pixel, however, because the displacement and rotation are unknown it is essential to apply the correlation for all possible alignments. The singularity statistics can be beneficial with a view to finding an approximated alignment. The main disadvantage of this method is its computational complexity and much less tolerance to non-linear distortion and assessment version. There had been a few opportunity proposals that compute the correlation locally or regionally instead of globally, wherein only interested regions (e.g., minutia and singularity regions) are decided on and coupled. These algorithms use simple strategies to align fingerprint images and subtract the entered or participation image from the template image to verify if the ridges correspond. This method has quite a few shortcomings.

It fails if the images are quite distorted. The distortion is extra pronounced in global fingerprint patterns; consequently thinking about the nearby areas or local patterns can limit distortion to some extent. Bazen et al., (2000) and Nandakumar and Jain (2004) present some techniques to localized correlation-based totally matching.

Another component that influences the overall performance of correlation-based totally matching algorithms is the discrepancy introduced through finger strain, pores and skin condition, image brightness, contrast and ridge thickness of the identical finger. When those conditions get up, a greater state-of-the-art correlation measures together with normalized pass-correlation or zero mean normalized -correlation are needed. Those strategies can be used to compensate evaluation and brightness changes and the enhancement, process binarisation, and thinning steps might also limit the ridge thickness problem (David et al., 2005).

Expanded complexity: This method introduces burden of computational complexity. This hassle can be solved via the usage of Fourier domain technique (Coetzee and Botha, 1993) and Fourier-Mellin transformation (Sujan and Mulqueen, 2002).

### 2.8. 4 Ridge Feature Based Matching

A matching the use of the ridge characteristic in shape of finger code consists of computing the difference of finger code vectors (query and reference). However, before making use of the finger code, it is essential to align the fingerprint images, which is clearly a large hassle, as in the case of different methods. In some cases, the singularity may be used for that motive. A finger code also can be used as a complementary to minutia based totally technique that allows you to enhance the overall matching accuracy. The original method of this method used round finger codes, considering as center the middle factor. The final result of the finger code distinction is normalized and averaged using the eight guidelines and received a value that varies from zero to one. The lower the score, the more comparable are the fingerprints. A few threshold values are used to determine whether or not there may be matching or no longer.

### 2.8.5 Hybrid Methods

These days, researchers have contributed to society hybrid fingerprint matches by means of using a couple of simple method to matching. For instance, Ross et al. (2003) have counseled the usage of each minutiae and ridge flow facts to represent and match fingerprints. They have revealed that the quality and efficiency of the minutia-based matcher offered by Jain et al. (1997) can be considerably progressed via using additional statistics provided through the finger code technique (Jain et al., 2000).

The neighborhood or local correlation-primarily based fingerprint matching set of rules offered in this paper is a similar attempt to improve the overall performance of a minutia-based totally matcher via introducing a correlation step to ascertain the high-quality of each minutia region. The gray-degree statistics of the pixels around the minutiae factors carries richer records about the nearby area than the attributes of the minutiae factors. For this reason, the spatial correlation of areas around corresponding minutiae factors is a superb measure of the diploma of similarity between them.

The correlation-primarily based fingerprint matcher proposed by way of Bazen et al., (2000) selects sure extraordinary areas inside the template fingerprint image and searches for the one's regions within the query image. However, their technique isn't very sturdy to the

rotation. Beleznai et al. (2001), that allows you to enhance the popularity overall performance of a minutia-based totally matching system, exploit the structural statistics around minutiae.

## 2.9 TEMPLATE PROTECTION SCHEMA

Commonly, all the profitable biometric systems shield the stored templates by using encrypting those using general cryptographic techniques. Either a public key cryptosystem like RSA (RSA laboratories, 1999) or a symmetric key cipher like AES (Advanced Encryption Standard, 2001) is usually used for template encryption. Considering that those cryptosystems are not unusual, they may be directly carried out to any biometric template and the encrypted templates are blanketed so long as the decryption secret is covered. But, encryption is now not a high-quality solution for biometric template protection because of few reasons. First, encryption isn't always an easy function and a small dissimilarity in the values of the function units extracted from the raw biometric records might direct to a very big difference within the resulting encrypted functions. Many acquisitions of the identical biometric features do no longer bring about the same function set. As a result, a biometric template cannot be saved in an encrypted shape after which perform matching within the encrypted area. Consequently, for every authentication, attempt (i) the template is decrypted, (ii) matching is accomplished between the query made by the user and decrypted template and (iii) the decrypted, and template is then removed from memory. For that reason, the template gets uncovered for the duration of all authentication aatempts. Secondly, the safety of the encryption scheme depends on the decryption key. Therefore, the decryption key must be securely stored in the machine and if the keys compromised, the template is not any extra comfortable. Because of these two reasons, well-known encryption algorithms alone are not sufficient for securing biometric templates and strategies that are designed completely to account for the intra-person variability in the biometric facts is needed. The template protection schemes mentioned in diverse literature can be widely classified into categories, namely, Feature transformation technique and Biometric cryptosystem as shown in Figure 2.9.

### 2.9.1 Feature Transform

In function transformation method, a transformation function (FN) is carried out to the biometric template (TE) and only the converted template (FN (TE; R)) is stored inside the database. The parameters of the transformation function are usually derived from a random

key (R) or a password. The identical transformation function is implemented to query characteristic (QE) and the transformed or altered query (FN (TE; R)) is at once matched with the altered or transformed template (FN (TE; R)). Relying on the characteristics of the transformation function FN, the feature remodels scheme can be classified as salting or non-invertible transform.

In salting, F is invertible, means if an intruder gains access to the key, the intruder can recover the biometric template easily. For this reason, the safety of the salting scheme is primarily based on the secrecy of the key or password. On the other hand, non-invertible transformation schemes commonly follow a one-way function at the template and very computationally hard to invert right into an initial template even if the secret is recognized.

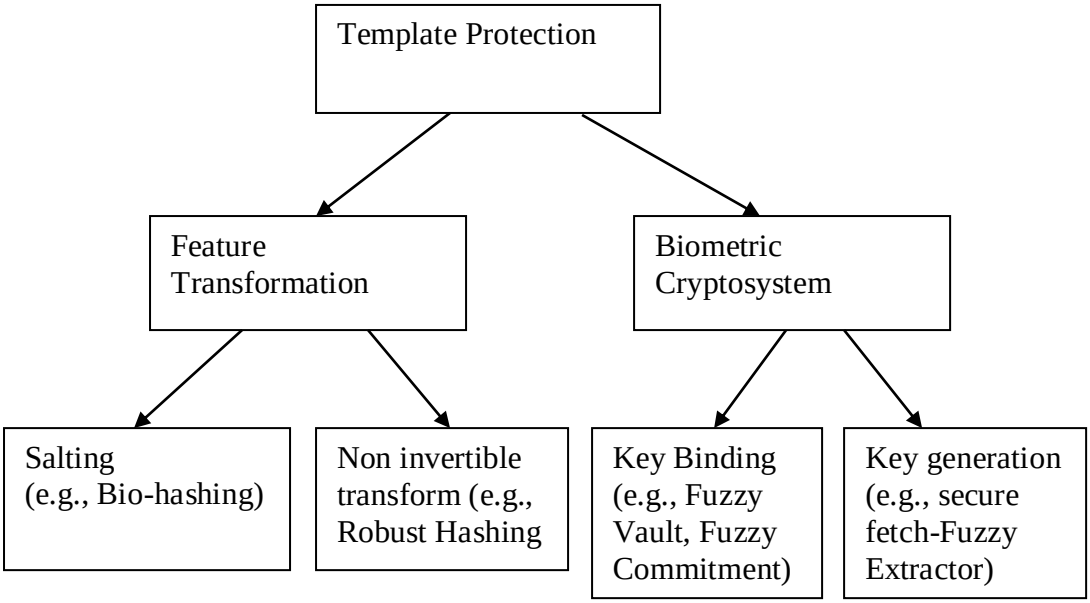



**Figure 2.9:** Template Protection Schema (Source: Jain, Nandakumar, and Nagar, 2008).

### 2.9.2 Biometric Cryptosystems

Biometric cryptosystems (Cavoukian and Stoianov, 2007 and Uludag et al., 2004) have been originally developed for the reason of either securing a cryptographic key using a biometric function or for at once producing a cryptographic key from biometric functions. But, they can also be used as template protection mechanisms. In a biometric cryptosystem, a few public statistics about the biometric template is saved. Such public information or facts is commonly known as helper data and hence, biometric cryptosystems also are known as helper information-primarily based methods (Vetro and Memon, 2007). The helper records do not screen any sizable information approximately the initial or original authentic biometric

template, it is far wished in the course of matching to extract a cryptographic key from the query biometric functions. Matching is carried out indirectly by way of verifying the validity of the extracted key. Each error or fault correction coding techniques are normally used to address intra-user variations. Biometric cryptosystems may be further categorized as key binding or key era systems relying on how the helper information is obtained. While the helper records are acquired via binding a key (that is impartial of the biometric capabilities) with the biometric template, it is far called a key-binding biometric cryptosystem. Even when simplest the helper data, it's far computationally tough to get better both the key and the original template. Matching in a key binding machine entails recovery of the key from the helper statistics using the query biometric features. If the helper data are derived simplest from the biometric template and the cryptographic key's directly generated from the helper statistics and the query biometric functions, it results in a key generation biometric cryptosystem.

A number of template protection strategies like fuzzy commitment (Juels and Wattenberg 1999), fuzzy vault (Juels and Sudan 2002), protecting functions (Tuyls et al., 2005) and distributed supply coding (Draper, 2007) can be considered as the key binding biometric cryptosystem. Different schemes for securing biometric templates along with those positioned forth in (Davida et al., 1999, Hao et al 2006, Kelkboom et al., 2007, Connie et al., 2005) also fall under this class.

### 2.9.3 Fingerprint Hash Function

One of the important challenges in biometric identification or verification system is keeping the biometric data or template safe and secure. A hash function is usually transformed functions, which converts or transform data or features from one form to another. Always transform function should be a one-way function or another way it should not be invertible. Tulyakov et al., 2005 proposed symmetric hash function for the biometric fingerprint. They proposed some hash function, which is independent of the order in which input is presented to the system or invariant to translation and rotation. They used the complex function in order to transform fingerprint features to another form. Tulyakov et al., 2005 used hash functions for ‘n’ fingerprint minutiae features. In literature, few methods are already proposed by different researchers for building cancellable biometric template. In this regard, there are mainly two techniques, out of which one is error correcting code and another one is noninvertible transformation. In error correcting code, it is assumed that biometric

fingerprint of the same person having little changes or variations and this variation can be corrected using error correcting code. And only error correcting data and cryptographic hash function of the original template is kept for recognition or matching purpose. This method is not efficient for the fingerprint. On the other hand, noninvertible transform functions are more convenient and efficient in case of fingerprint biometrics. All most all researchers related to Hash function considers n number of hashes and if it is used for full security purpose then it should translation and rotation invariant.

## 2.10 RESEARCH GAP

The research gap helps to understand the study made or available at present in respective field or area and which also helps to improve the existing system towards an ideal or standard system. In literature, many studies are available which addresses the problem of template protection. In literature, enough studies are available that throws light or insight on Fingerprint Template protection using Fingerprint Hash code. All the research study focuses on translation, rotation, and rarely scaling invariant models. Most of the attacks for fingerprint image occur either in the network, at the time of transmission or in the template or database, which is not under the control of the user. User level security is having direct control in the hand of the user. User level security can be further improved using proper education and training. Some of the following research questions are not been well answered in the literature and a true attempt is made in this research work to answer these questions.

- When fingerprints are easily mimicable, what is the use of developing Hash code Translation and Rotation or orientation change invariant?
- Is it possible to compare and match fingerprint with only one Hash code stored in the database?
- Is there any possibility of using a fingerprint as identity-key or index-key with the aid of Hash code, without capturing through sensors every time, by considering the image captured at the beginning or onetime only (using a static image of the fingerprint)?
- What are the multiple methods of fingerprint feature or minutiae extraction for developing Fingerprint Hash code, which is Translation, Rotation, and Scaling variant?
- Is there any difference in developing fingerprint Hash Code using fingerprint image skeletonization and non-skeletonisation process?

- Is there any difference in applying and not applying fingerprint skeleton post-processing technique while generating Fingerprint Hash Code?
- Does fingerprint alone is secured in case of secure Authentication process? If no, how to combine Password and OTP along with fingerprint Hash code as Multifactor Authentication tool?
- Is it possible to improve the revocability of fingerprint biometrics Hash code?
- Is the Multifactor Authentication Model is able to achieve few characteristics of ideal authentication system?

## 2.11 CHAPTER SUMMARY

The review of the literature reveals that the fingerprint identification is one of the oldest and popular approaches within the biometric recognition system. In relation to the research study, the review examines also reveals the fact that even though numerous achievement are posted with relation to fingerprint reputation and recognition, there are a not enough robust techniques in connection with template protection.

Even though biometric structures provide a number of functionalities such as verification, fantastic identification, and screening, those structures are not perfect, due to factors like intra-consumer or user variations and inter-person similarity, the mistake or failure rates related to biometric structures is non-zero. So it's essential and necessary to develop noninvertible, revocable and highly robust biometric templates. Advances in cryptographic and hashing techniques can be efficiently used to make the biometric system more secure and robust.

To improve the security of template, fingerprint biometric details, the research work proposes hashing techniques based on existing MD5 hashing technique. If the intruder gets this hash code, it is nonreversible or in any circumstances intruder not able to get original fingerprint template. Modern Research also reveals that fingerprint alone is not sufficient for full security purpose, but it can work well as one of the factors in multifactor authentication model.

**********

# CHAPTER THREE

# *Methodology and Fingerprint Image Preprocessing Techniques*

**Contents** **Page No.**

## 3.1 INTRODUCTION

Automatic Fingerprint Identification System (AFIS) contain the use of automatically and reliably enhance the image, reduce the noise and extract the minutiae features from the biometric images of the fingerprint. The performance of a minutiae extraction principle relies heavily on the pleasant quality of the input biometric image. Most of the fingerprint recognition systems result in poor matching due to impurity or noisy images. With an intention to improve the performance of Automated Biometric Identification/Verification System, it is essential to incorporate a biometric preprocessing process prior to minutiae feature extraction.

Fingerprint recognition system utilizes two types datasets called as training data set and test datasets. The training dataset is used for training purpose, initially, the fingerprint image is preprocessed and enhanced and later features are extracted and stored as a template. In test datasets, the same process is repeated but the template is not stored and just compared with the already stored template and matching score is calculated by utilizing an automated computer system. The stored features are compared for one to one match called verification and one-to-many called as identification.

Reliable authentication of the fingerprint image is a growing stressful service in many fields, not only in police and crime or legal environments but also in civilian programs, which include access control or economic transactions. It could additionally be understood from the literature survey that even though many recognition techniques were devised, none of the techniques proposed is a 100% secure and accurate. As a consequence, it's far clear that advancements are required in the field of template protection or there is the necessity of a change of set rules or methods in fingerprint matching process.

Initially enrolled fingerprint image is preprocessed prior to feature extraction process and consists of series of the process like filtering, enhancement, binarization, segmentation and thinning. Filtering is part of the noise filtering or smoothing process, which is essential in automatic fingerprint identification or recognition systems to get higher efficiency. Enhancement process uses either filtering technique or some other techniques on the binarized image or direct grayscale image to further remove the noise. These two processes sometimes merged and considered as a single step. Prior to the segmentation process, the fingerprint image is converted to binary form, which is referred as binarization. The purpose of binarisation is to remove the background or noise associated with the input image. Fingerprint segmentation is the one of the main process involved in fingerprint pre-

processing and it refers to the process of dividing or separating the image into two disjoint regions as the foreground and background. Thinning or skeletonization is the special process, which reduces the width or thickness of the ridge pattern to single pixel width.

### 3.2 OBJECTIVES OF THE RESEARCH

The most of the research work in fingerprint identification system fails to provide template protection with main characteristics like revocability, diversity, non-invertible, and permanence. Most of the fingerprint identification algorithms or techniques are not able to match or recognize partial fingerprints. These two are the motivation for this study. The main objective of this research is;

- To study multiple methods of Fingerprint Hash code generation based on MD5 Algorithm using modified filtering techniques and minutiae details and the extracted feature are unique features of the fingerprint such that there are no collisions in hash code.
- To propose an alternative approach for User Authentication using Multifactor, which includes, Fingerprint Hash code, Password and time synchronized One Time Password (OTP) based on different methods used in this research study.

The sub-objectives of this research work include the study of six methods, which are mentioned below.

- To Study, a Fingerprint Hash code using a different process like Preprocessing, Thinning and Minutiae Extraction, and Minutiae table formation and generating Hash code from these minutiae table (Method-1).
- To Study a Fingerprint Hash code using Gabor filter which includes techniques like Contrast adjustment filtering, Binarisation, Segmentation and generating Hash code from the Gabor filtering details (Method-2).
- To Study a Fingerprint Hash code using Gabor filter with techniques like Binarisation, and Segmentation and without including Contrast adjustment (Method-3).
- To Generate a Fingerprint Hash code as like Method-1 but without storing its location or pixel positions while forming Minutiae Table (Method-4).
- To Produce a Fingerprint Hash code using Freeman chain code and its first difference value for every 8-connected boundary points by making use of different process like enhancement and binarisation (Method-5).

- To Study a Fingerprint Hash code generation using Euclidean distance value by making use of different process like enhancement and binarisation (Method-6).
- To study and analyze Fingerprint Hash code, OTP, and Password-based Multifactor Authentication Model using ABCD Analysis Framework and also compare this new model with existing almost similar systems.

Finally to evaluate the performance of Hash code generation using all fingerprint recognition performance evaluation matrices and to ensure that all these methods generate unique Hash code for even different fingers of the same person using FVC ongoing 2002 benchmark datasets.

### 3.3 SCOPE OF THE RESEARCH

As the biometric features are utilized for a few security-related applications because of its uniqueness, can't be shared, replicated, lost and safe to physical attacks. The framework is extremely classified and it gives a safe kind of recognizable proof to each client. So the framework is utilized as a part of high-security applications over the world.

The secured fingerprint recognition system can be used for various different identification and verification purposes in diverse applications. The different application that makes use fingerprint biometrics is as follows.

- Attendance maintenance
- Entry control system
- Mobile banking services
- Authenticate purchases
- Checkout payment
- Login control for Apps as a replacement for password
- Manages and organizes password using password manager
- Integration of smartphone functions

The major application of this research work is in a client-server model, which makes use of mobile or computer technology in authentication procedure. The biometric sensors or reader used in mobile phones are very poor in terms of capturing fingerprint minutiae or simply features. The fingerprints captured through mobile sensors are having huge noise and which makes difference in hash code. So if we use dynamic fingerprint, at the time of authentication request, verification or identification is not accomplished. Fingerprint Hash code is used as an identity element or key in the authentication request. Its only half secured. The different

applications which can be benefited by Multifactor authentication with Fingerprint Hash code, Password and OTP are following.

- Mobile Banking services
- Internet banking services
- Mobile-based any financial transactions
- E-shopping websites

## 3.4 PROPOSED METHODOLOGIES

The proposed work is implemented using MATLAB2015a. FVC ongoing 2002 benchmark dataset is used for training and test purpose. To develop the proposed fingerprint recognition system based on modified filtering and Minutiae Table various techniques and algorithms are combined and the methodology consists of the following steps and which is shown using Figure 3.1.

**Method-1:**

This is the main Method of this study. Other studies are subsidiary methods which are obtained by removing or adding few techniques.

1. *Preprocessing Phase*: Raw fingerprint image of FVC ongoing 2002 dataset is input for this phase and this input image, initially filtered using τ-tuning based contrast adjustment method. Filtering is used for removing noise from the input image, whereas enhancement is applied to improve contrast and enhancing fingerprint pattern
2. *Segmentation Phase:* Segmentation consists of approaches or algorithms which separates foreground or Region of Interest (ROI) from the background image. ROI is ridge and valley structure of fingerprint or simply real fingerprint structure. For segmentation, in this research work surfeit clipping method is utilized.
3. *Skeletonization Phase*: This is actually further extension of preprocessing phase. Here the output of the segmented image is converted into fingerprint skeleton using the edge prediction based method. Skeleton image is obtained by doing series of operation, which includes preprocessing, segmentation, and binarization.
4. *Minutiae Identification and Extraction Phase*: The skeleton image is again processed with the aid of crossing number based method, which considers eight windows of the ridge flow pattern. This processing is done here again on skeleton and minutiae table to remove background region which is located either outside the foreground or within it. Here ridge ending and ridge bifurcation are considered as minutiae. Again after

extracting minutiae its post-processed to remove spurious minutiae. The minutiae table consists of four columns, which stores ridge ending, ridge bifurcation, and crossing number and some of first three columns. Finally, in this phase feature are extracted in a format which is easily convertible into hash code by adding salt to hash code in order to make hash harder, which is hard to decrypt.

5. *Hash code creation Phase*: The extracted features are combined and hash code is generated using MD5 hashing technique. The MD5 hash algorithm generates 32-bit long hash code. The goal is to perform key for identification by simultaneously hiding or keeping the fingerprint information secretly or noninvertible way. Even though fingerprint is compromised intruder should not get original features of the fingerprint image.
6. *Hash Matching Phase*: Hash code is stored in the database. Here WampServer is used for database construction. In WampServer MYSQL database package is utilized for creating database and table. Here two process are involved one is training process and test process. For training purpose FVC ongoing 2002 benchmark dataset is considered and trained and finally stored in database table. As a test sample, one fingerprint image is considered and all the six phases are repeated and finally hash code is compared against already stored hashed code of database.

Each of the phases is dealt separately and usually, the output of one phase acts as an input for next phase. The entire approach is tested using different performance evaluation matrices, which includes, False Match Rate (FMR), False Non Match Rate (FNMR), Receiver Operating Characteristic (ROC), Equal Error Rate (EER), Failure to Enroll Rate (FTER), Failure to Capture Rate (FTCR) and respose time. In this research work, many existing techniques are combined and one alternative approach is proposed for filtering.

There are another five methods are proposed for Fingerprint hash generation, which varies in terms of few procedures and methods. But all these methods produce exact matching or similar hash code for static or already taken and preserved fingerprint image. These Hash codes are having applications in authentication as one factor for identity purpose and can be used to know whether any files or images are altered.

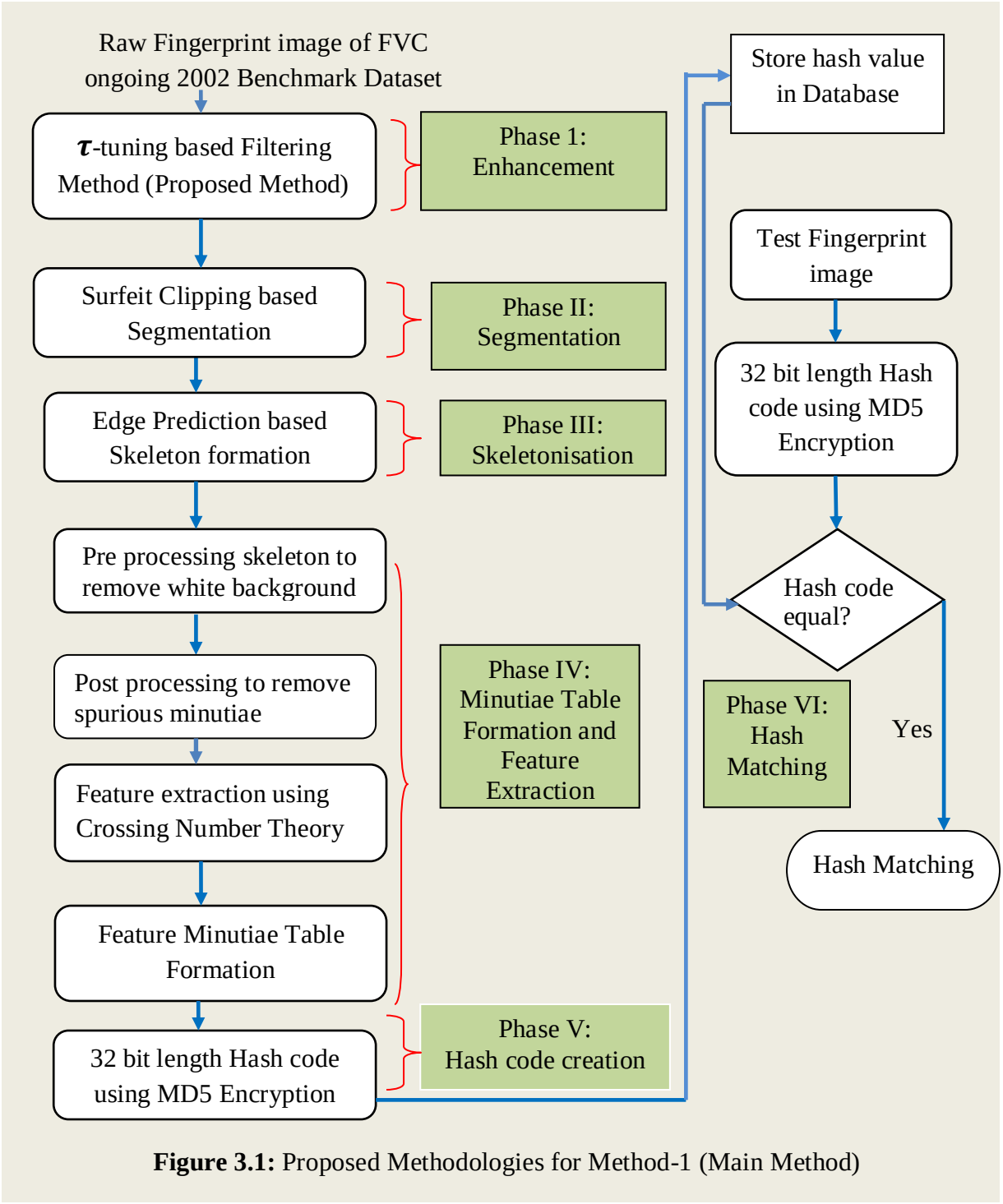



**Figure 3.1:** Proposed Methodologies for Method-1 (Main Method)

**Method-2:**

This is almost similar to Method-1 in terms of first few steps, from first step-enhancement to segmentation. Unlike Method-1, here thinning or skeletonization process is not performed. Instead of that from the segmented image fingerprint features are extracted using Gabor filtering techniques and finally, Hash code is generated using an MD5 hash algorithm like Method-1. The methodologies of this method are shown in Figure 3.2

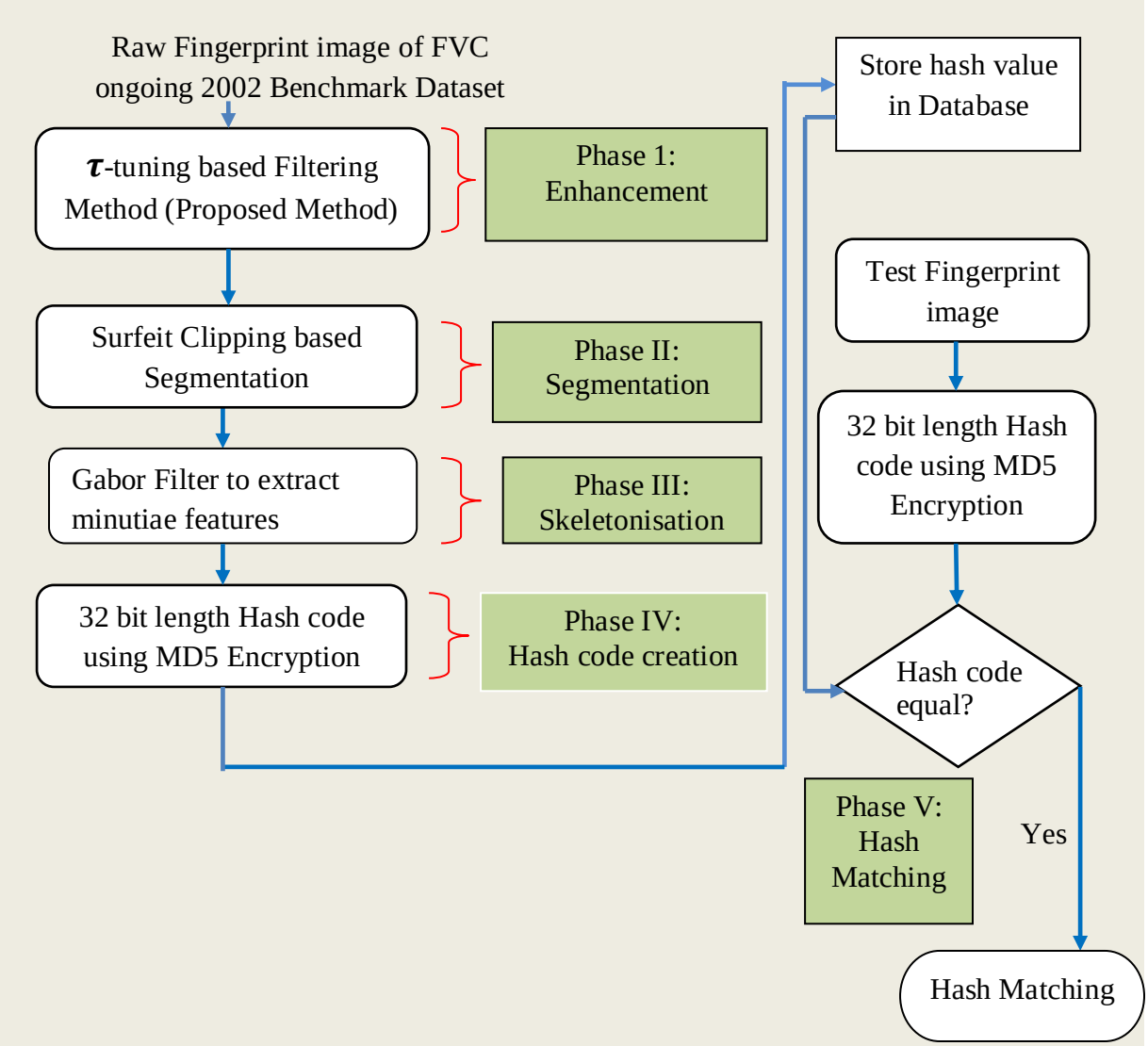



**Figure 3.2:** Proposed Methodologies for Method-2

**Method-3:**

This method is exactly similar to Method-2, but here initial Contrast Adjustment filtering and conversion of the image from integer data type to double type is discarded or ruled out. Like Method-2 here also fingerprint features are extracted using Gabor filtering techniques and finally Hash code is generated using an MD5 hash algorithm like Method-2. Due the elimination of two steps compare to Method-2, this will be faster than Method-2. The minutiae features are extracted directly from the segmented image with the help of Gabor filtering technique. The methodologies of this method are shown in Figure 3.3.

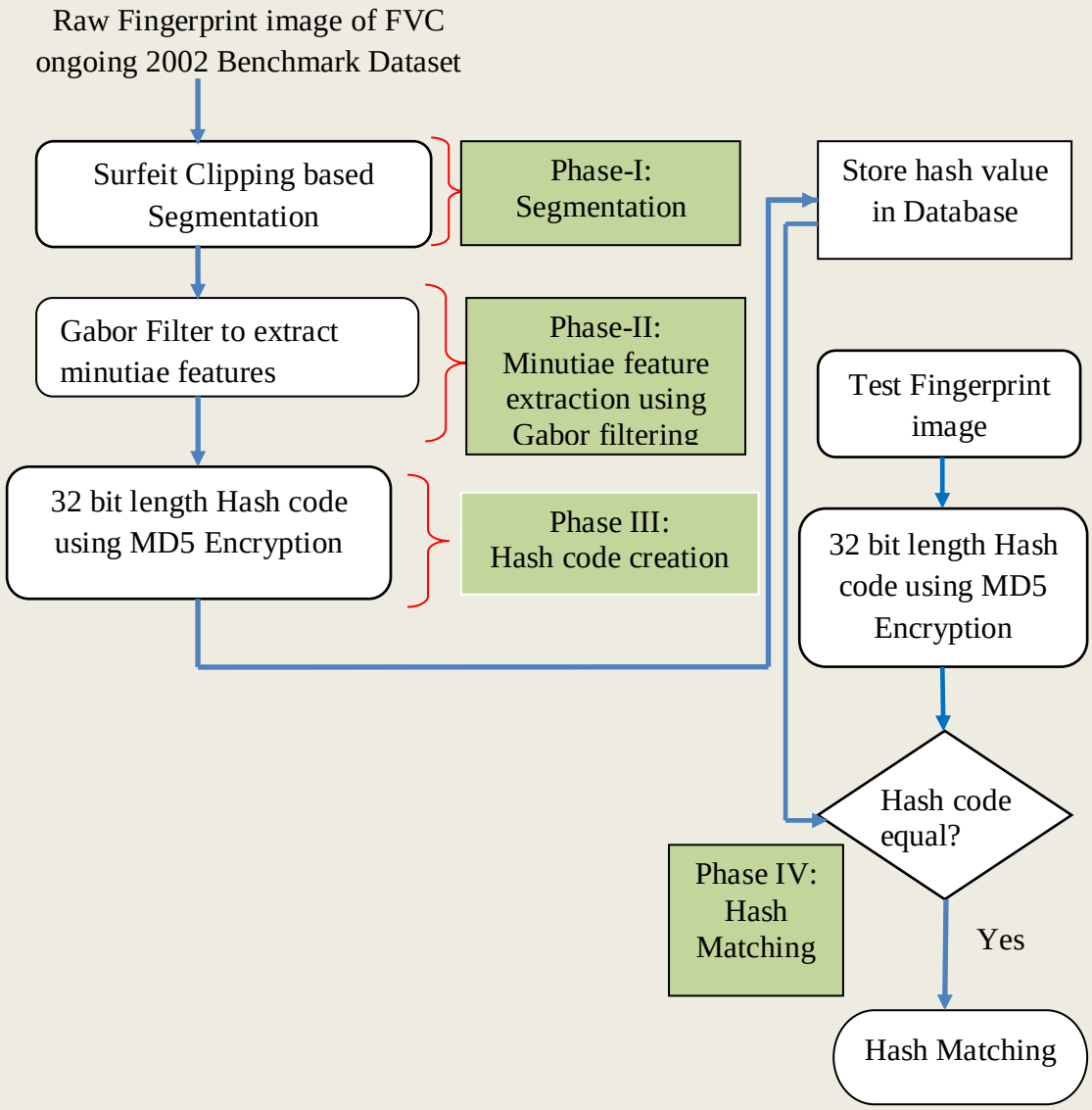



**Figure 3.3:** Proposed Methodologies for Method-3

**Method-4:**

This method is almost similar to Method-1. In Method-1 we extract the ridge ending and bifurcation along with its location details. The location details are nothing but pixel position in the pre-processed thinned image. Here we skip post processing because in fingerprint hash code post-processing does not affect the performance of matching efficiency. The different techniques involved in Method-4 are depicted in Figure 3.4

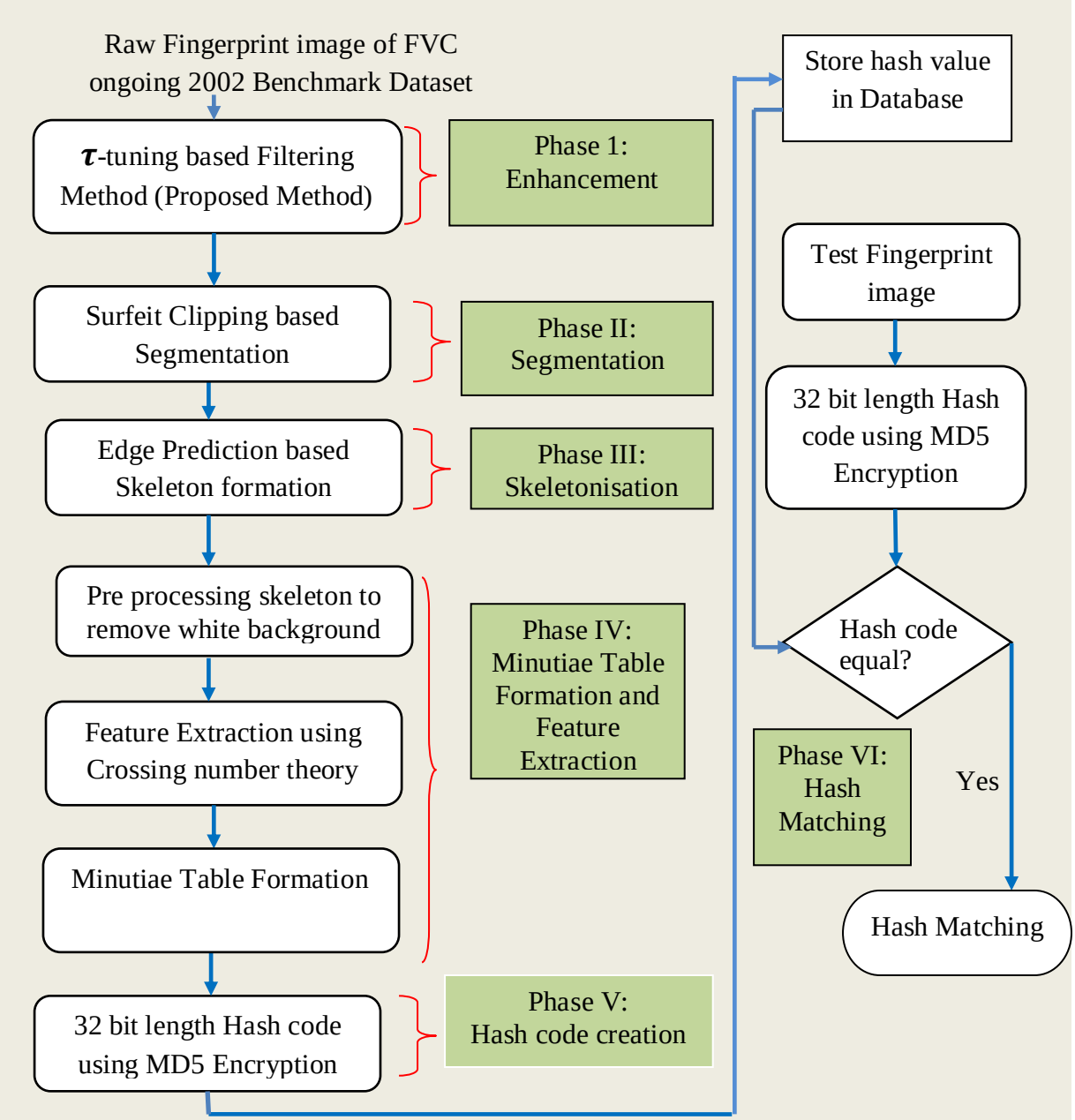



**Figure 3.4: Proposed Methodologies for Method-4**

**Method-5:**

Method-5 is based on Freeman chain coding. Freeman chain code extracts all possible boundaries for an image. Which gives starting x and y positions as x0 and y0. This works based on 8 or 4 connected points with respect to a central pixel. The 8 points are represented from 0 to 7 with is a particular format. In order to generate Hash code, we use x0 and y0 position and chain code value for all boundaries of the image. These values are unique to each fingerprint. This method makes use of segmentation process. This method is invariant to

translation. If we translate the image also hash code does not change. Initially, the fingerprint is resized to 256 × 256 sized images and then normalized. Figure 3.5 shows methodologies used in Method-5.

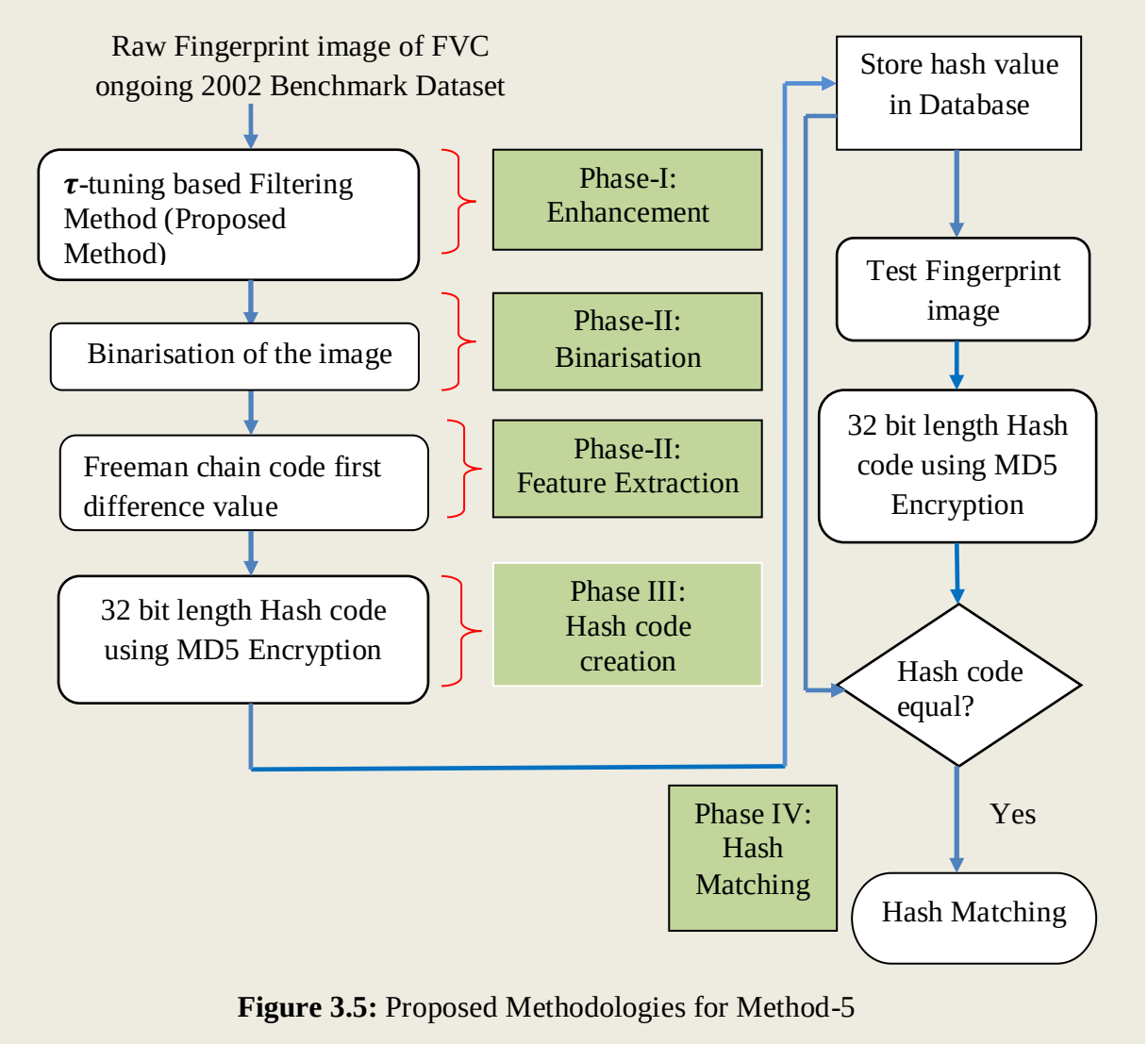



**Figure 3.5:** Proposed Methodologies for Method-5

**Method-6:**

Method-6 is based on Euclidean distance matrices of a binary image. In this, it calculates distance from each pixel to its nearest neighbor pixel with value 1 or not equal to zero. The unique distance value, mean and standard deviation are combined to form hash code. This method also makes use of segmentation process.

Euclidean distance is distance as like measured on a scale from every pixel to next nearest neighbor pixel with value 1. It is effectively used in the binary image. The binary image contains only bi values or two-pixel values as 1 or 0. The different processes used in this Method are as follows and which is depicted in Figure 3.6. Fingerprint image enhancement through contrast adjustment with the aid of proposed $\tau$-tuning based Filtering Method

- Binarisation of the fingerprint image
- Euclidean distance for binary image
- Finding unique values of Euclidean distance without any repetition or duplication

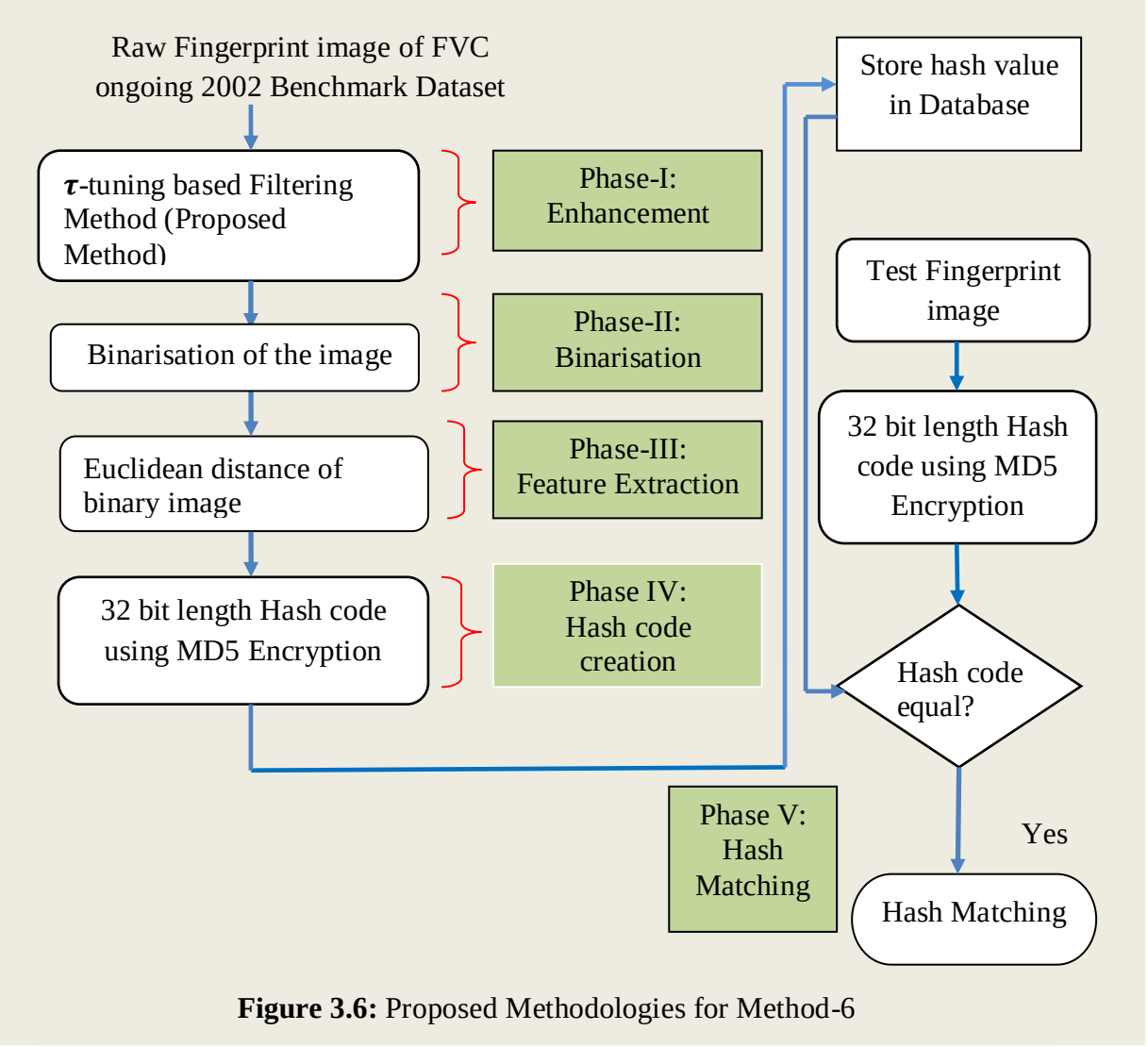



**Figure 3.6:** Proposed Methodologies for Method-6

### 3.5 FILTERING THE CONTRAST AND BRIGHTNESS OF FINGERPRINT IMAGE

In Filtering contrast, brightness and normalization of the image are performed with an ultimate goal to remove or reduce the noise to a maximum extent. Contrast and Brightness are two major factors, which affect the superiority of an image for easy or stainless or pleasant viewing (Krishn Prasad K., & Aithal P. S., 2017f). Overall lighting condition and darkness condition of the image collectively called brightness, whereas differences in brightness or intensity range between the low and high-intensity value of an image are called as contrast. Equalization through Histogram (HE) is a very famous approach for image contrast adjustment or enhancement in image processing. In general, the histogram

equalization distributes pixel values consistently and produces an outcome in a superior image with the linear increasing histogram. Some useful applications of HE enhancement consist of scientific image processing, speech recognition, fingerprint identification and texture synthesis, which might be typically employed with histogram adjustment (Wahab et al., 1998; Pizer, S. M., 2003; Pei et al., 2004; De et al., 2005).

Fingerprint enhancement can be performed on both binary ridge images and grayscale images. The binarization process may cause lack of information approximately the true ridge structure and it has inherent boundaries (Hong et al., 1998). In literature, many types of techniques are available for image enhancement which directly makes use of grayscale images of fingerprint assuming that the local ridge frequency and orientation may be reliably envisioned (O'Gorman & Nickerson, 1989; Sherlock, 1994). But, this assumption is not legitimate for poor quality fingerprint image, and other composition techniques like Gabor filters are used to input fingerprint image, which can gain reliable orientation estimation even for the corrupted image but they are computationally expensive (Hong et al., 1996; Hong et al., 1998).

Different techniques of making use of histogram equalization are determined in the literature. Global histogram equalization or GHE (Gonzalez & Woods, 2002) makes use of the entire information of the input image to map into new distinct intensity levels of the image. Although this Global technique is suitable for ordinary or general enhancement, it fails to consider with the local brightness capabilities of the entered image. The gray ranges with very excessive frequencies (wide variety of occurrences) dominate over the opposite gray levels having decrease frequencies in an image. In any such situation, GHE remaps the gray levels in a way that the contrast stretching turns into confined in some dominating gray levels having large image histogram components, and it causes sizable contrast loss for other small ones. Local histogram equalization (LHE) can overcome the problem encountered in GHE (Gonzalez & Woods, 2002). LHE uses a small window that slides on all pixel of the image sequentially and handiest the block of pixels that fall within this window are taken into consideration for HE and then gray level mapping for enhancement is carried out for the center pixel of that window. Therefore, it may make splendid use of local information also. But, LHE requires excessive computational cost and occasionally reasons over enhancement in some part of the image. Another shortfall of this approach is that it also enhances the noises inside the input image. To overcome the problem of high computational cost one more approach is to use the non-overlapping block for HE (Gonzalez & Woods, 2002; Krishna

Prasad K., & Aithal P. S., 2017f). But almost all times this method produces checkboard effect. Mean preserving bi-histogram equalization (MPBHE) proposed to get rid of the brightness problem issues (Kim, 1997; Xu et al., 2013). MPBHE separates the entered or captured input image or video histogram into two classifications as mean of the input before equalizing them independently. Some other variants of bi-histogram equalization are a similar area or equal area or place dualistic sub-image or picture histogram equalization or DSIHE (Chen& Ramli, 2003a) minimum or lower mean brightness or luminance error bi-histogram equalization (MMBEBHE) [19-20]. DSIHE (Wahab et al., 1998) technique uses entropy value for histogram separation. MMBEBHE (Chen& Ramli, 2003a; Chen& Ramli, 2003b) is the extension of BBHE technique that offers maximal brightness maintenance. Even though these strategies can carry out exact contrast adjustments, additionally they generate some side effects depending on the variation of gray level distribution in the histogram (Chi et al., 2005). Recursively Separating the mean and finding histogram Equalization (RMSHE) another up gradation of BHE (Chen& Ramli, 2003a) however, it additionally is not free from drawbacks. Moreover, such strategies won't ensure desirable upgrades of all of the partitions (Ziaei et al., 2008). The difference in the ranges of upgrades of various components might also create undesired artifacts in the image. There are many variations, MPBHE (Jagatheeswari et al., 2009), Recursive Separated and Weighted HE (RSWHE), Multipeak HE or MPHE (Wongsritong et al., 1998), Brightness preserving Weight Clustering HE (BPWCHE) (Sengee & Choi, 2008), Brightness preserving Dynamic HE or BPDHE (Ibrahim & Kong, 2011) and HE with Range Offset or HERO (Ibrahim, 2011; Abdullah, 2012).

In Global Histogram Equalization, Suppose that an image k (x, y) consists of distinct gray levels in the range of [0, R-1]. The transformation function T ($d_k$) is defined as

$$G_k = \mathrm{T}(d_k) = \sum_{j=0}^{l} \mathrm{P}(d_j) = \sum_{j=0}^{l} \frac{m_i}{m}$$

Where $0 \leq Gk \leq 1$ and l=0, 1, 2 ...R-l. In above function, $m_i$ depicts the count of pixels having gray level $d_k$, m is the maximum count of pixels in the entered image and P ($d_j$) correspond to Probability Density Function (PDF) of the input $d_j$. The cumulative density function here referred as T ($d_k$). $G_k$, is a mapping function, which maps to a dynamic range of [0, R-1] values by multiplying it with R-1.

In 256 × 256 sized gray scale images Transfer function value of $G_k$ is $0 \leq G_k \leq 255$ where l can take distinct 256 values from zero to 255 and a maximal number of pixels are 65536 (256 × 256). $G_k$, is a mapping function, which maps to a dynamic range of [0, 255] values by multiplying it by 255. GHE typically offers a good image enhancement, but sometimes ends

up with some artifacts and unwanted aspect results along with the washed out look. In $G_k$ , larger values of $m_i$ purpose the respective gray levels to be mapped aside from every different that guarantees precise enhancement.

### 3.6 IMAGE ENHANCEMENT- $\tau$ -TUNING BASED FILTERING ALGORITHM (PROPOSED METHOD)

The input for this algorithm is row image referred as I, and final output will be I_filter. Initially, the maximum intensity value of the image is found (Krishna Prasad, K., & Aithal P. S., 2018a). We consider here 256 × 256 sized grayscale image. If the input fingerprint image is greater than this size then it will be converted into 256 × 256 sized grayscale images. The maximum intensity value in a 256 × 256 sized grayscale image is 255. The range of values is 0 to 255, which means that minimum value is 0 and the maximum value is 255. The maximum intensity value of the image is represented as max (I). Each pixel intensity value is compared with max (I). If the pixel value is equal to max (I), then that pixel is assigned to $\rho_{max}$. The $\rho_{max}$, is an individual count of maximum intensity value. The total count of $\rho_{max}$ is represented using lower case delta symbol $\delta_{max}$ and is calculated as follows using eqs. (3.1).

$$\delta_{max} = \frac{\sum \rho_{max}}{R \times C} \quad \text{----------} \quad (3.1)$$

Where R, and C, are the total number of rows and columns respectively. $\sum \rho_{max}$, indicates all pixels, whose intensity value is equal to the maximum intensity value of the grayscale fingerprint image (I). Next minimum intensity values of the grayscale image are found and are referred as min (I). If pixel value is equal to min (I), then that pixel is assigned to $\rho_{min}$. The $\rho_{min}$, is individual count of the minimum intensity value of the image. The total count of $\rho_{min}$ is represented using lower case delta symbol $\delta_{min}$ and is calculated as follows using eqs. (3.2).

$$\delta_{min} = \frac{\sum \rho_{min}}{R \times C} \quad \text{----------} \quad (3.2)$$

As like Eq. 3.1, R, and C is the total number of rows and columns respectively. $\sum \rho_{min}$, indicates all pixels, whose intensity value is equal to intensity value of the grayscale fingerprint image (I).

Each row of the intensity matrix of the image is considered as a window and is represented as $\delta_w$, which is expressed using eqs. (3.3).

$$\delta_w = \delta_{max}\left(\frac{\delta(l)-\delta_{min}}{\delta_{max}-\delta_{min}}\right)^{\epsilon} \quad \text{---------- (3.3)}$$

Where $\epsilon$ value is 0.5, which is a constant. $\delta(l)$ is the low or minimum value of each row. The difference value of $\delta(l) - \delta_{min}$ is divided by $\delta_{max} - \delta_{min}$. The quotient is multiplied by $\delta_{max}$.

$\partial_w$ which is almost equal to Histogram equalization, cumulative density function, of window l is represented using 'tho' or partial derivative symbol and is defined using eqs. (3.4).

$$\partial_w = \sum_{l=0}^{l_{max}} \frac{\delta_w(l)}{\sum \delta_w} \quad \text{---------- (3.4)}$$

Where $\sum \delta_w$ represents summation value of all window l or summation of $\delta_w$. $\sum \delta_w$ is calculated as follows using eqs. (3.5).

$$\sum \delta_w = \sum_{l=0}^{l_{max}} \delta_w(l) \quad \text{---------- (3.5)}$$

The final output of this proposed algorithm ($I_{filter}$ ) is obtained using eqs. (3.6).

$$I_{filter} = (l_{max} \times (\frac{I(i,j)}{l_{max}}))^{\tau} \text{---------- (3.6)}$$

In the eqs. (3.6), tau ( $\tau$ ) is an important value, which filters or maps input pixel intensity value to new intensity value in the output image and is defined using eqs. (3.7).

$$\tau = round(1 - \max((\partial_w(:))) \text{---------- (3.7)}$$

The eqs. (3.7) is rounded to 6 decimal points to get higher precision or accuracy.

The output of the tuning based algorithm (proposed method), $I_{filter}$ is converted from grayscale 256 × 256 uint8 to double type for the purpose of grayscale image adjustment. The 256 × 256 double image consists of only two intensity values as 0 and 1. 0 represents dark and 1 represents bright or 0 dark black and 1 bright white. Here in image enhancement we focus more on $\tau$ - Tuning based Filtering Algorithm and in concluding part of the enhancement we just convert the output of this phase to just double type with an ultimate goal to achieve grayscale image adjustment.

Tuning based Filtering procedure is explained using Figure 3.7. The input for the procedure is a raw image which is referred as I. In this study, we consider grayscale fingerprint image size as 256 × 256. Here maximum intensity value of the image is 255 and the minimum intensity value of the pixel is 0. R and C are rows and column size of the Image I.

The Tuning based Filtering procedure is explained using workflow. The input for this is row grayscale fingerprint image of size 256 × 256 which is represented as I. The final output is

filtered image is $I_{filter}$. The different workflows of the proposed procedure are shown in Figure 3.8.

### 3.8.1 Tuning Based Filtering Algorithm-Procedure

Input: Raw Image; I

Output: Filtered Output Image, $I_{filter}$

1. **for all pixels** in I(i, j) **do**

   Compare with maximum intensity value of the image. **if** I(i ,j) = max(I)

   Find the total count of maximum intensity pixels. $\rho_{max} = I(i,j)$

   **end if**

   **end for**

2. Find probability density function of $\rho_{max}$. $\delta_{max} = \frac{\sum \rho_{max}}{R \times C}$
3. **for all pixels** in I(i, j) **do**

   Compare with minimum intensity value of the image. **if** I(i ,j) = min(I)

   Find the total count of minimum intensity pixels. $\rho_{min} = I(i,j)$

   **end if**

   **end for**

4. Find probability density function of $\delta_{min}$. $\delta_{min} = \frac{\sum \rho_{min}}{R \times C}$ // Where R & C //are row and Colum size of the image
5. Find probability density function for each window by taking minimum or low value for each row as $\delta_w = \delta_{max}(\frac{\delta(l) - \delta_{min}}{\delta_{max} - \delta_{min}})^{\epsilon}$ // $\epsilon \rightarrow$Constant; // $\epsilon = 0.2$
6. Find cumulative density function for each row or window of the image as $\partial_w = \sum_{l=0}^{l_{max}} \frac{\delta_w(l)}{\sum \delta_w}$ ,where $\sum \delta_w = \sum_{l=0}^{l_{max}} \delta_w(l)$
7. Map the input image pixel value to new value as $\tau = round(1 - \max((\partial_w(:)))$ //round to 6 decimal points
8. Obtain the filtered image as $I_{filter} = (l_{max} \times (\frac{I(i,j)}{l_{max}}))^{\tau}$

**Figure 3.7:** Tuning based filtering image Procedure

### 3.6.2 Workflow of Tuning based Filtering Algorithm

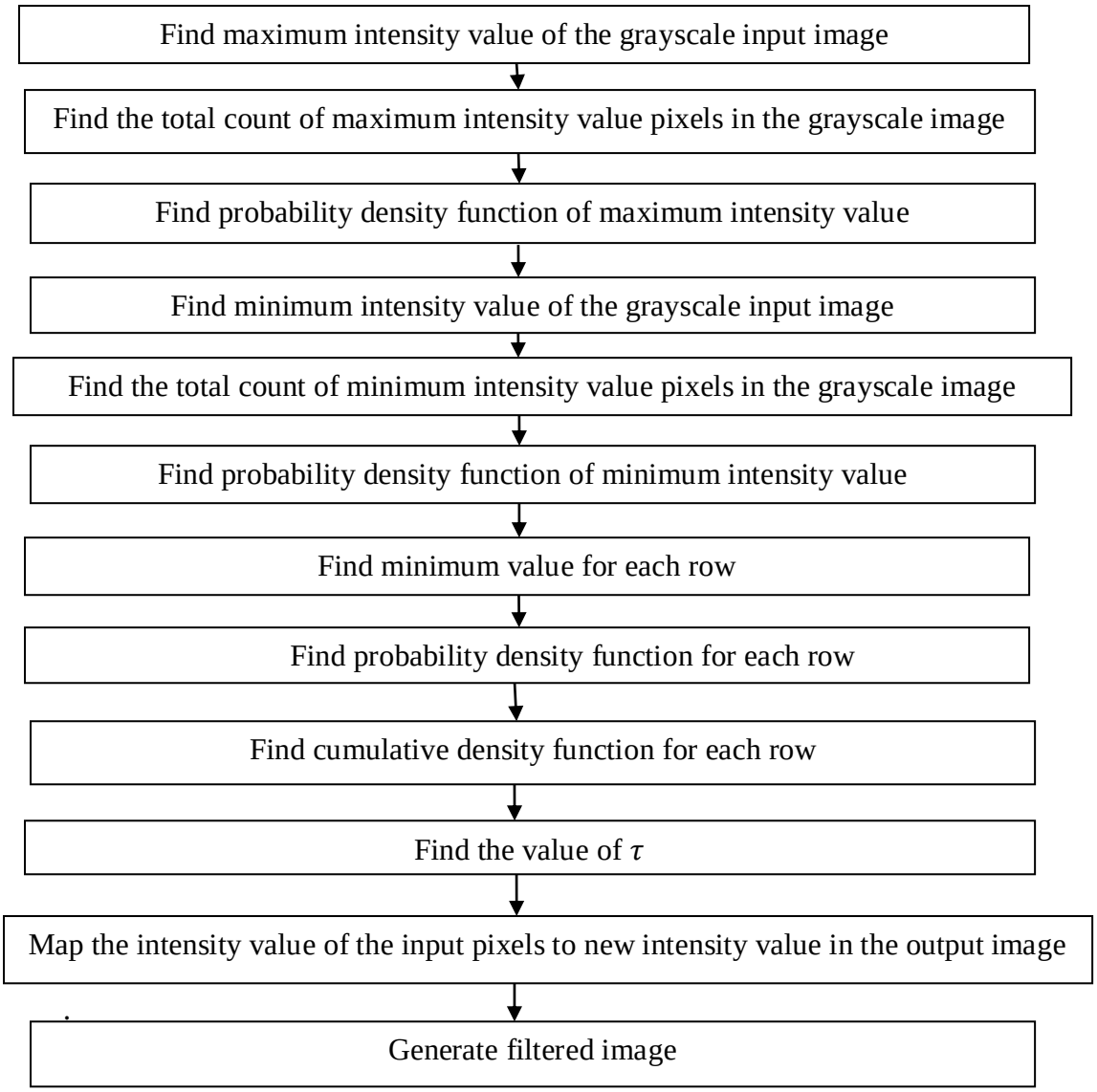
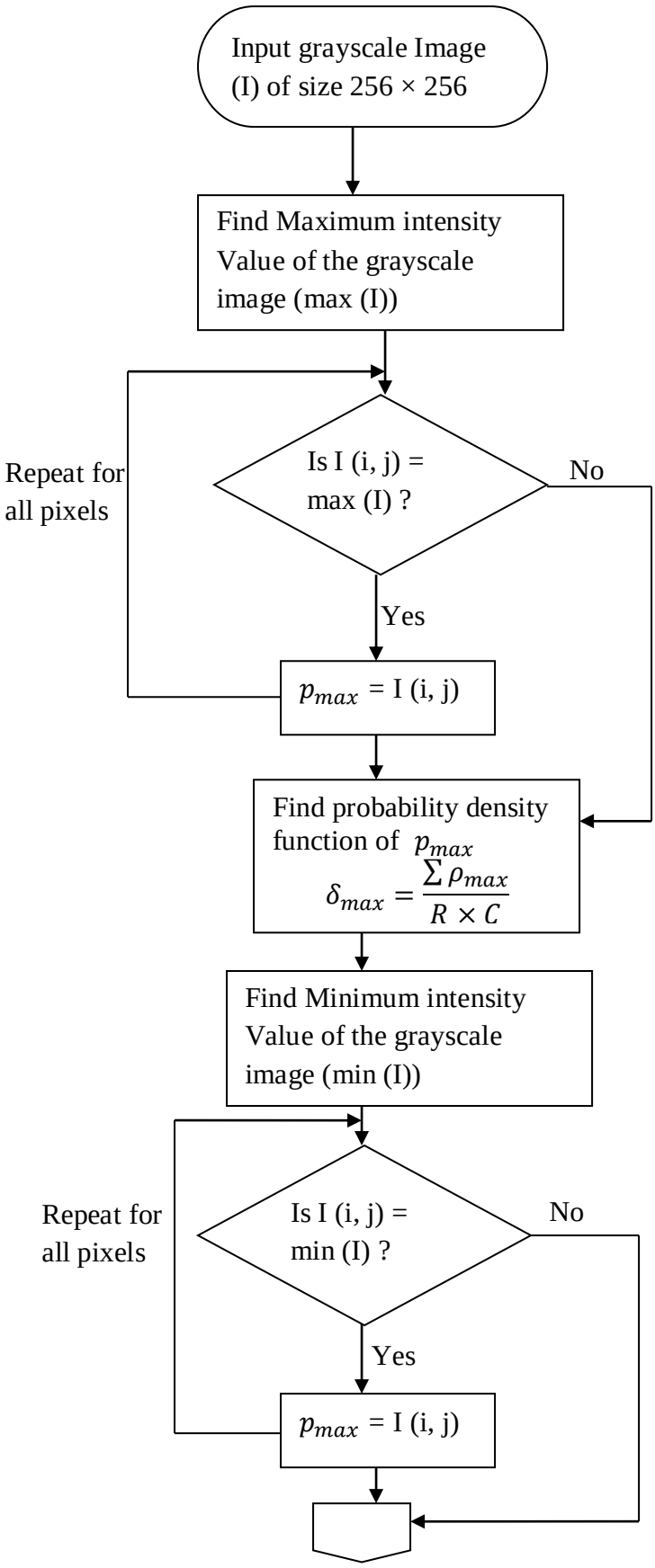



**Figure 3.8:** Work flow of tuning based filtering algorithm

The Figure 3.9 shows a flowchart for Tuning based Filtering procedure, which is extended to two pages and off-page connector symbol of the flowchart is used to connect between two pages. In order to analyze the algorithm benchmark fingerprint dataset is considered from FVC ongoing 2002 DB1_B (Maltoni et al., 2009). Table 3.1 shows the range of grayscale intensity values for the few of FVC 2002 DB1_B datasets before using the proposed filtering algorithm and after applying filtering algorithm. The Table 3.1 also shows range of grayscale intensity values using Histogram equalization. In this benchmark dataset each user's different eight fingerprints are considered for training or testing purposes.

### 3.6.3 Flowchart of Tuning Based Filtering Algorithm



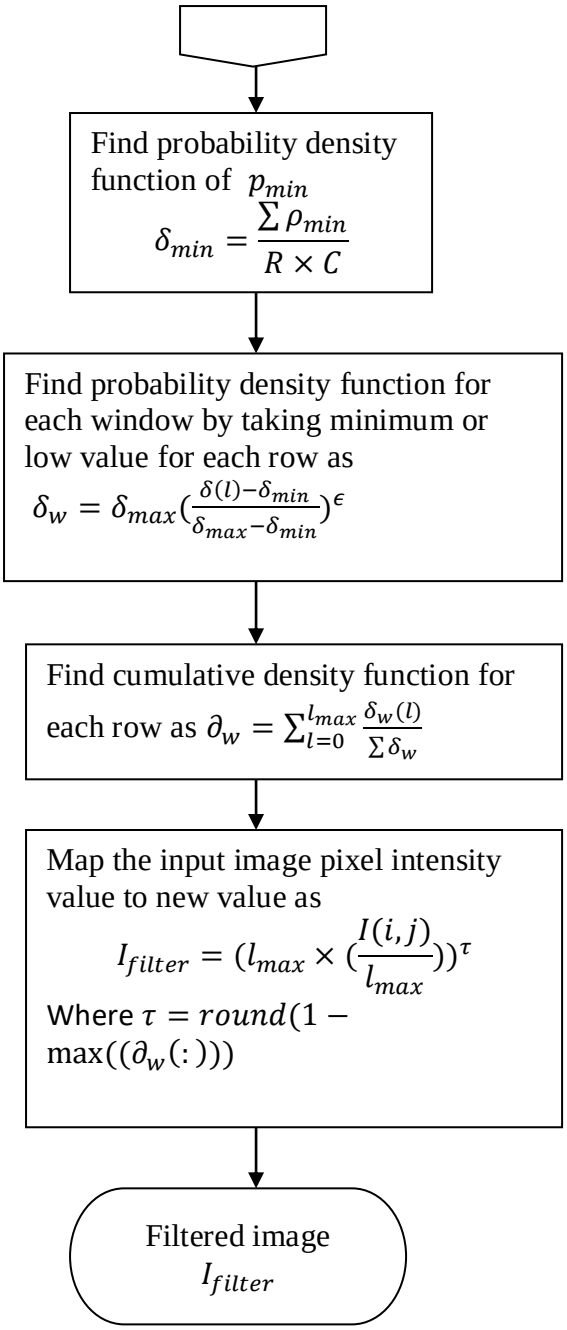



**Figure 3.9:** Flowchart of proposed filtering algorithm

### 3.6.3 Analysis of Proposed Filtering Algorithm

From the table 3.1, it is clear that proposed method having less intensity range compared to Histogram equalization. In τ- Tuning Based Filtering Algorithm, dark pixels are the highest dark and bright pixels are either highest or near to high bright values. This algorithm is best suited for grayscale fingerprint image, especially image of size 256 × 256.

**Table 3.1:** Range of intensity values in 256 × 256 sized grayscale fingerprint image

| **Fingerprint Image Name** | **Range of Intensity values before applying proposed filtering algorithm** | **Range of Intensity values after applying proposed filtering algorithm** | **Range of Intensity values using Histogram Equalization** |
|---|---|---|---|
| 101_1.tif | 0 to 255 (256 values) | 0, 250, 252 (3 values) | 0, 4, 8, 12, 16, 20, 24, 28,32, 36, 40, 45,49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 162, 255 (24 values) |
| 102_1.tif | 0 to 255 (256 values) | 0, 249, 250, 251, 252 (5 values) | 0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 45, 39, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97, 101, 162, 255 (24 values) |
| 103_5.tif | 0 to 255 (256 values) | 0, 249, 250, 251, 252 (5 values) | 0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97, 101,105,109, 113, 117, 121, 125, 130, 134, 138, 194, 255 (37 values) |
| 104_4.tif | 0 to 255 (256 values) | 0, 249, 250, 251, 252, 253 (6 values) | 0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97, 101, 105, 109, 178, 255 (30 values) |
| 105_8.tif | 0 to 255 (256 values) | 0, 246, 247, 248, 249, 250, 251, 252, 253 (9 values) | 0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 45, 49, 53, 57, 61, 65, 69, 73, 150, 255 (21 values) |

The Table 3.2 shows the number of occurrence of each grayscale intensity value for the proposed algorithm, for the same image considered in Table 3.1. As like histogram equalization, one of the pixel intensity values dominates over other. So this algorithm is not best for the natural image because it may cause wash out appearance. But this is very good for a grayscale fingerprint image. In fingerprint image usually black color represents ridges and white color represents valley.

In Table 3.2 we can note that the dominating intensity values usually fall in the upper boundary region of intensity range, which makes the image brighter. Figure 3.10 shows

some sample images of FVC ongoing 2002 DB1_B benchmark datasets with labels as 101_1.tif, 102_1.tif, 103_5.tif, and 104_4.tif. Figure 3.11 shows input fingerprint image and filtered image with its histogram representation.

**Table 3.2:** Intensity and frequency count of the fingerprint image for the proposed filtering algorithm

| **Fingerprint Image Name** | **Intensity value and frequency count of the fingerprint image for the proposed algorithm** | |
|---|---|---|
| 101_1.tif | 0 | 8084 |
| | 250 | 57196 |
| | 252 | 256 |
| 102_1.tif | 0 | 5300 |
| | 249 | 43808 |
| | 250 | 14954 |
| | 251 | 1222 |
| | 252 | 252 |
| 103_5.tif | 0 | 25855 |
| | 249 | 23914 |
| | 250 | 14237 |
| | 251 | 1020 |
| | 252 | 510 |
| 104_4.tif | 0 | 14152 |
| | 249 | 34515 |
| | 250 | 15333 |
| | 251 | 1024 |
| | 252 | 256 |
| | 253 | 256 |
| 105_8.tif | 0 | 3053 |
| | 246 | 245 |
| | 247 | 252 |
| | 248 | 756 |
| | 249 | 41592 |
| | 250 | 15006 |
| | 251 | 3165 |
| | 252 | 1228 |
| | 253 | 239 |

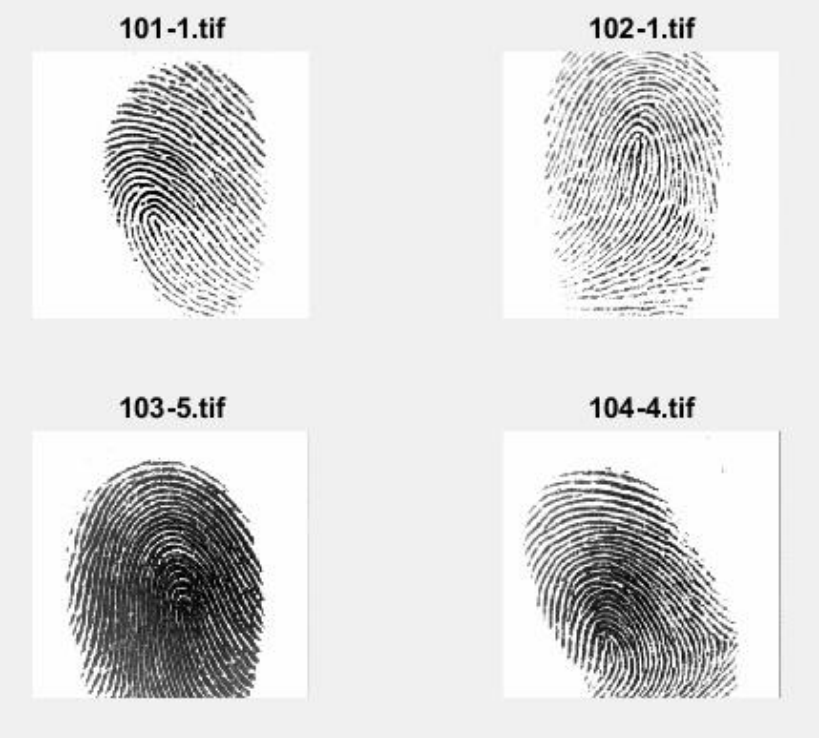



**Figure 3.10:** Sample original fingerprint images of FVC ongoing 2002 DB1_B dataset

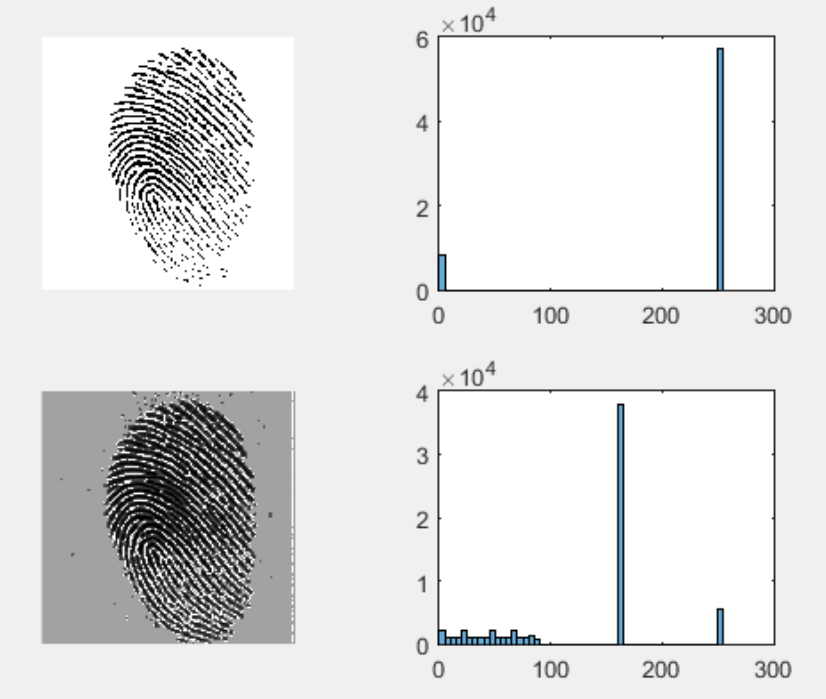



**Figure 3.11:** '101_1.tif'-Sample fingerprint image of FVC ongoing 2002 DB1_B after filtering process. (Top left: Filtered image using proposed method, Top Right: Histogram of top left, Bottom right: Filtered image using Histogram Equalization, Bottom right: Histogram of bottom left)

**Time complexity Analysis of the Algorithm**

In this research study, the new algorithm is analyzed for time complexity using hypothetical Model Machine. Some characteristics of the Hypothetical machine are given below.

- Single processor machine
- 32-bit architecture
- Sequential Execution
- Arithmetic and logical operation takes 1 unit of time
- Assignment statement takes 1 unit of time
- Function return takes 1 unit of time

In order to calculate time complexity of the algorithm, the entire algorithm is divided into different fragments, the time complexity for them is calculated first and later all this fragments time complexity is added in order to get overall time complexity of the algorithm. The different fragments time complexity is shown in Table 3.3.

**Table 3.3:** Time complexity of different fragments of Tuning based contrast adjustment algorithm

| **Sr. No** | **Fragments of new algorithm** | **Time complexity** |
|---|---|---|
| 1 | Finding the Maximum and minimum intensity of the input image and probability density value of min and max intensity | $6n^2$ +10 |
| 2 | Finding the lowest intensity value (local minimum) in each row and then finding a total number of local minimum and probability density value of local or row minimum. | $3n^2$ + 11n + 1 |
| 3 | Finding cumulative density function of local minimum | 3n+3 |
| 4 | Map the input image pixel intensity value to higher intensity rage using the value **τ.** | $13n^2$ + n + 1 |
| 5 | Overall | $22n^2$+ 15n+15 |

f (n) = $22n^2 + 15n + 15$

g (n) = $n^2$

f (n) = O (g(n))

f (n) ≤ cg(n) , c > 0, $n_0 \geq 1$

$22n^2 + 15n + 15 = cn^2$ where c=23, n ≥ 16

So the rate of growth of the time for new algorithm is O ($n^2$). [Big (Oh) of $n^2$]. When the size of the image is generally m × n (in this study we consider -256 × 256), it is O (mn).

### 3.7 EDGE DETECTION ALGORITHMS

Edge detection is a first and foremost phase of image processing technique for finding or locating the boundary of the objects within the image. It works by detecting discontinuities in brightness. One of the important and major applications of edge detection is image segmentation out of many diverse applications. Five major edge detection algorithms are discussed in this session, to detect or identify edge efficiently or effectively from fingerprint image without any hurdles. From these five major methods, choice of edge detection is based totally on their ability to identify edges accurately. The five major types of edge detection are,

- Sobel operator
- Prewitt operator
- Roberts operator
- Laplacian of Gaussian (LoG) operator
- Canny Operator

Almost all type of edge detection consists of small kernels to blur the image; technically the process is referred as convolution to approximate or estimate first-order directional derivatives of the image brightness distribution. Kernels have already defined a collection of edge pattern to match or compare it with another part of the same image or segment with some fixed size. The edge value is considered by keeping the pixel in the center and surrounded by eight neighborhood pixels in all eight directions or simply forming a matrix. If the calculated value is greater than the value of the threshold then that pixel is considered as part of the edge. The entire gradient-based algorithms find edge strength with the help of kernel operator for all pixels which are orthogonal to each other or vertical and horizontal each other. While calculating edge strength both values are taken into account. The different algorithm uses a different value for kernel function.

Usually, edge detection algorithms are classified into two types as Gradient operator and Laplacian operator (Harris and Stephens, 1988). Gradient operator detects edge pixel by way of acquiring the maximum and minimum value calculated from the first derivative level of the image. The eqs. (3.8) finds the gradient operator, $\delta$, and its application on vector E.

$\delta = \left(\frac{\partial}{\partial r}, \frac{\partial}{\partial c}\right)$ $\delta E = \left(\frac{\partial E}{\partial r}, \frac{\partial E}{\partial c}\right)$ ---------- (3.8)

The $\delta E$ later used for the purpose of calculating the gradient magnitude, which is represented as $|\delta E|$, and $\phi$, be the orientation angle of the image. Gradient magnitude and direction are used for two different purposes, the gradient for the strength of an image edge and gradient orientation for image edge pixel orientation. The different gradient operators used in this present study are four as Sobel, Prewitt, Roberts, and Canny (Heath et al., 1997; Ziou and Tabbone, 1998).

Laplacian operator is based on second order derivative, in which output value obtained for edge pixel in the first order derivative is considered as zero crossing for the second order derivative. The drawback of this function is its touchy characteristic in the direction of noise impact. In fixing this hassle, The Gaussian feature is being applied to the image, which is termed as Laplacian of Gaussian (LoG), which will be explained later in this study.

### 3.7.1 Sobel Operator

Sobel operator makes use of 3×3 matrix for the purpose of convolution which utilizes x and y-direction on the image. It uses first-order derivative level. Sobel operator makes use of two-pixel masks one for horizontal as $G_h$ and another for vertical as, $G_v$. Figure 3.12 shows Sobel, operator.

$G_h$=

| | | |
|---|---|---|
| -1 | 0 | 1 |
| -2 | 0 | 2 |
| -1 | 0 | 1 |

(a)

$G_v$=

| | | |
|---|---|---|
| -1 | -2 | -1 |
| 0 | 0 | 0 |
| 1 | 2 | 1 |

(b)

**Figure 3.12:** Sobel Operator

This pixel mask is moved for all pixels of the image by placing the pixel at the center of the mask. This process is repeated till all the pixels values are kept into output array. The gradient magnitude can be calculated as shown in eqs. (3.9)

$$|G| = |G_h|\,|G_v| \quad \text{----------} \quad (3.9)$$

Where $G_h$ and $G_v$ are give by the formulae or eqs. (3.10) and (3.11) respectively.

$$G_h = (a_2 + ca_3 + a_4) - (a_0 + ca_7 + a_6) \quad \text{----------} \quad (3.10)$$

$$G_v = (a_0 + ca_1 + a_2) - (a_6 + ca_5 + a_4) \quad \text{----------} \quad (3.11)$$

C is constant which takes value 2. Figure 3.13 shows neighbourhood pixels or how the each pixel are compared with eight pixels placed in eight directions with reference to central pixel.

| | | |
|---|---|---|
| $a_0$ | $a_1$ | $a_2$ |
| $a_7$ | i, j | $a_3$ |
| $a_6$ | $a_5$ | $a_4$ |

**Figure 3.13:** Neighbourhood pixel used in Sobel operator

### 3.7.2 Prewitt Operator

Prewitt operator works on the basis of central difference and is given by eqs. (3.12)

$\frac{\partial_I}{\partial_X} \approx$ [ I (x+1, y) – I (x-1, y)/ 2] ---------- (3.12)

The convolution mask of Prewitt operator is given below using Figure 3.14.

| | | |
|---|---|---|
| -1 | 0 | 1 |

**Figure 3.14:** Prewitt operator convolution mask

Prewitt operator is easily prone to noise problems. Due to this reason, an averaging method could be used to remedy the noise hassle. The convolution masks for Prewitt operator has been implemented after averaging the procedure at x and y-axis for $\frac{\delta y}{\delta x}$. The equations for Prewitt operator and Sobel operator are quite comparable except for the cost of the constant c=1. Prewitt operator is best suitable for judging or estimating the magnitude and orientation of an edge. Even though differential gradient edge detection estimates the orientation from the magnitude of the x and y-axis, it is having more time complexity. The Prewitt operator is limited to 8 possible orientations, however, experience shows that most direct orientation estimates are not much more accurate. This gradient-based edge detector is estimated in the 3x3 neighborhood for eight directions.

### 3.7.3 Robert Operator

Robert cross operator makes uses of 2x2 convolution mask. It utilizes {+1, -1} operator that will calculate the value as shown in eqs. (3.13).

I ($\bar{x_i}$) - I ($\bar{x_j}$) ---------- (3.13)

For (i, j) pixel are referred as environs pixel. In mathematical equations, this are referred as forward differences and is shown in eqs. (3.14).

$\frac{\partial I}{\partial X} \approx$ I (x +1, y) – I (x, y) ---------- (3.14)

Convolution mask for Robert cross operator consists of +1 and -1 in only two directions opposite to each other is shown below using Figure 3.15.

| | |
|---|---|
| +1 | |
| | -1 |

$g^1$

| | |
|---|---|
| | +1 |
| -1 | |

$g^2$

**Figure 3.15:** Convolution mask for Robert Cross Operator

Gradient magnitude is calculated using eqs. (3.15).

$$G=\sqrt{((g1 * f)^2) + ((g2 * f)^2} \quad \text{----------} \quad (3.15)$$

### 3.7.4 LoG Operator

If the pixel intensity values are considered as I (x, y) then the Laplacian value is represented as L (x, y) and which is given by eqs. (3.16).

$$L(x, y) = \frac{\partial^2 I}{\partial x^2} + \frac{\partial^2 I}{\partial y^2} \quad \text{----------} \quad (3.16)$$

The Input image is made by a set of discrete pixels, the second derivative can be approximated using discrete convolution kernel within the definition of the Laplacian. Three normally used small kernels are shown in Figure 3.16

| | | |
|---|---|---|
| 0 | 1 | 0 |
| 1 | -4 | 1 |
| 0 | 1 | 0 |

| | | |
|---|---|---|
| 1 | 1 | 1 |
| 1 | -8 | 1 |
| 1 | 1 | 1 |

| | | |
|---|---|---|
| -1 | 2 | -1 |
| 2 | -4 | 2 |
| -1 | 2 | 1 |

**Figure 3.16:** Discrete approximation to the Laplacian filter

The relevance of Gaussian smoothening as a pre-processing step reduces the excessive frequency noise module prior to the differentiation step. The two-dimensional LoG characteristic focused on zero and with the general or normal Gaussian deviation σ has the shape and is shown in eqs. (3.17)

$$LoG(x, y) = -\frac{1}{\pi\sigma^4}\left[1 - \frac{x^2+y^2}{2\sigma^2}\right] e^{-\frac{x^2+y^2}{2\sigma^2}} \quad \text{----------} \quad (3.17)$$

### 3.7.5 Canny Operator

The canny edge detection consists of five separate steps and each step does some special works. They are

1. Smoothing: Blurring of the image to get rid of noise or removing the noise from the image.

2. Locating gradients: The edges should be marked or pointed out where the gradient of the image has higher magnitudes.

3. Non-maximum suppression: Only pixels which are satisfying the condition of local maxima are marked as edges.

4. Double thresholding: Potential or all probable edges are decided by thresholding.

5. Edge tracking by using hysteresis: Final edges are determined by way of suppressing or smoothing all edges that are not linked to a very positive (robust) edge.

The Canny edge detector first smoothes the image, to remove or reduce to maximum extent noise and then finds the image gradient to spotlight regions with high spatial derivatives. The algorithm then tracks along those regions and suppresses any pixel this is not on the local maxima (non-maximum suppression). The gradient array is then further reduced or processed through hysteresis. Hysteresis is used to track alongside the remaining pixels which have no longer be suppressed or traced in the initial tracing process. Hysteresis uses thresholds and if the magnitude is beneath the primary threshold, it's far set to zero (made a non-side), else it's far made an edge. If the significance is between the two thresholds (T1 and T2), then it is set to zero, until there may be a path from this pixel to a pixel with a gradient above T2.

### 3.7.6 Analysis of edge detection algorithms

The analysis of the edge detection algorithms are done via visual inspection of the edge detection methods and speed of the algorithms. The result here is presented for a sample FVC ongoing 2002 DB1_B benchmark dataset's fingerprint image. Similar results were received for different images additionally. The visual effects, in conjunction with the speed of the algorithms, are presented in figures 3.17, 3.18, 3.19, 3.20, and 3.21. The speed is measured only the times taken for particular type of edge detection function without taking into account other parameters like input or output. As edge detection is the maximum emphasised step of the image preprocessing or enhancement, the quality of the image required for feature extraction and matching process is geared by canny operator.

**Figure 3.17:** Original image and canny edge detection image (speed = 0.021636 second)

From the outcomes, it may be seen that the canny operator produces the satisfactory edge detection output or result with admire to best.

**Figure 3.18:** Original image and Sobel edge detection image (speed = 0.013507 seconds)

**Figure 3.19:** Original image and Prewitt edge detection image (speed = 0.011755 seconds)

**Figure 3.20:** Original image and Laplacian edge detection image (speed = 0.018300 seconds)

**Figure 3.21:** Original image and Roberts edge detection image (speed = 0.007443 seconds)

Table 3.4 shows a total number of pixels of identified edges through five edge detection algorithms for few sample grayscale fingerprint images of FVC ongoing 2002 DB1_B

datasets of 256 × 256 sized. This also proves that canny edge detection method identifies a maximum number of edges, which signifies that canny edge detection outperforms compared to other types of edge detection methods used in this study. Even though canny edge detection method takes little bit more time for execution, which is negligible compared to its edge detection capacity.

**Table 3.4:** Number of edges identified in different edge detection algorithms

| Sr. No | Image name | Sobel | Prewitt | Roberts | Laplacian | Canny |
|---|---|---|---|---|---|---|
| 1 | 101_1.tif | 1307 | 1217 | 428 | 1773 | 2526 |
| 2 | 102_1.tif | 8117 | 8006 | 5762 | 15155 | 19365 |
| 3 | 103_5.tif | 9080 | 8955 | 6009 | 15455 | 19561 |
| 4 | 104_4.tif | 9827 | 9645 | 4904 | 14758 | 18910 |
| 5 | 105_8.tif | 8302 | 8159 | 7157 | 15085 | 15986 |
| 6 | 101_6.tif | 10149 | 9931 | 4685 | 13711 | 18366 |
| 7 | 103_2.tif | 9299 | 9296 | 4829 | 14097 | 16710 |

### 3.8 FINGERPRINT SEGMENTATION

One of the significant processes in Automatic Fingerprint Recognition System (AFIS) is the segmentation of fingerprint. The process of decomposing an image into different components is referred as segmentation. Fingerprint segmentation is the one of the main process involved in fingerprint pre-processing and it refers to the process of dividing or separating the image into two disjoint regions as the foreground and background. The foreground also called as Region of Interest (ROI) because only the region which contains ridge and valley structure is used for processing, while the background contains noisy and irrelevant content and that will be discarded in later enhancement or orientation or classification process (Krishna Prasad K., & Aithal P. S., 2017g). The task right here is to determine which part of the image belongs to foreground, and which part belongs to background.

The emphasis is on ROI-segmentation is to accurately extract the ROI, which is real ridge details, which directly influences on the performance of feature extraction and matching process. The examples of ROI are shown below using figure 3.22.

(a) Original Image (b) ROI of the image

**Figure 3.22:** Example of ROI

### 3.8.1 Surfeit Clipping based Segmentation Algorithm (Proposed Modified Method)

This algorithm considers Enhanced fingerprint image and produces a good quality segmented image. Let I_enhanced be the enhanced image using τ-tuning based filtering method. The enhanced image is converted to a binary image and stored as I_binary. Initially to find the edges of the I_binary image efficiently canny edge detection method is used. Canny edge detection finds the edges of the image through different processes, which includes, smoothing, locating gradients, non-maximum suppression, double thresholding, and edge tracking by using hysteresis. Smoothing of the image is done with the help of convolution, which blurs the image to get rid of the noise. Canny edge detection uses double thresholding in order to find edges of the image. The result of the Canny edge detection method is stored as I_canny. Next, the edge detected an image, I_canny is converted into a low-resolution image by converting 256 × 256 sized grayscale image to 128 × 128 sized grayscale images.

$I_{LRE} = I_{binary}(i \times 2, j \times 2)$

The low-resolution image is represented as I_LRE. In the next phase I_LRE image is padded with zeros using pad array and usually for simplicity in this method we use pad array size is eight and is referred as P. For I_(LRE) eight zeros are added in row and column respectively, and it enhanced to 144 × 144 sized grayscale images, which is denoted as I_Parray. The $I_{Parray}$ is clipped into 15×15 sized image and processed. The clipped image is stored in temp1. The entire 225 pixels of temp1 are reshaped as 1×225 matrix and denoted as temp2. The covariance of the matrix of the image, temp2 is calculated and if it is less than the threshold then the pixel of the $I_{binary}$ (256 × 256 sized image) image is considered as not a

part of ROI or foreground. Covariance of a matrix is calculated by considering row as observations and columns as random variables. Every pixel of the $I_{binary}$ image is traced like this and marked as either foreground or background of the image based on covariance value. If it is greater than the threshold value then the pixel is considered to be foreground, means which is a real part of the fingerprint image. Each time when padarray is considered, this takes into account one pixel out of 128×128 low-resolution image and two pixels out of 256 ×128 sized images.

As the algorithm name suggests surfeit, means maximum, we discard maximum background part of the image by checking whether all the pixels of each column intensity value sum becomes 256. If the column sum is 256 means all the pixels of that particular column contains intensity value 1. This signifies that this column contains the background of the image. If anyone column intensity value sum leads to value less than 256, which signifies that the particular column contains part of the foreground or ROI of the image. Then we skip the iteration and count considering starting of the column pixel for the output of the segmented image from just previous to that column number. The same process we repeat from the last column to the first column in reverse direction and stop moving backward until we get a column number sum of intensity value less than 256 for the purpose of finding last column number, which contains at least one pixel of foreground pixel. This means that from the last column to till this position image contains only background part of the image. The above-mentioned method repeated for rows also. So that it eliminates background or white blank area in left edge, right edge, top edge and bottom edge regions.

### 3.8.2 Surfeit Clipping based Segmentation Algorithm-Procedure

Input: binary image, $I_{binary}$

Output: Segmented Image, $I_{segment}$

1. Read $I_{binary}$ image
2. Apply canny edge formation to the $I_{binary}$ and store it in a variable $I_{canny}$
3. **for exactly half of all** pixels do

   $I_{LRE} = I_{binary}(i \times 2, j \times 2)$ // $I_{LRE}$→Low Resolution Edge Image

   **end for**
4. Find size of low resolution image, $[R_{LRE}, C_{LRE}] = size\,(I_{LRE})$
5. Find the size of padding size and pad with Low resolution image,

   P=floor (max (15, 15)/2+1), $I_{Parray}$ = padarray$(I_{LRE}, [P\ P])$

6. **for** p-size row and p-size column **do**

   Create a temporary padded variable as

   temp1= $I_{Parray}\left(\left(i - floor\left(\frac{15}{2}\right) to\ i + floor\left(\frac{15}{2}\right)\right), \left(j - floor\left(\frac{15}{2}\right) to\ j + floor\left(\frac{15}{2}\right)\right)\right)$

   Reshape temp1 and assign to another variable as temp2=reshape (temp1, 1, 225)

   Find the co-variance of temp2, $V_1 = covariance(temp2)$

   Compare $V_1$ with threshold value, if $V_1 < T$ \\ T→Threshold value=0.101

   Find $I_{binary}$ image background pixels as

   $I_{binary}\left((i-P)*2-2+1:(i-P)*2, (j-P)*2-2+1:(i-P)*2\right) = 1$

   **end if**

   **end for**

7. Find the column size of the image, $N_R = ColumnSize\ of\ I_{binary}$
8. **for all pixels** of the column **do**

   Find sum of all pixels in each column, $C_{sum} = \sum I_{binary}(for\ all\ row, i)$

   // i, represents each column

   Check if column sum is equal to $N_R$ , if $C_{sum} = N_R$

   Track the position of pixel in the image as, $\text{Position}_1 = i$

   **end if**

   **end for**
9. **for all pixels** of the column, from last column pixel **do**

   Find sum of all pixels in each column, $C_{sum} = \sum I_{binary}(for\ all\ row, N_R + 1 - i)$

   Check if column sum is equal to $N_R$ , if $C_{sum} = N_R$

   Track the position of pixel in the image as, $\text{Position}_2 = \frac{({N_R}^2 - i^2)}{N_R + i}$

   **end if**

   **end for**
10. **for all pixels** of the Row **do**

    Find sum of all pixels in each row, $R_{sum} = \sum I_{binary}(i, for\ all\ column)$

    // i, represents each row

    Check if column sum is equal to $N_c$ , if $R_{sum} = N_c$

    Track the position of pixel in the image as, $\text{Position}_3 = i$

    **end if**

**end for**

11. **for all pixels** of the row, from last row pixel **do**

Find sum of all pixels in each row,

$$R_{sum} = \sum I_{binary}(N_C + 1 - i, for\ all\ column)$$

Check if column sum is equal to $N_C$ , if $R_{sum} = N_c$

Track the position of pixel in the image as, $\text{Position}_4 = \frac{({N_C}^2 - i^2)}{N_C + i}$

**end if**

**end for**

12. Obtain the segmented image as

$$I_{segment} = I_{binary}(\text{Position}_3 to\ \text{Position}_4 :, \text{Position}_1 to\ \text{Position}_2)$$

The work flow diagram of Surfeit Clipping based Segmentation Algorithm is shown in Figure 3.23.

### 3.8.3 Workflow for Surfeit Clipping based Segmentation Algorithm

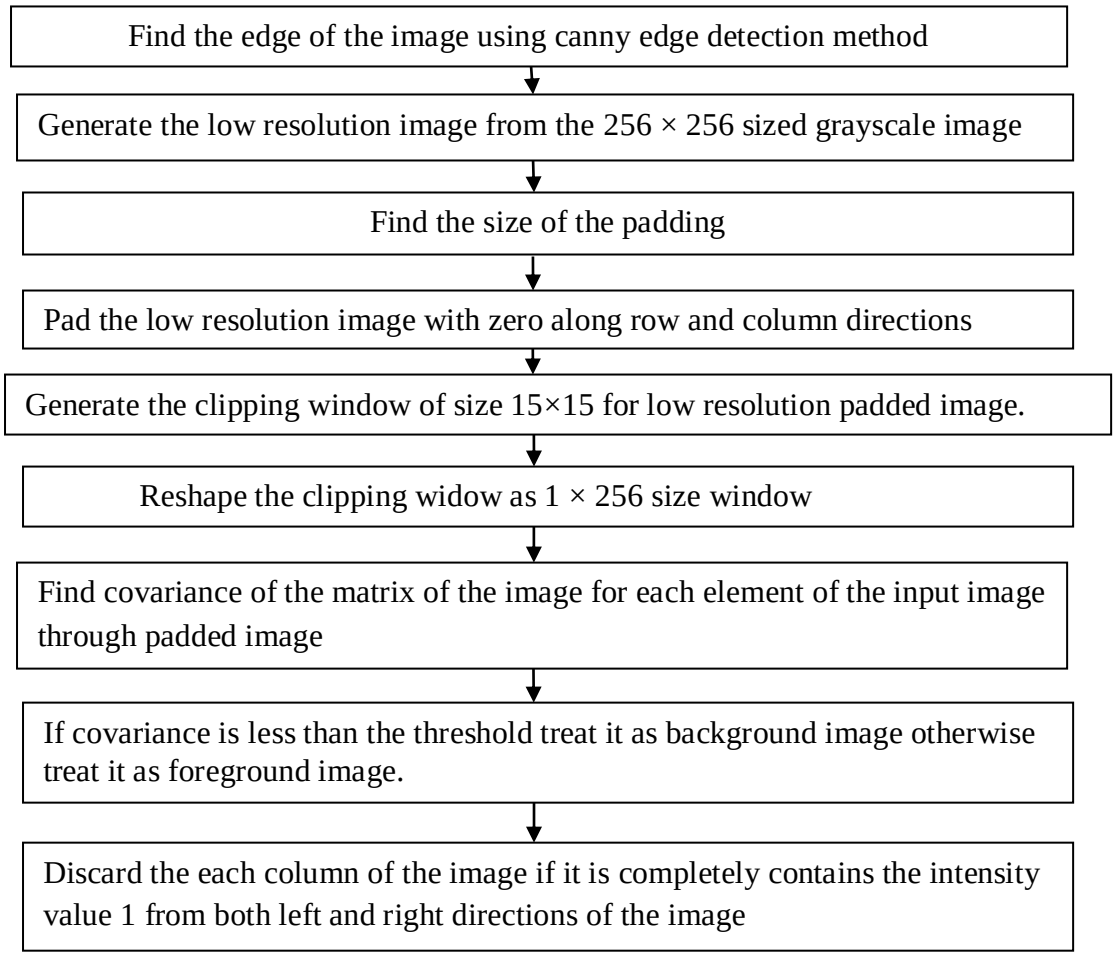
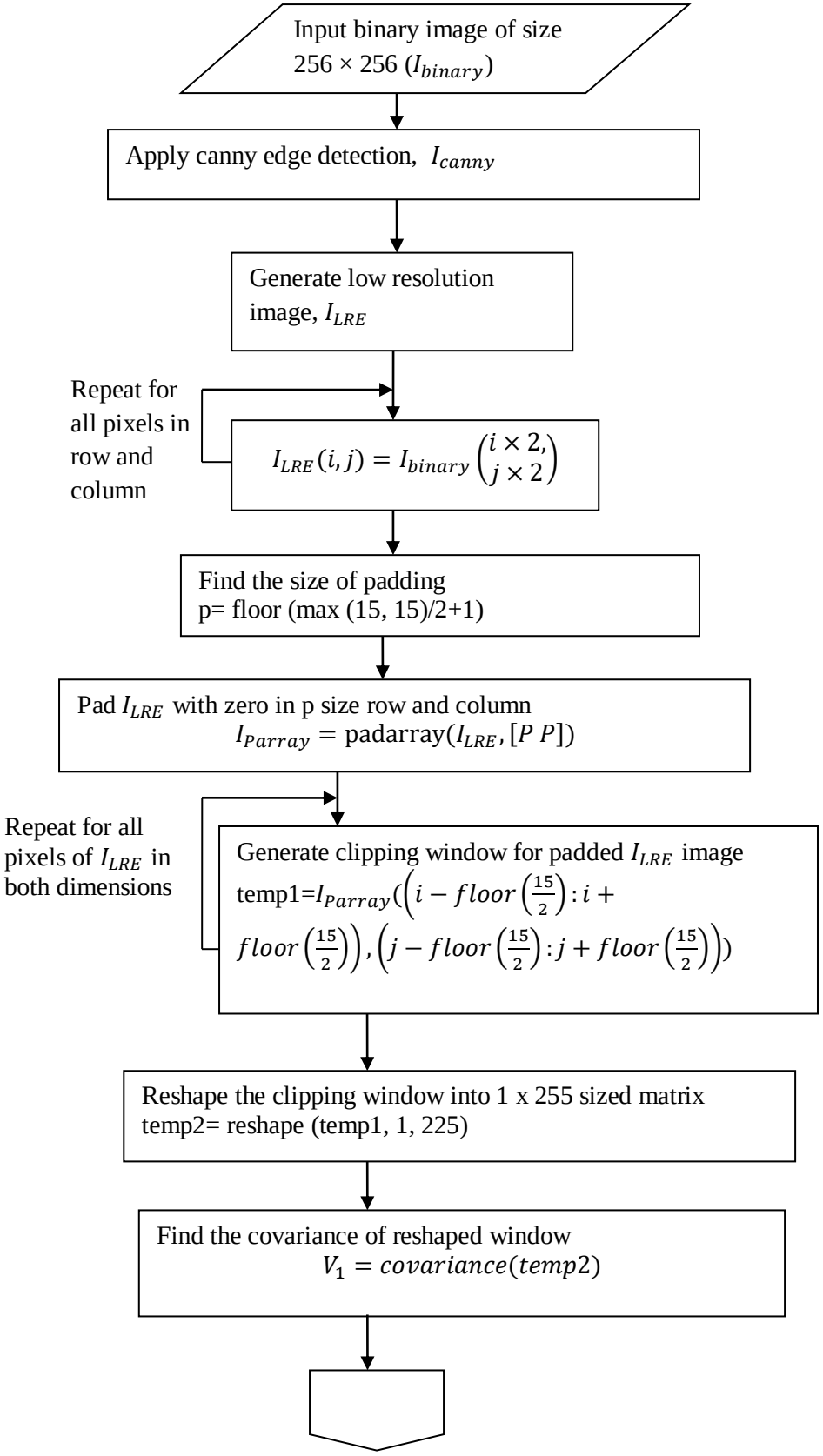
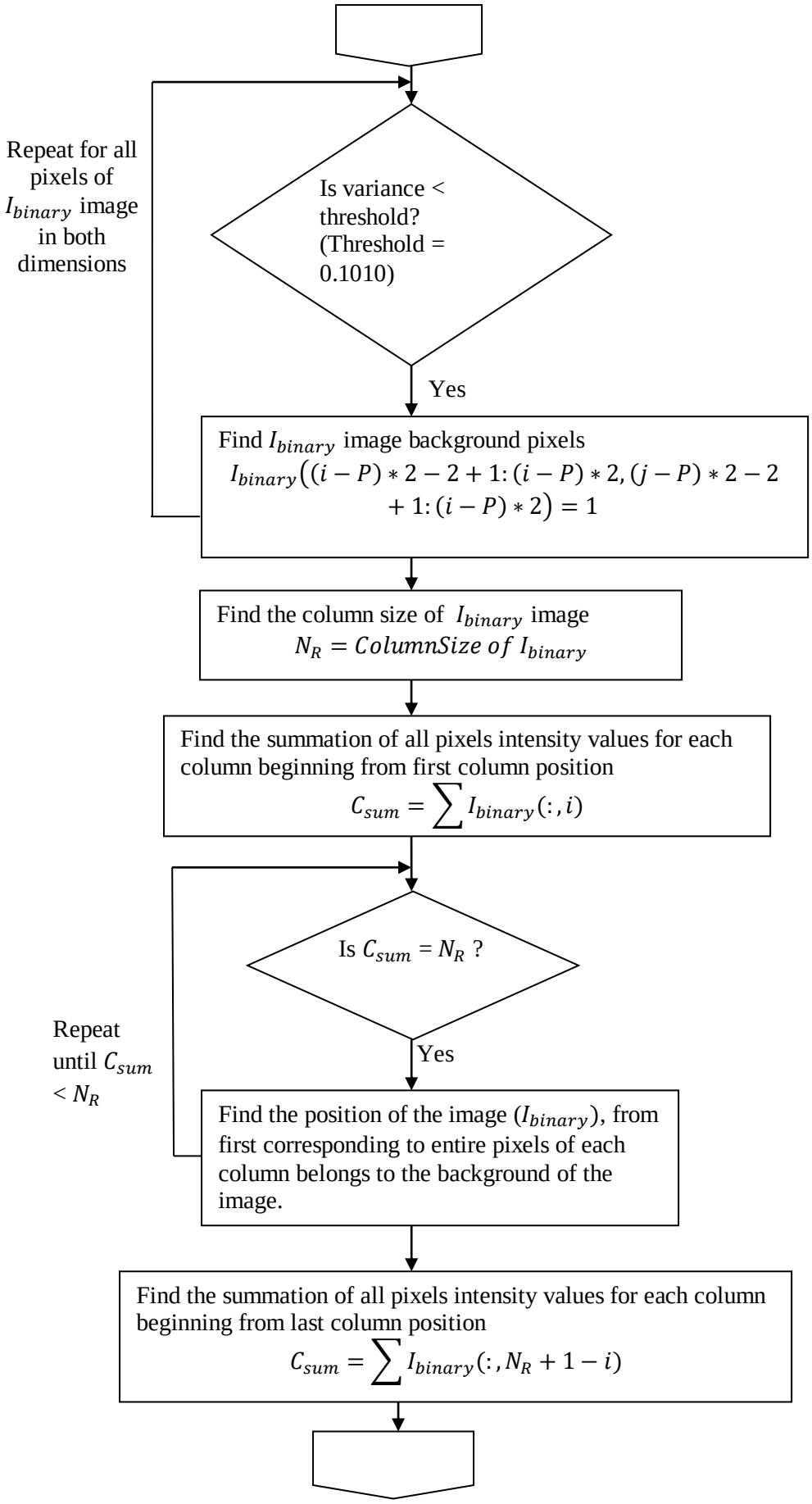
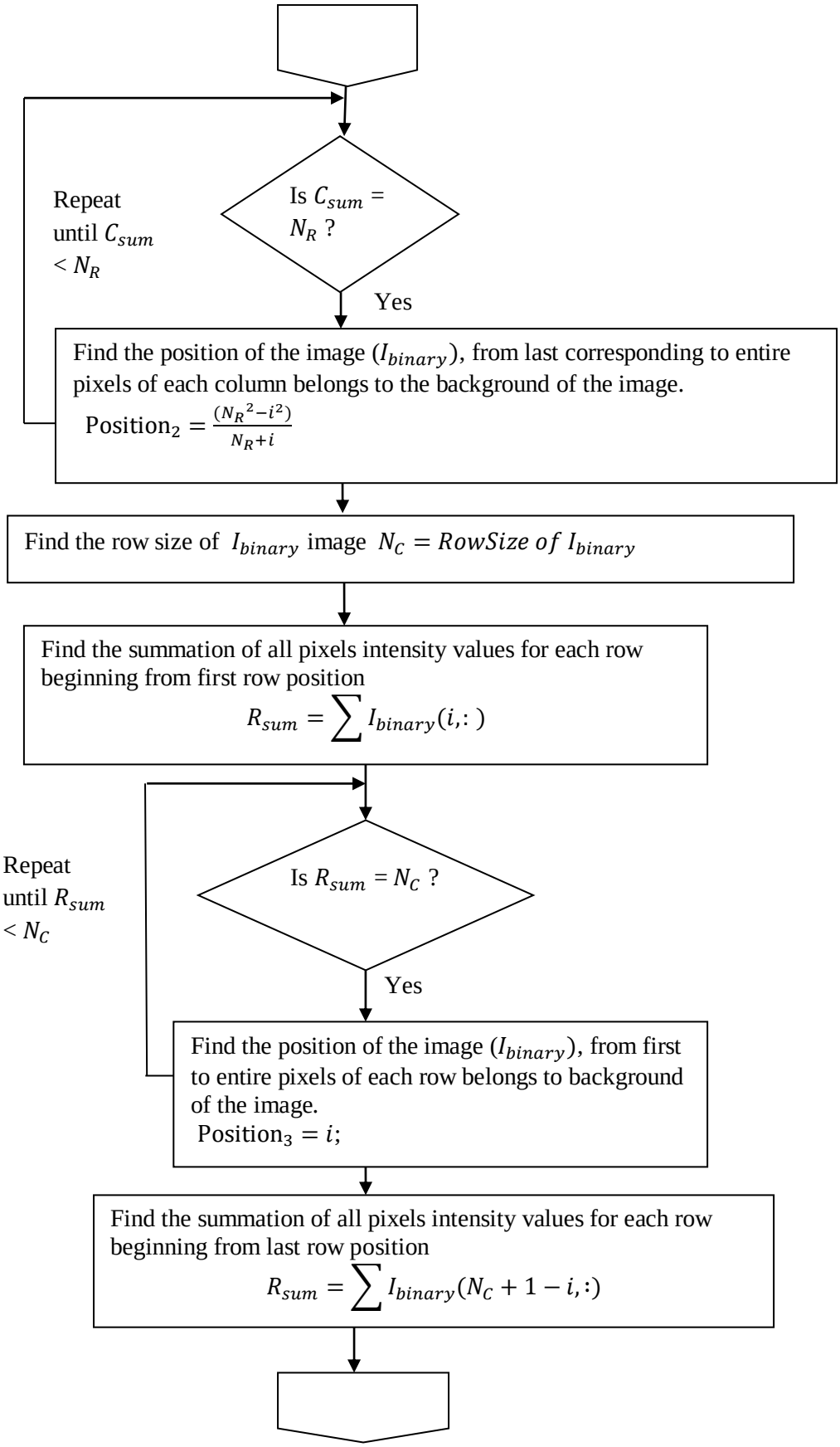



**Figure 3.23**: Workflow of Surfeit clipping based Segmentation algorithm

### 3.8.4 Flowchart of Surfeit Clipping based Segmentation Algorithm




Repeat for all pixels of $I_{binary}$ image in both dimensions
Is variance < threshold? (Threshold = 0.1010)
Yes
Find $I_{binary}$ image background pixels
$I_{binary}\big((i-P)*2-2+1:(i-P)*2, (j-P)*2-2+1:(i-P)*2\big)=1$
Find the column size of $I_{binary}$ image
$N_R = ColumnSize\ of\ I_{binary}$
Find the summation of all pixels intensity values for each column beginning from first column position
$C_{sum} = \sum I_{binary}(:,i)$
Is $C_{sum}$ = $N_R$ ?
Repeat until $C_{sum}$ < $N_R$
Yes
Find the position of the image ($I_{binary}$), from first corresponding to entire pixels of each column belongs to the background of the image.
Find the summation of all pixels intensity values for each column beginning from last column position
$C_{sum} = \sum I_{binary}(:, N_R+1-i)$


Repeat until $C_{sum} < N_R$
Is $C_{sum} = N_R$ ?
Yes
Find the position of the image ($I_{binary}$), from last corresponding to entire pixels of each column belongs to the background of the image.
$\text{Position}_2 = \frac{(N_R{}^2 - i^2)}{N_R + i}$
Find the row size of $I_{binary}$ image $N_C = RowSize\ of\ I_{binary}$
Find the summation of all pixels intensity values for each row beginning from first row position
$R_{sum} = \sum I_{binary}(i,:)$
Repeat until $R_{sum} < N_C$
Is $R_{sum} = N_C$ ?
Yes
Find the position of the image ($I_{binary}$), from first to entire pixels of each row belongs to background of the image.
$\text{Position}_3 = i;$
Find the summation of all pixels intensity values for each row beginning from last row position
$R_{sum} = \sum I_{binary}(N_C + 1 - i,:)$

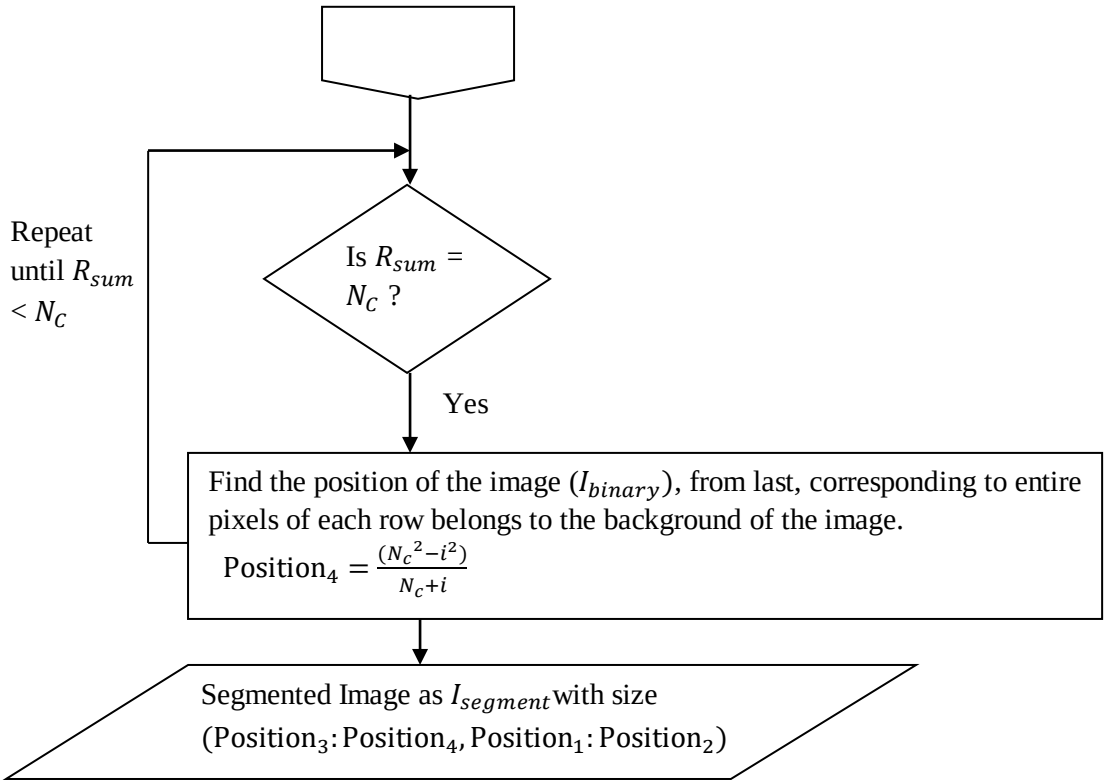



**Figure 3.24:** Flowchart of Two dimensional clipping based segmentation

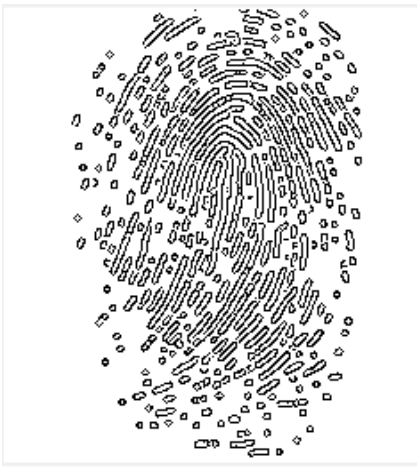
This proposed algorithm for segmentation is explained using flowchart in Figure 3.24. The input for this algorithm is enhanced grayscale fingerprint image of size 256 × 256 which is represented as $I_{enhanced}$ and which is a binary image. The final output is segmented image denoted as $I_{segment}$.

### 3.8.5 Analysis of the Surfeit clipping based Segmentation

The Surfeit clipping based segmentation is analysed by considering FVC ongoing 2002 DB1_B datasets. A sample fingerprint image named as 102_1.tif from FVC ongoing 2002 dataset is considered in Figure 3.25.

Table 3.5 shows edges obtained without filtering and with filtering techniques using canny edge detection method. Total numbers of edges are considered in terms of a total number of pixels.

(a) Original image



(b) Canny edge image

(c) Low-resolution Image

(d) Segmented image with margins

(e) Segmented image by clipping left right top and bottom border

**Figure 3.25:** Examples of Surfeit clipping based segmentation

**Table 3.5:** Total number of edges identified through canny edge detection

| Sr. No | Image name | Total number of Edges with filtering |
|---|---|---|
| 1 | 101_1.tif | 8774 |
| 2 | 102_1.tif | 8302 |
| 3 | 103_5.tif | 10023 |
| 4 | 104_4.tif | 10402 |
| 5 | 105_8.tif | 7354 |
| 6 | 101_6.tif | 10921 |
| 7 | 103_2.tif | 10136 |

Figure 3.26 filtered image, and results of segmentation process using surfeit clipping based segmentation for different sample images of FVC ongoing DB1_B datasets. While seeing the two images we don't find any differences. But if we observe carefully after segmentation left and right part of the filtered image is clipped, which corresponds to background pixels.

Table 3.6 shows the total number of pixels before the segmentation and after segmentation. If the numbers of pixels are reduced, this improves the execution performance or speed in following stages of automatic fingerprint identification systems like minutiae formation, feature extraction, and matching.

(a) Filtering image (b) Segmented image

**Figure 3.26:** Examples of filtered and segmented image using proposed methods

**Table 3.6:** Comparison of total number of pixels before and after segmentation

| Sr. No | Image name | Size of the image before segmentation | Size of the image after segmentation | Total number of pixels before segmentation | Total number of pixels after segmentation |
|---|---|---|---|---|---|
| 1 | 101_1.tif | 256 × 256 | 230 × 148 | 65536 | 34040 |
| 2 | 102_1.tif | 256 × 256 | 251 × 149 | 65536 | 37399 |
| 3 | 103_5.tif | 256 × 256 | 228× 183 | 65536 | 41724 |
| 4 | 104_4.tif | 256 × 256 | 222 × 193 | 65536 | 42846 |
| 5 | 105_8.tif | 256 × 256 | 236 × 153 | 65536 | 36108 |
| 6 | 101_6.tif | 256 × 256 | 213 × 180 | 65536 | 38340 |
| 7 | 103_2.tif | 256 × 256 | 222 × 150 | 65536 | 33300 |

**Time complexity Analysis of the Surfeit based Segmentation Algorithm**

In order to calculate time complexity of the algorithm, the entire algorithm is divided into different fragments, the time complexity for them is calculated first and later all this fragments time complexity is added in order to get overall time complexity of the algorithm. The different fragments time complexity is shown in Table 3.7.

**Table 3.7:** Time complexity of different fragments of Tuning based contrast adjustment algorithm

| Sr. No | Fragments of modified algorithm | Time complexity |
|---|---|---|
| 1 | Canny Edge Detection | mn log (mn) |
| 2 | Finding low-resolution edge and padding the low-resolution edge with zero | $3 * \left(\frac{n}{2}\right)^2 + 10$ |
| 3 | Finding foreground image through variance and threshold for padded array | $7 * \left(\frac{n}{2}\right)^2$ |
| 4 | Removing white background from left, right, top and bottom. | $4 * (3n) + 4$ |
| 5 | Overall | $10n^2 + 48n + 56 + mn \log (mn)$ |

Here m and n represents row and column dimension of image. In this study we use 256 × 256 sized image. M and n are equal i.e. 256 and 256. So equation becomes

f (n) = $10n^2 + 48n + 56 + mn\log(mn)$ [where $n^2$ = m × n= 256×256]

or

f(n) = 10mn+48m+56+mn×log(mn)

So the rate of growth of the time for new algorithm is O ($mn\log(mn)$ ) for very large value (very much greater than 256). In this study it is 10mn+48m+56+mn×log (mn) only.

f (n) = 10mn+48m+56+mn×log(mn)

g (n) = mn×log(mn)

f (n) = O (g(n))

f (n) ≤ cg(n) , c > 0, $n_0 \geq 1$

10mn+48m+56+mn×log(mn) = cmn×log(mn) where c=3.2, n ≥ 11

So the rate of growth of the time for surfeit based clipping algorithm is O (mn×log(mn)).

## 3.9 FINGERPRINT SKELETONIZATION (THINNING)

Fingerprint thinning or skeletonization is the technique of lowering the thickness of every line of a fingerprint pattern or ridge pattern to just a single pixel width (Hastings, 1992 & lam et al., 1992). The necessities of a good thinning algorithm with respect to the fingerprint are

- The thinned fingerprint image received must be of single pixel width without discontinuities.
- Each ridge must be thinned to its center pixel.
- Noise and singular pixels have to be removed.
- Elimination of pixels should not cause elimination of true minutiae or after the completion of thinning method none of the pixels eliminated.

There are many techniques to be had in literature for skeletonization or thinning process. After extracting the minutiae from the improved, binarized and thinned image a post-processing is accomplished in this final fingerprint image to filter or remove any spurious minutiae. The techniques on this post processing are of types–crossing number based and morphology-based.

### 3.9.1 Edge Prediction based Skelton formation

The Edge Prediction based Skelton formation is totally based on the conditional thinning set of rules (You & Wang, 2003), which is used to carry out thinning. Mark the target point 1, the background as zero. The main idea is here to use, eight-neighbourhood and there may be at least one background pixel or point, defined as boundary point (Krishna Prasad K., & Aithal P. S., 2017h).

This method considers the segmented image, I_segment as input for this process. The output from this method is skeletonized or thinned image, denoted as I_skeleton. Initially, the size of the $I_{segment}$is calculated. In this method 3 × 3 frame is moved across every pixel of the image. If $I_{segment}$ (i, j) =1, then it signifies that particular pixel is not part of the image's foreground, it's just background pixel. Where i, and j represents the index of row and column dimension of the image. The image is traced in row and column order from second row and column to till the second last row and column. If $I_{segment}$ (i, j) =1, then for each pixel,

including that pixel, a 3 × 3 frame is created based on following equations. The frame image is referred as temp.

$$temp = I_{segment}\big((i-1:i+1),(j-1:j+1)\big)$$

In above assignment statement, i and j represent row and column position of the $I_{segment}$ image. The shape of the frame for $I_{segment}$ (2, 2), image matrix is as follows. The actual pixel position is (2, 2), which is surrounded by 8 pixels in different eight directions. The central pixel is surrounded by a ring shape starting from (1, 1), (1, 2), (1, 3), (2, 3), (3, 3), (3, 2), (3, 1), (2, 1), and (1, 1). The central pixel is checked with all eight neighboring pixels as shown in Figure 3.27.

| | | |
|---|---|---|
| (1, 1) | (1, 2) | (1, 3) |
| (2, 1) | (2, 2) | (2, 3) |
| (3, 1) | (3, 2) | (3, 3) |

**Figure 3.27:** Example of 3 x 3 frame used in Edge Prediction based Skelton formation

The image type is logical so it contains either zero or one as its intensity values. One represents background of the fingerprint image and zero represents foreground of the image. Next we find values of these eight positions and store that values in a variable called, $RE_{temp}$. Generally Ring structure for any pixel position is created as follows,

Trace from first column of the temporary variable to column size value-1 for following two statements

$RE_{temp}(i) = temp(1,i)$ \\$RE_{temp}$→Ring Extracted for temp Matrix

$RE_{temp}\left(\left(C_{temp}-1\right)+\left(R_{temp}-1\right)+i\right) = temp(R_{temp}, C_{temp}+1-i)$ \\$C_{temp}$→column size, variable i, is index of column.

Trace from first row of the temporary variable to row size value-1 for following two statements.

$RE_{temp}\left(C_{temp}+i\right) = temp\left(1, C_{temp}\right)$

$RE_{temp}\left(\left(C_{temp}-1\right)+\left(R_{temp}-1\right)+i\right) = temp(R_{temp}+1-i, C_{temp})$ \\$R_{temp}$→Row size of temporary variable, variable i, is index of Row.

Assign the temporary variable first element value to Ring Extracted for temp Matrix's last position ( $RE_{temp}$ ), which is usually becoming (9, 9) position in 3 × 3 frame. This assignment statement is shown below.

$$RE_{temp}\left((C_{temp}-1)+\left(R_{temp}-1\right)+(C_{temp}-1)+\left(R_{temp}-1\right)+1\right)=temp(1,1)$$

Consider, For example, central pixel position as (2, 2). The pixels positions of the $RE_{temp}$ matrix are assigned as shown in table 3.7.

**Table 3.8:** Example of Edge Vector used in Edge Prediction based Skelton formation

| Sr. No | Edge Vector ($RE_{temp}$) | Temporary Image formed from $I_{segment}$ (temp) |
|---|---|---|
| 1 | $RE_{temp}$ (1) | temp (1, 1) |
| 2 | $RE_{temp}$ (5) | temp (3, 3) |
| 3 | $RE_{temp}$ (2) | temp (1, 2) |
| 4 | $RE_{temp}$ (6) | temp (3, 2) |
| 5 | $RE_{temp}$ (3) | temp (1, 3) |
| 6 | $RE_{temp}$ (7) | temp (3, 1) |
| 7 | $RE_{temp}$ (4) | temp (2, 3) |
| 8 | $RE_{temp}$ (8) | temp (2, 1) |
| 9 | $RE_{temp}$ (9) | temp (1, 1) |

Next, we find the NP corresponds to a total number of points which is having logical value 1 or which contains background part of the fingerprint segmented image. Simply, NP is Temporary Variable to save the result of that corresponding calculation. NP can be obtained using eqs. (3.18)

$$N_p=\frac{\left(\sum RE_{temp}\right)^2-(RE_{temp}(1))^2}{\left(\sum RE_{temp}\right)+RE_{temp}(1)} \text{ ---------- } (3.18)$$

The $RE_{temp}$ matrix is reshaped as 1 × 9 logical matrices. Next, we find total number of terminating point around the central pixel. We consider a variable $T_p$, corresponds to terminating point. The last position of $RE_{temp}$ matrix contains the value of first position itself. So we trace and find only eight neighborhood pixel position values and at a time we consider contiguous two-pixel position starting from the first position. If first-pixel position contains zero and next succeeding pixel contains one then it is marked as $T_p$. This is shown in following statement,

$$\text{if } (RE_{temp}(p)=0)\ \&\ (RE_{temp}(p+1)=1)\quad T_p=T_p+1$$

Here p can take any value from 1 to 8. When $RE_{temp}$ contains NP > =2 and NP<=6 and TP=1 and $(RE_{temp}(2)*RE_{temp}(4)*RE_{temp}(6)=0)$ and $(RE_{temp}(4)*RE_{temp}(6)*RE_{temp}(8)=0)$, we have to store the current central pixel row and column position or index value to one temporary matrix denoted as F1 with two columns and n number of rows.

| | | |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 1 | 1 |
| 1 | 0 | 0 |

| | | |
|---|---|---|
| 1 | 1 | 0 |
| 1 | 1 | 0 |
| 1 | 1 | 1 |

| | | |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 1 | 0 |
| 1 | 0 | 0 |

| | | |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 1 | 1 |
| 0 | 0 | 1 |

| | | |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 1 | 0 |
| 1 | 0 | 0 |

| | | |
|---|---|---|
| 1 | 1 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |

| | | |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 1 | 1 |

| | | |
|---|---|---|
| 1 | 0 | 0 |
| 1 | 1 | 0 |
| 1 | 1 | 1 |

| | | |
|---|---|---|
| 1 | 0 | 0 |
| 1 | 1 | 0 |
| 1 | 1 | 0 |

**Figure 3.28:** Examples of few different possibilities where thinning function is repeated

Where n represents a total number of central pixels which is having value 1 or which is a part of background pixels of the segmented image.

We trace eight neighbourhood pixel position values starting from 1 position to 8 through P. The statement can be expresses as

if ( $N_p$ >=2) & ( $N_p$ <=6) & ( $T_p$ ==1) & $\left(RE_{temp}(2) * RE_{temp}(4) * RE_{temp}(6) == 0\right)$ & $\left(RE_{temp}(4) * RE_{temp}(6) * RE_{temp}(8) == 0\right)$ (Eq. 3.16)

F1 (F+1, 1) = i and F1 (F+1, 2) = j where F is a temporary variable with initial value as 0.

Increment the value of F as F= F+1.

Figure 3.28 shows examples of different possibilities where temporary matrix F1 is initialized with the position of central pixel position. In general words, the nearby pixel of the central pixel, which contains foreground pixel has to be thinned. In figure 3.28 red color represents a central pixel.

All the central pixel positions are stored in temporary matrix F1 if it satisfies the Eq. 3.16. The F1 matrix corresponding to $I_{segment}$ image is reassigned with value 0, which is shown below.

$$I_{segment}\left(F1(i,1), F1(i,2)\right) = 0$$

The above statement is repeated from the first-row position of F1 to till last row position with fixed column size as 2. Next, we create another temporary variable $N_{F2}$ and initialize it with

value zero. Next, we repeat the same process starting from, if $I_{segment}$ (i, j) =1 to $I_{segment}\big(F2(i,1), F2(i,2)\big) = 0$. Until condition (F > 0 or $N_{F2} > 0$) fails, repeat all above steps for $I_{segment}$.

### 3.9.2 Edge Prediction based skeleton Formation Algorithm-Procedure

Input: Segmented Image, $I_{segment}$

Output: Skeletonised Image, $I_{skeleton}$

1. Find the row and column size of the segmented image, $I_{segment}$ and create a temporary variable F and assign F = 0
2. **for each pixel** of the segmented image **except first and last** pixel **do**

   Check the value of each pixel for 1, if $I_{segment}(i,j) = 1$

   Extract 3 × 3 sized image from $I_{segment}$ and store it in temporary image

   $temp = I_{segment}\big((i-1\ to\ i+1), (j-1\ to\ j+1)\big)$ // Where, i, corresponds to //individual pixels of $I_{segment}$

   Extract the ring structure pixel values; keep the i[th] pixel in the center and extract pixel values of 8 connected points and again the first-pixel to form ring structure. Create a temporary image as $RE_{temp}$

   **for each column pixel** of the temp image except last pixel

   $$RE_{temp}(i) = temp(1,i)$$

   $$RE_{temp}\Big(\big(C_{temp}-1\big) + \big(R_{temp}-1\big) + i\Big) = temp(R_{temp}, C_{temp} + 1 - i)$$

   **end for**

   **for each row pixel** of the temp image except the last pixel

   $$RE_{temp}\big(C_{temp} + i\big) = temp\big(1, C_{temp}\big)$$

   $$RE_{temp}\Big(\big(C_{temp}-1\big) + \big(R_{temp}-1\big) + i\Big) = temp(R_{temp} + 1 - i, C_{temp})$$

   **end for**

   $$RE_{temp}\big((C_{temp}-1) + \big(R_{temp}-1\big) + (C_{temp}-1) + \big(R_{temp}-1\big) + 1) = temp(1,1)$$

   Create a temporary variable to save the corresponding calculation as

   $$N_p = \frac{\left(\sum RE_{temp}\right)^2 - (RE_{temp}(1))^2}{\left(\sum RE_{temp}\right) + RE_{temp}(1)}$$

   **for all pixels** of $RE_{temp}$ -1 **do**

if $(RE_{temp}(i) = 0)$ & $(RE_{temp}(i+1) = 1)$

increment terminating point as, $T_p = T_p + 1$

**end if**

**end for**

**for all pixels** of $RE_{temp}$ -1 **do**

**if** ($N_p$>=2) & ($N_p$<=6) & ($T_p$=1) &$\big(RE_{temp}(2) * RE_{temp}(4) * RE_{temp}(6) = 0\big)$&$\big(RE_{temp}(4) * RE_{temp}(6) * RE_{temp}(8) == 0\big)$

Store pixel in another temporary variable F1.

F1(F+1,for all column)=[i j];

Increment index as, F=F+1

**end if**

**end for**

**end for**

3. Check for value of F, **if** (F>0)

**for each value** of F1 **do**

$I_{segment}\big(F1(i,1), F1(i,2)\big) = 0$ // delete from original image

**end for**

**end if**

4. $N_{F2} = 0$ // $N_{F2}$→Temporary Variable which will change for every iteration of for $loop$

Repeat step-2 except for some changes as

$N_p = \frac{\left(\sum RE_{temp}\right)^2 - (RE_{temp}(1))^2}{\left(\sum RE_{temp}\right) + RE_{temp}(1)}$ //$N_p$→ Temporary Variable to save the result of that // corresponding calculation

F2($N_{F2}+1, all\ column\ pixles$)=[i j];

$N_{F2} = N_{F2} + 1$

Increment index as, $N_{F2}$=$N_{F2}$+1

5. Check for value of $N_{F2}$, **if** ($N_{F2}$>0)

**for each value** of $F2$ **do**

$I_{segment}\big(F2\ (i,1), F2\ (i,2)\big) = 0$ // delete from original image

**end for**

**end if**

6. **if** (F>0 or $N_{F2} > 0$)

$I_{skeleton} = repeat\ all\ the\ steps\ for\ I_{segment}$

**end if**

### 3.9.3 Workflow and Flowchart of Edge Prediction based skeleton Formation Algorithm

The workflows of the proposed algorithm are shown using Figure 3.29. Figure 3.30 shows the Flowchart of this algorithm. Finding a number of edges for each central pixel is a very important calculation, because which decides, whether the central pixel is converted to zero or not. Indirectly also helps to decide, whether skeleton formation function should be repeated or not. The thinning process helps to reduce the ridge pattern to a single pixel wide or without discontinuities. The flowchart is shown below in Figure 3.30.

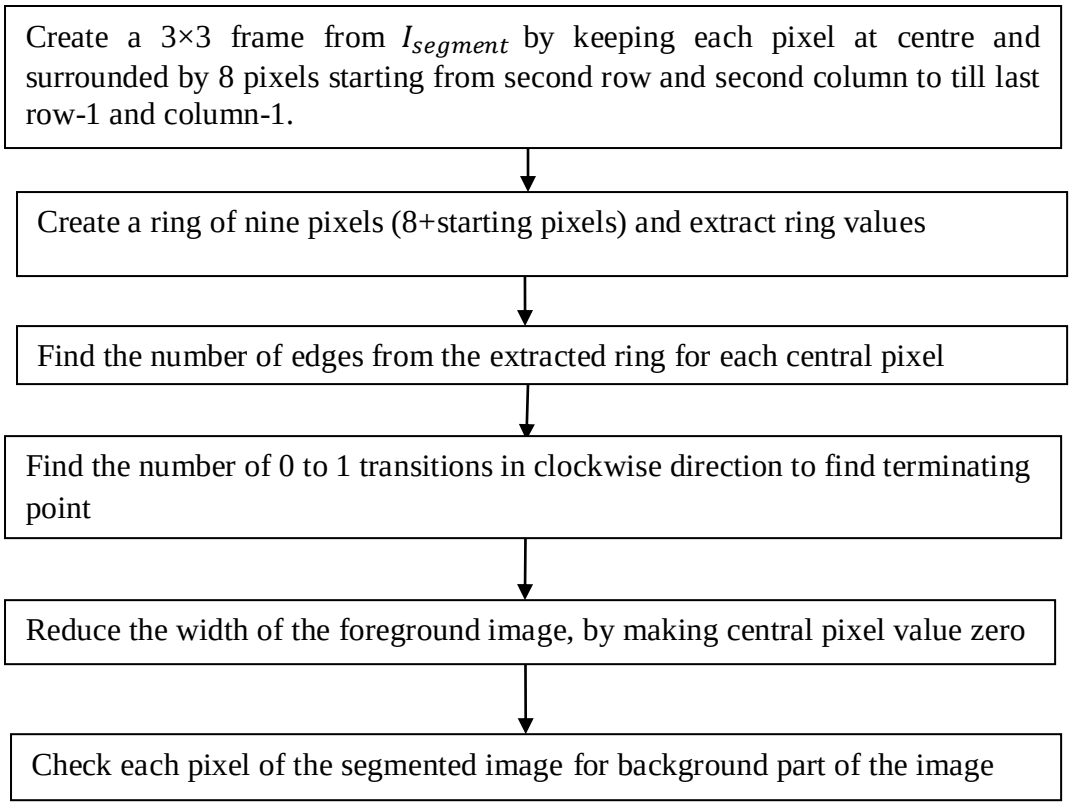
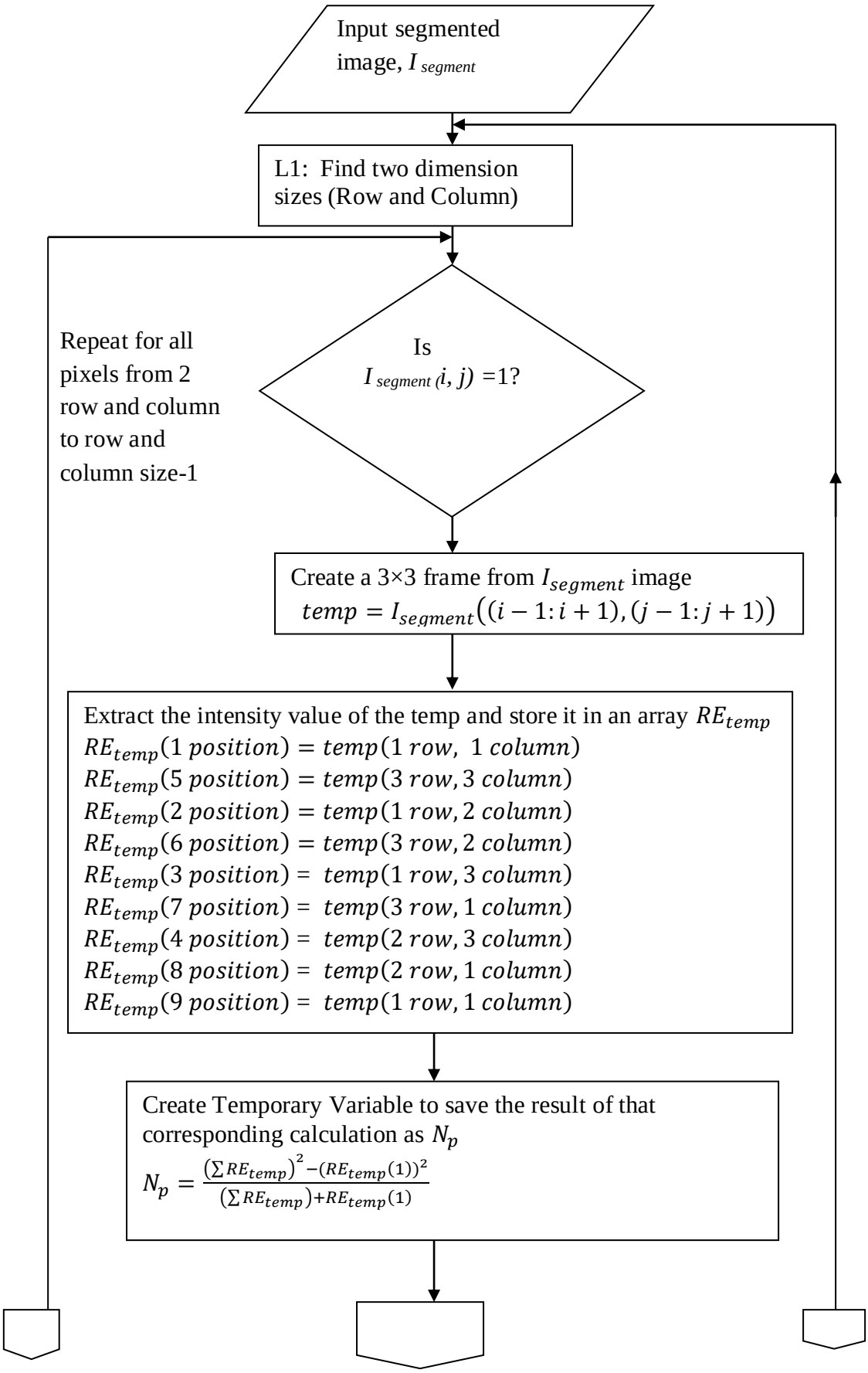
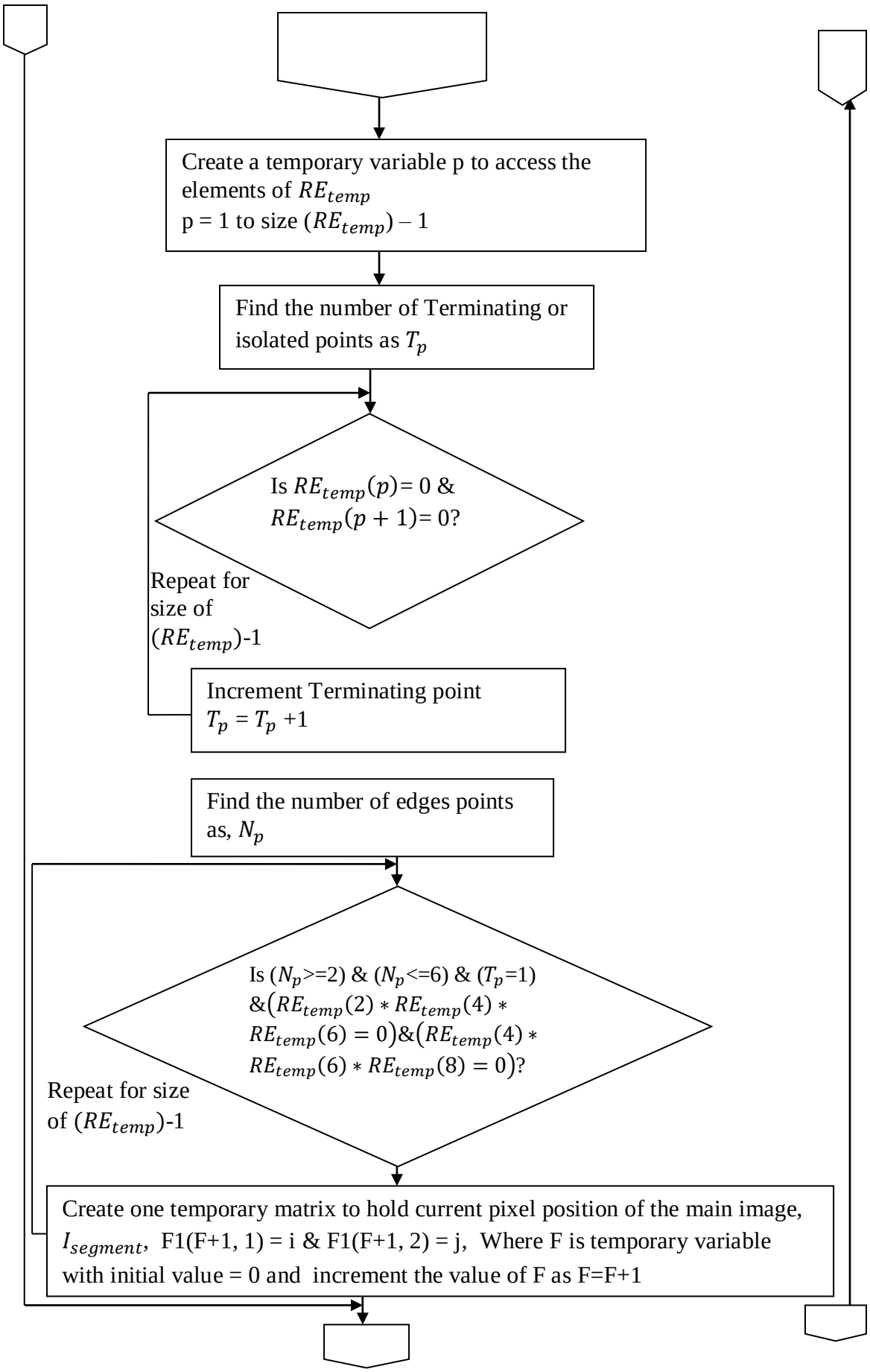



**Figure 3.29**: Work flow of Edge Prediction based Skeleton Formation Algorithm


Input segmented image, $I_{segment}$
L1: Find two dimension sizes (Row and Column)
Repeat for all pixels from 2 row and column to row and column size-1
Is $I_{segment}(i, j)$ =1?
Create a 3×3 frame from $I_{segment}$ image
$temp = I_{segment}((i-1:i+1),(j-1:j+1))$
Extract the intensity value of the temp and store it in an array $RE_{temp}$
$RE_{temp}(1\ position) = temp(1\ row,\ 1\ column)$
$RE_{temp}(5\ position) = temp(3\ row, 3\ column)$
$RE_{temp}(2\ position) = temp(1\ row, 2\ column)$
$RE_{temp}(6\ position) = temp(3\ row, 2\ column)$
$RE_{temp}(3\ position) = temp(1\ row, 3\ column)$
$RE_{temp}(7\ position) = temp(3\ row, 1\ column)$
$RE_{temp}(4\ position) = temp(2\ row, 3\ column)$
$RE_{temp}(8\ position) = temp(2\ row, 1\ column)$
$RE_{temp}(9\ position) = temp(1\ row, 1\ column)$
Create Temporary Variable to save the result of that corresponding calculation as $N_p$
$N_p = \frac{(\sum RE_{temp})^2 - (RE_{temp}(1))^2}{(\sum RE_{temp}) + RE_{temp}(1)}$


Create a temporary variable p to access the elements of $RE_{temp}$
p = 1 to size ($RE_{temp}$) – 1
Find the number of Terminating or isolated points as $T_p$
Is $RE_{temp}(p)$= 0 & $RE_{temp}(p+1)$= 0?
Repeat for size of ($RE_{temp}$)-1
Increment Terminating point $T_p$ = $T_p$ +1
Find the number of edges points as, $N_p$
Is ($N_p$>=2) & ($N_p$<=6) & ($T_p$=1) &$(RE_{temp}(2) * RE_{temp}(4) * RE_{temp}(6) = 0)$&$(RE_{temp}(4) * RE_{temp}(6) * RE_{temp}(8) = 0)$?
Repeat for size of ($RE_{temp}$)-1
Create one temporary matrix to hold current pixel position of the main image, $I_{segment}$, F1(F+1, 1) = i & F1(F+1, 2) = j, Where F is temporary variable with initial value = 0 and increment the value of F as F=F+1

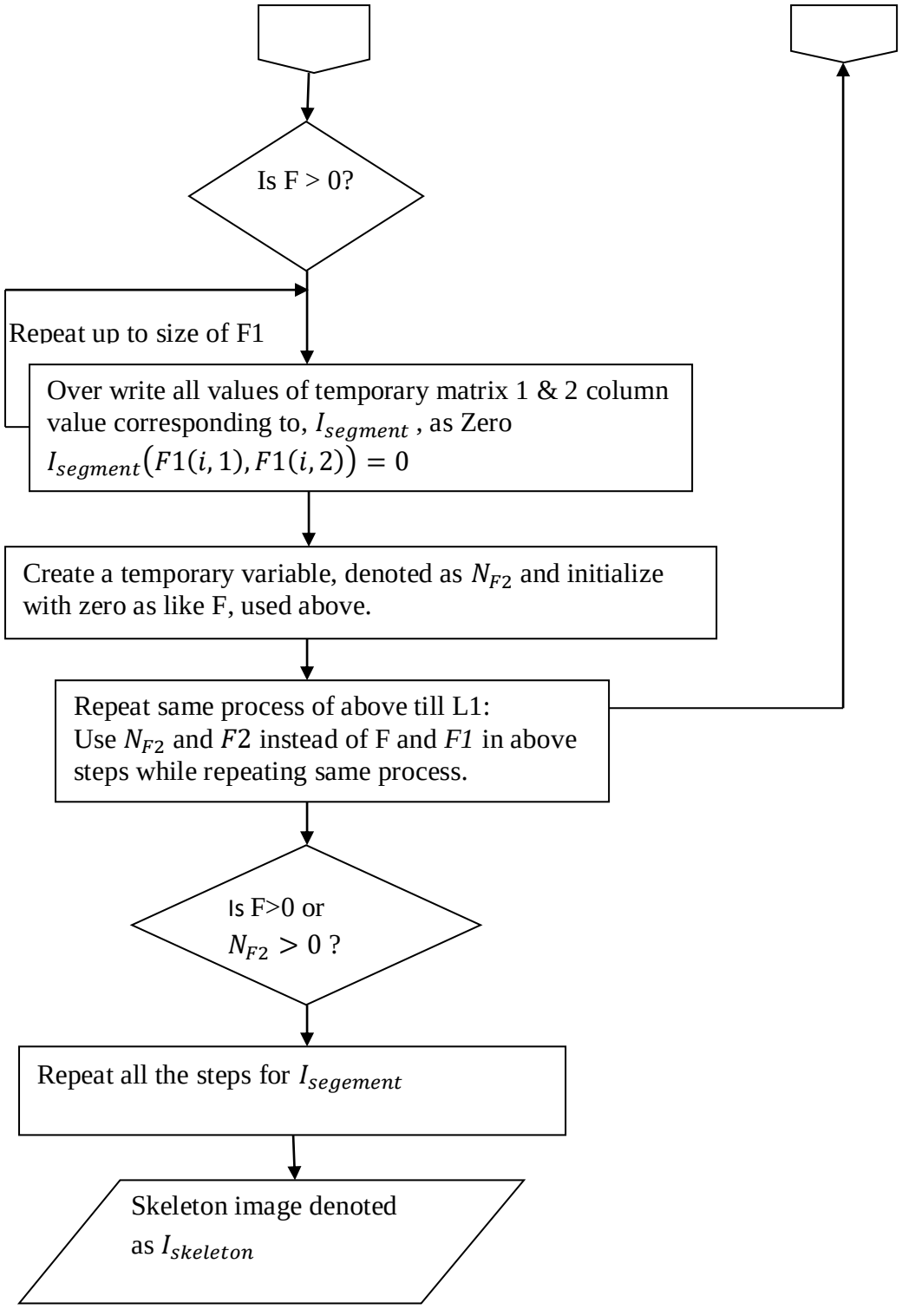



**Figure 3.30:** Flow chart for Edge Prediction based skeleton Formation Algorithm

### 3.9.4 Analysis of Edge Prediction based skeleton formation Algorithm

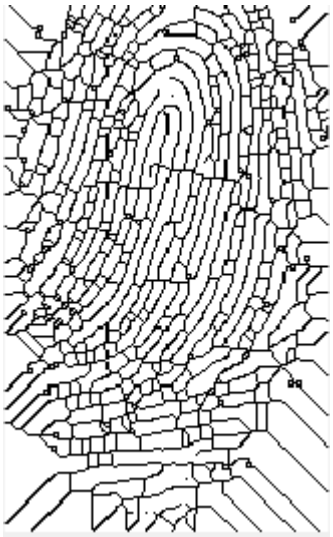
The Edge Prediction based Skeleton formation algorithm is analysed by considering FVC ongoing 2002 datasets. Figure 3.31 shows segmented image and skeleton image for sample

image 101_1.tif. In figure 3.31, 101_1.tif is a sample fingerprint image taken from FVC ongoing 2002 DB1_B dataset, which is of size 388 × 374 pixels. This image is initially converted into 256 × 256, before filtering process. After segmentation this image is again resized into 256 × 148. The figure 3.31 (a) represents this segmented image, and 3.31 (b) represents, its skeleton image. The skeleton image size is again resized into 254 × 146.

(a) Segmented image-101_1.tif

(b) Skeleton image of (a)

(c) Segmented image-105_1.tif



(d) Skeleton image of (c)

**Figure 3.31:** Example of Edge prediction based skeleton Formation

Same way, in figure 3.31, 101_5.tif is a sample fingerprint image taken from FVC ongoing 2002 DB1_B dataset, which is of size 388 × 374 pixels. This image is initially converted into 256 × 256, before filtering process. After segmentation, this image is again resized to 256 × 148. The figure 3.31 (c), represents this segmented image, and 3.31 (d) represents its skeleton image. The skeleton image size is again resized to 254 × 156. The edge prediction based skeleton formation is mainly based on Zang-Suen and time complexity of this algorithm is Big-Oh ($k \times n^2$), when k is greater than 1 and less than m or n. The m and n are rows and column size of the fingerprint image.

### 3.10 CHAPTER SUMMARY

In this chapter initially, we have discussed the research objectives and followed by the scope of the research. This research has mainly scope in internet banking or mobile banking or any other systems which utilizes client-server architecture. Next, we have discussed the Methodologies used in this research work. In this study there are six methods for Hash code generation and for all the six methods methodologies are shown with the help of diagrams. This chapter also discusses the fingerprint preprocessing technologies. The preprocessing techniques cover Contrast Adjustment or filtering or simply image enhancement, Segmentation, and Thinning or Skeletonisation. For Contrast Adjustment, we have proposed Tuning based filtering algorithm, which shifts the intensity values of the image to higher intensity values. For segmentation we have proposed modified algorithm called Surfeit clipping based Segmentation, which clips the background part of the image in all four directions as top, bottom, left, and which primarily makes use of canny edge detection method. Thinning or skeletonization of the segmented image is done with the help of edge prediction based skeleton formation algorithm. These entire three algorithms are discussed with the aid of Algorithm-procedure or steps, Workflow diagram, and Flowchart. The input for this algorithm is considered from FVC ongoing 2002 benchmark datasets.

*********

# CHAPTER FOUR

# *Fingerprint Feature Extraction & Hash Code Creation Phase*

**Contents** **Page No.**

## 4.1 INTRODUCTION

After the initial preprocessing, the feature is extracted from the fingerprint thinned image. Extraction of crucial and beneficial capabilities or features of interest from a fingerprint image is an essential venture during recognition. Feature extraction algorithms pick handiest or only applicable features important for enhancing the performance of matching and recognition rate and outcomes with the feature vector. The feature extraction methods or algorithms have to take the following points into consideration.

- The feature extraction algorithms or techniques require only relevant features like minutiae details and do not require any background details or domain-specific details.
- They need to be smooth or easy to compute with a purpose to gain a viable or practicable technique for a huge image series.

Minutiae details or fingerprint ridge ending or bifurcation details using skeletonized or thinning approach is a very popular method for feature extraction. Initially, the fingerprint image is preprocessed and the last stage of preprocessing is thinning. The preprocessing is usually consists of series of a process like filtering, image enhancement, binarization, segmentation and thinning. The binarized image after segmentation is then thinned using a set of policies that eliminate pixels from ridges till the ridges are one-pixel period or length (V. Espinosa, 2002). There are numerous strategies available in the literature for skeletonization or thinning method (Ahmed & ward, 2002; Patil et al., 2005; x. you, 2005). After extracting the minutiae from the thinned image a few post-processing is carried to cast off any spurious minutiae and final features of the fingerprint image are obtained.

However, techniques based totally on thinning are sometimes sensitive to noise and the skeleton shape does no longer relate to initial image. Nonskeletonized feature extraction uses a binary image based techniques. The main problem within the minutiae extraction technique the use of thinning processes comes from the reality that minutiae within the skeleton image do not usually correspond to true minutiae inside the fingerprint image. In fact, quite a few spurious minutiae are determined because of undesired spikes, breaks, and holes. Consequently, put up processing is usually followed to keep away from spurious minutiae, which are based on each statistical and structural fact after characteristic or feature detection.

In this research, we use either skeletonized or thinned image minutiae feature extraction based on crossing number and non-skeletonized feature extraction using statistical techniques. In both the techniques minutiae table and hashing code is used at the time of the matching process.

## 4.2 PREPROCESSING OF THINNED IMAGE

After skeleton formation or on thinned image some preprocessing operation is done in order to remove spurious minutiae or ridge patterns. We mainly use here morphological operation called erosion. The morphological establishing operation is blended with the morphological erosion and the dilation operations. Wherein erosion operation is implemented to shrink or thin an object and dilation operation is utilized to make bigger or thicken an object. In a Skeletonised, fingerprint image, white regions encompass background and some styles of noises. For obtaining an amazing and easier skeleton or minutiae features the provided set of rules adapts the morphological erosion operation to delete the white areas occupied via noise or to identify non-minutiae points.

An eight connected pixel mask is moved across the thinned image in order to remove white spaces or non-minutiae points. The 8-connected pixel mask is also called window. The window size is 3 × 3. The eight windows are obtained by keeping each pixel of the thinned image in a central position with value 1. If the 8-connected pixel mask with respect to this central position contains any edge means similar value (i.e. 1) in any one of the eight directions then central pixel is deleted. The 8 windows or pixel masks are shown below.

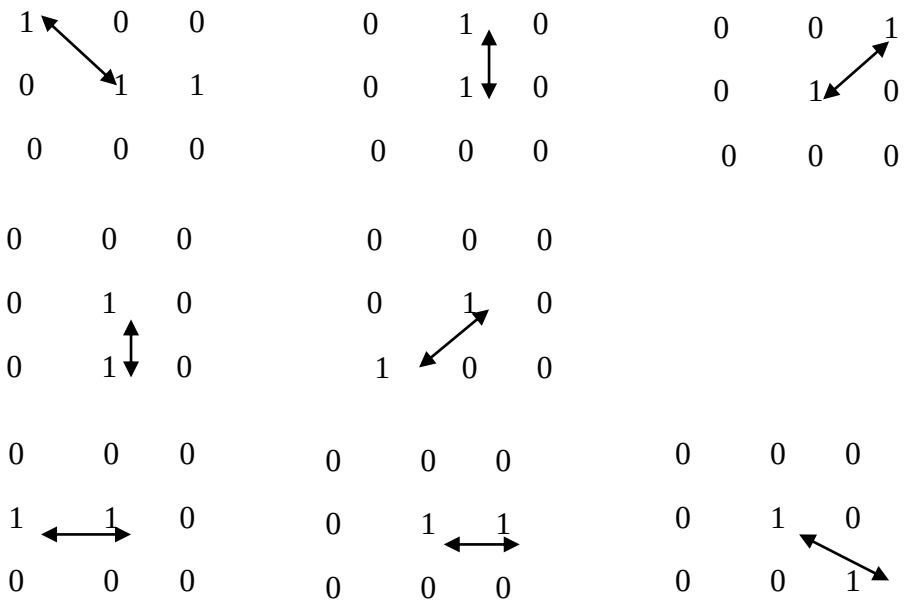


**Figure 4.1:** Eight windows of size 3 × 3 (pixel mask) used in skeleton preprocessing

The eight-pixel masks are in eight directions, North-West, South-West, South, North, South, South-East, West, and East from central pixel.

The preprocessing function is called twice with an intention to remove more non-minutiae points or simply to improve the efficiency. Here erosion is thinned the white spaces or non-minutiae points. The result of the first window is taken as input for the second window and so on till the last or 8th window.

### 4.2. 1 Algorithm for Preprocessing of Thinned image

This algorithm considers thinned image, $I_{skeleton}$ as input image and $I_{preprocessed1}$as output image for the first function call. $I_{preprocessed1}$ as input and $I_{preprocessed2}$as output image for

1. Initialise 8 windows which are shown below

$$temp_1 = erosion(I_{skeleton}, W_1) \quad \backslash\backslash \text{ w1= [1 0 0; 0 1 0; 0 0 0]}$$

$$temp_2 = erosion(temp_1, W_2) \quad \backslash\backslash \text{ w2= [0 1 0; 0 1 0; 0 0 0]}$$

$$temp_3 = erosion(temp_2, W_3) \quad \backslash\backslash \text{ w3= [0 0 1; 0 1 0; 0 0 0]}$$

$$temp_4 = erosion(temp_3, W_4) \quad \backslash\backslash \text{ w4= [0 0 0; 0 1 0; 1 0 0]}$$

$$temp_5 = erosion(temp_4, W_5) \quad \backslash\backslash \text{ w5= [0 0 0; 0 1 0; 0 1 0]}$$

$$temp_6 = erosion(temp_5, W_6) \quad \backslash\backslash \text{ w6= [0 0 0; 0 1 0; 0 0 1]}$$

$$temp_7 = erosion(temp_6, W_7) \quad \backslash\backslash \text{ w7= [0 0 0; 1 1 0; 0 0 0]}$$

$$I_{erosion} = erosion(temp_7, W_8) \quad \backslash\backslash \text{ w8= [0 0 0; 0 1 1; 0 0 0]}$$

$\backslash\backslash$ $I_{erosion}$→Erosion Applied image

2. Find the size of Erosion Applied image

$$[R_{erosion} C_{erosion}] = size(I_{erosion})$$

3. **for each pixel** of the $I_{erosion}$ image except first and last pixel do

Check for $I_{erosion}$ image pixel value, **if** $I_{erosion} = 1$

Assign to a temporary images of 3 × 3 size, as

$$temp1 = I_{erosion}(i-1:i+1, j-1:j+1)$$

temp2=[temp1(1,1);temp1(1,2);temp(1,3);temp(2,1),

temp(2,2),temp(2,3);temp(3,1);temp(3,2);temp(3,3);]

Initialize a counter as, counter=0;

**for each pixel** of temporary image **do**

Check, **if** (temp2 (1, k) = temp1 (1, k))

Increment counter, counter = counter +1

**end if**

**end for**

Check, if ( counter = 9 )

$I_{preprocessed1}$ (i, j) = 0 or $I_{preprocessed2}$ (i, j) =0

**end if**

**end for**

### 4.2.2 Workflow and Flowchart for Preprocessing of Thinned image

This above algorithm for Preprocessing of Thinned image is explained using a flowchart. The input for this algorithm is skeletonized or first processed image, which is represented as I_skeleton, and I_preprocessed1. The final output is preprocessed image denoted as I_preprocessed1 and I_preprocessed2. The Workflow of the preprocessing of the thinned image is shown in Figure 4.2.

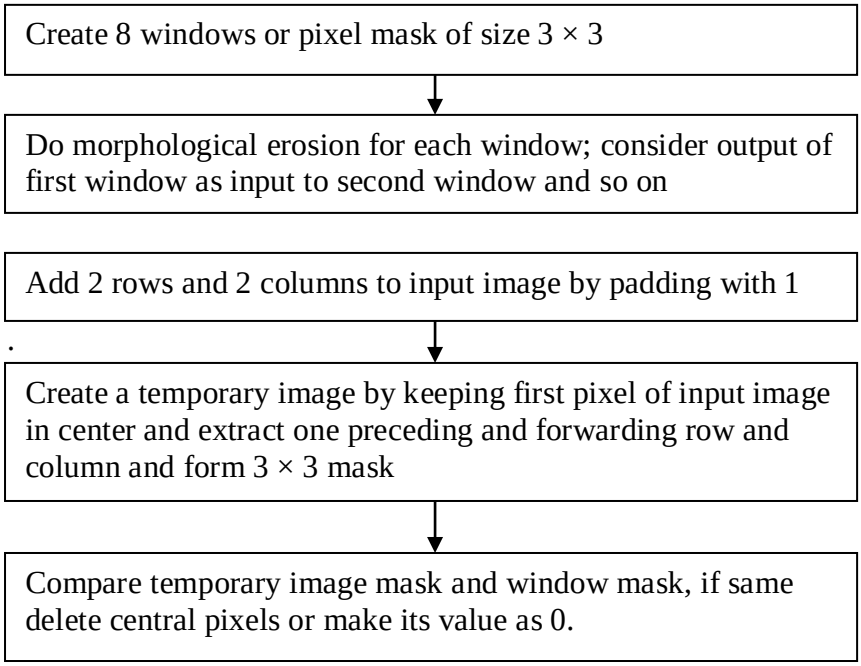



**Figure 4.2:** Workflow of the preprocessing of the thinned image

### 4.2.3 Flowchart for Preprocessing of Thinned image

The Flowchart of the preprocessing of thinned image is shown in Figure 4.3.

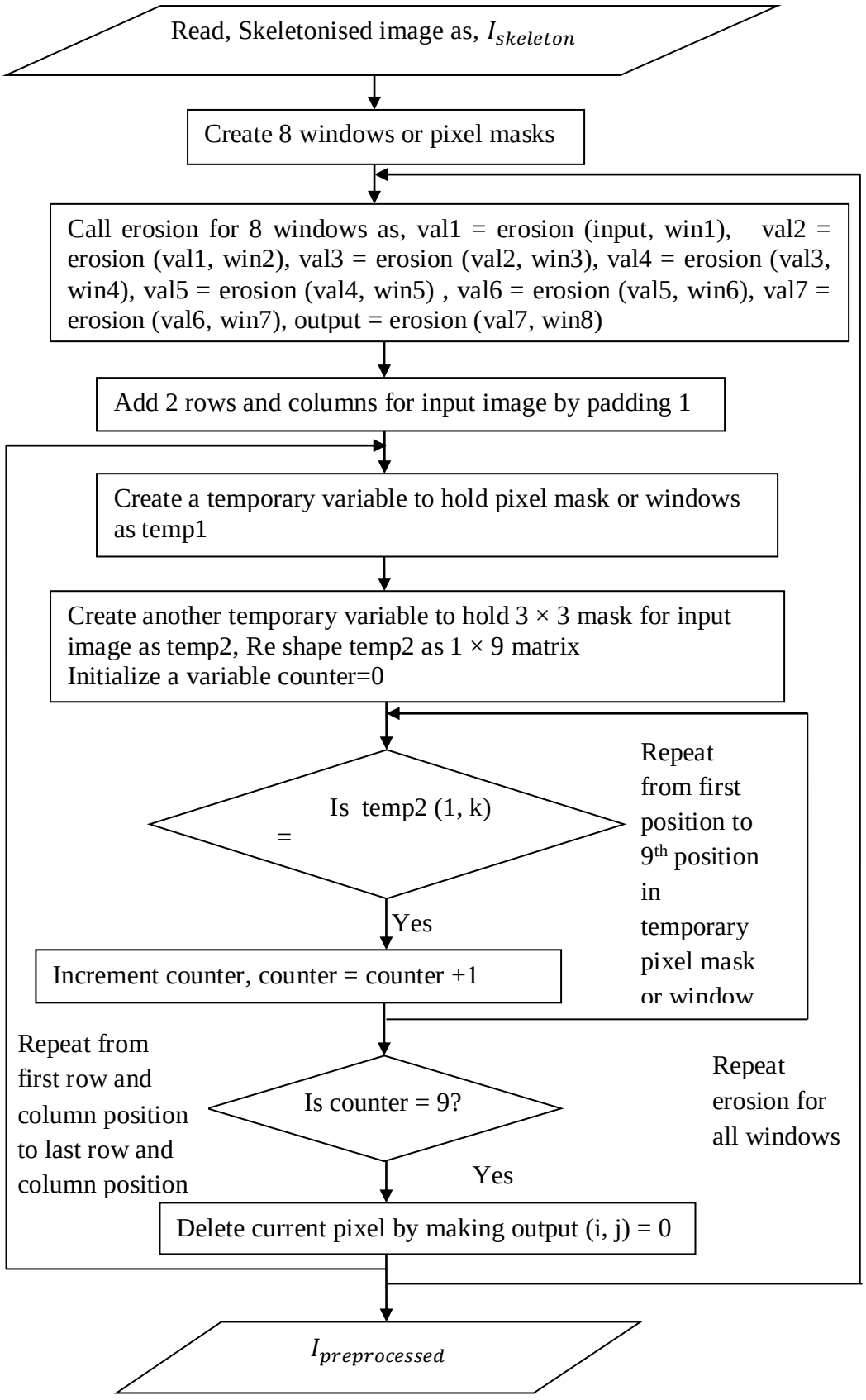



**Figure 4.3:** Flow chart for Preprocessing of Thinned image

### 4.2.4 Analysis of Preprocessing of Thinned image

Preprocessing for the thinned image is performed with an ultimate intention remove white spaces or non-minutiae points. Minutiae include ridge ending and ridge bifurcation, crossing, and isolated pixel and many more. But we concentrate only on ridge ending and bifurcation. Preprocessing removes white edges in all 8 directions. The table 4.1 shows thinned image pixel position removed for a 101_1.tif image taken from FVC ongoing DB1_B dataset.

**Table 4.1:** Thinned image pixel position removed during preprocessing

| Sr. No | Pixel Position of Input image | Window Value | Window Name | Function call name |
|---|---|---|---|---|
| 1 | (101, 46) | [[100]; [010]; [000]] | window1 | $preprocessing_1$ |
| 2 | (118, 103) | [[000]; [010]; [001]] | window6 | $preprocessing_1$ |
| 3 | (85, 45) | [[000]; [110]; [000]] | window7 | $preprocessing_1$ |
| 4 | (102, 09) | [[000]; [011]; [000]] | window8 | $preprocessing_1$ |
| 5 | (09, 100) | [[100]; [010]; [000]] | window1 | $preprocessing_2$ |
| 6 | (85, 44) | [[000]; [110]; [000]] | window7 | $preprocessing_2$ |
| 7 | (99, 44) | [[000]; [110]; [000]] | window7 | $preprocessing_2$ |
| 8 | (09, 102) | [[000]; [011]; [000]] | window8 | $preprocessing_2$ |

In table 4.1, column name, 'Function call name' values $preprocessing_1$ and $preprocessing_2$ indicates, preprocessing function called during first and second call respectively.

We call preprocessing functions twice with an intention to improve the efficiency of filtering process and thereby enhanced the efficiency of the matching process based on extracted features. The time complexity of pre-processing is Big-Oh ($n^2$ ).

## 4.3 FEATURE EXTRACTION TECHNIQUES

The individuality characteristic of the fingerprint is determined by the local ridge characteristics known as minutiae, which can be one of the most important standards utilized in fingerprint identification systems (Newham, 1995; Moenssens, 1975). There are more than one hundred fifty minutiae characteristics are diagnosed in literature. These local ridge

characteristics aren't similarly distributed. Minutiae are labeled in two sorts primarily based on minutiae factors as ridge ending and bifurcation. We concentrate only ridge ending and bifurcation. From a preprocessed thinned image, we can able to classify pixel positions into one of the possible 8-connected neighbors. A ridge pixel is called an isolated pixel if it does not contain any 8 connected neighbors. The ending is referred based on 8-connected neighbor having value 1. When 8-connected neighbor having value 3, then it's referred as bifurcation. If 8-connected neighbor having value exactly 4 then that is called as crossing.

The minutiae extraction processed defined in (Zhang & Suen, 1984), used a 3 × 3 pixel mask to find or search ridge ending and ridge bifurcations. This method caused some problems or flaws due to the ridge ending repository at borders and spurious bifurcation or false minutiae inside the fingerprint. To remove these false minutiae, a series of rules are used (Arcelli & Di, 1985). In this regard, usually, fingerprints are less corrupt. In this all the fingerprint ridge patterns located at the border of the image are referred as invalid, this is due to the fact that, while capturing fingerprint image through sensors or any other capturing device only finite or countable number of points are only in contact. In this research, we make use of crossing number based theory to extract minutiae details-ridge ending and bifurcations.

### 4.3.1 Crossing Number Theory

The preprocessed, thinned fingerprint image's ridge pixel usually contains only single pixel with value 1 or 0. Consider that (x, y) denote a pixel on a thinned ridge, and, p_0, p_1..... p_8, denotes its 8 neighborhood pixels. Because the number of minutiae detected is more, the possibility of correct result increases. The concept of the crossing number (CN) is initially used by kasaei et al., (1997), for the purpose of extracting the minutiae from thinned or skeleton image. The nearby pixel of every ridge pixel in the image has scanned the usage of a 3×3 window from which the minutiae are extracted as shown in Figure 4.3. The crossing number may be used to categorize a ridge pixel as a finishing, bifurcation or non-minutiae point. As an example, a ridge pixel with a crossing-number of zero will correspond to an isolated factor and a crossing number of 4 correspond to a crossing factor. The Rutovitz's, crossing number for a ridge pixel is found based on following formula

$$CN_p = \frac{1}{2}\sum_{i=1}^{8}|p_i - p_{i+1}| \quad \text{----------} \quad (4.1)$$

In eqs. (4.1) $p_i$ is a pixel value in the neighborhood of pixel p which is a central pixel with $p_i$ value is 1 or 0 and also, $p_1 = p_9$. The crossing number $CN_p$ at a point p is expressed as half of the cumulative total between pairs of adjacent pixels belonging to the eight- neighborhood of p and is shown in Figure 4.4.

| | | |
|---|---|---|
| P1 | P2 | P3 |
| P8 | P | P4 |
| P7 | P6 | P5 |

**Figure 4.4:** 3 × 3 neighbourhood of crossing number based feature extraction

A pixel is then categorized as a ridge finishing or ending if it has most effective one neighboring ridge pixel for p, and categorized as a bifurcation if it has 3 neighboring ridge pixels.

### 4.3.2 Minutiae Extraction Algorithm based on Crossing Number

In our study, minutiae are extracted from the preprocessed-thinned image using the crossing number theory. This algorithm takes I_preprocessed2 as input and produces output in the form of Minutiae table. The algorithm for feature extraction is as follows.

1. Find the row and column size of $I_{preprocessed2}$ and assign to the m and n
2. Declare a variable to hold number of neighborhood as, count=0
3. for each pixel of $I_{preprocessed2}$ except first and last pixel, **do**

Check, **if** $I_{preprocessed2}$(i, j) = 1

Create a temporary image of size 3 × 3 neighborhood

tempimg = $I_{preprocessed2}$ ( i-1 to i+1 , j-1 to j+1 )

Reshape temping and assign to temping1 as

tempimg1 = [ tempimg(1,1) ; tempimg(1,2) ; tempimg(1,3) ; tempimg(2,3) ; tempimg(3,3) ; tempimg(3,2) ; tempimg(3,1) ; tempimg(2,1) ; tempimg(1,1) ]

Declare a variable to hold crossing number count and initialize with value 0

$$N_c = 0$$

**repeat for** 8-connected neighbour

$$N_c = N_c + |temp1(k) - temp1(k+1)|$$

**end for**

Divide value of $N_c$ by 2, $N_c = 0.5 * N_c$

Check, if ($N_c = 1$) or ($N_c = 3$)

Increment the count as count = count+1

Assign to $M_{table}$ as, $M_{table}(Count, :) = [i, j, N_c, (i + j + N_c)]$

\\$M_{table}$ → Minutiae Table

**end if**

**end for**

### 4.3.3 Workflow and Flowchart for Minutiae extraction based on crossing number

The above algorithm for Minutiae extraction based on crossing number is explained using a flowchart. The input for this algorithm is preprocessed thinned image, I_preprocessed2. The final output is Minutiae Table, represented as, M_table. The workflows of the crossing number based minutiae extraction are shown using Figure 4.5. The flowchart of this is shown in figure 4.6.

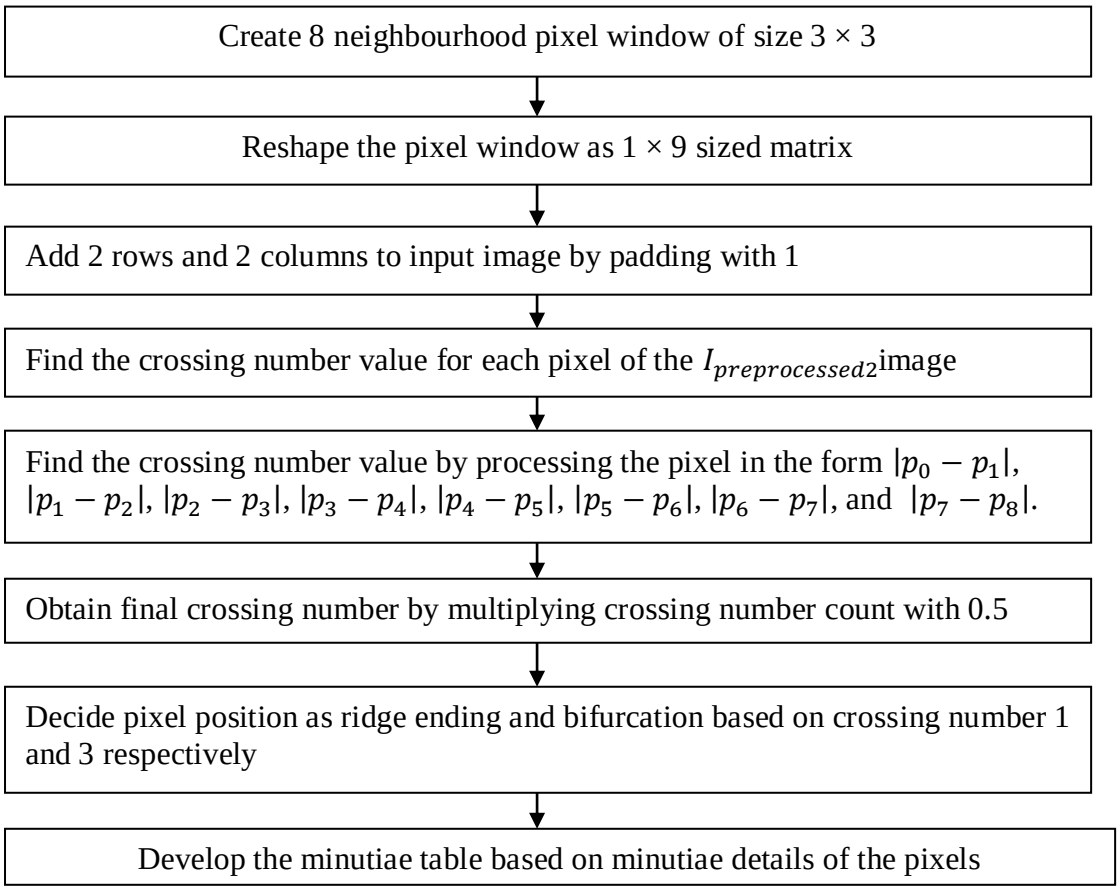



**Figure 4.5:** Workflow of the minutiae extraction using crossing number theory

.

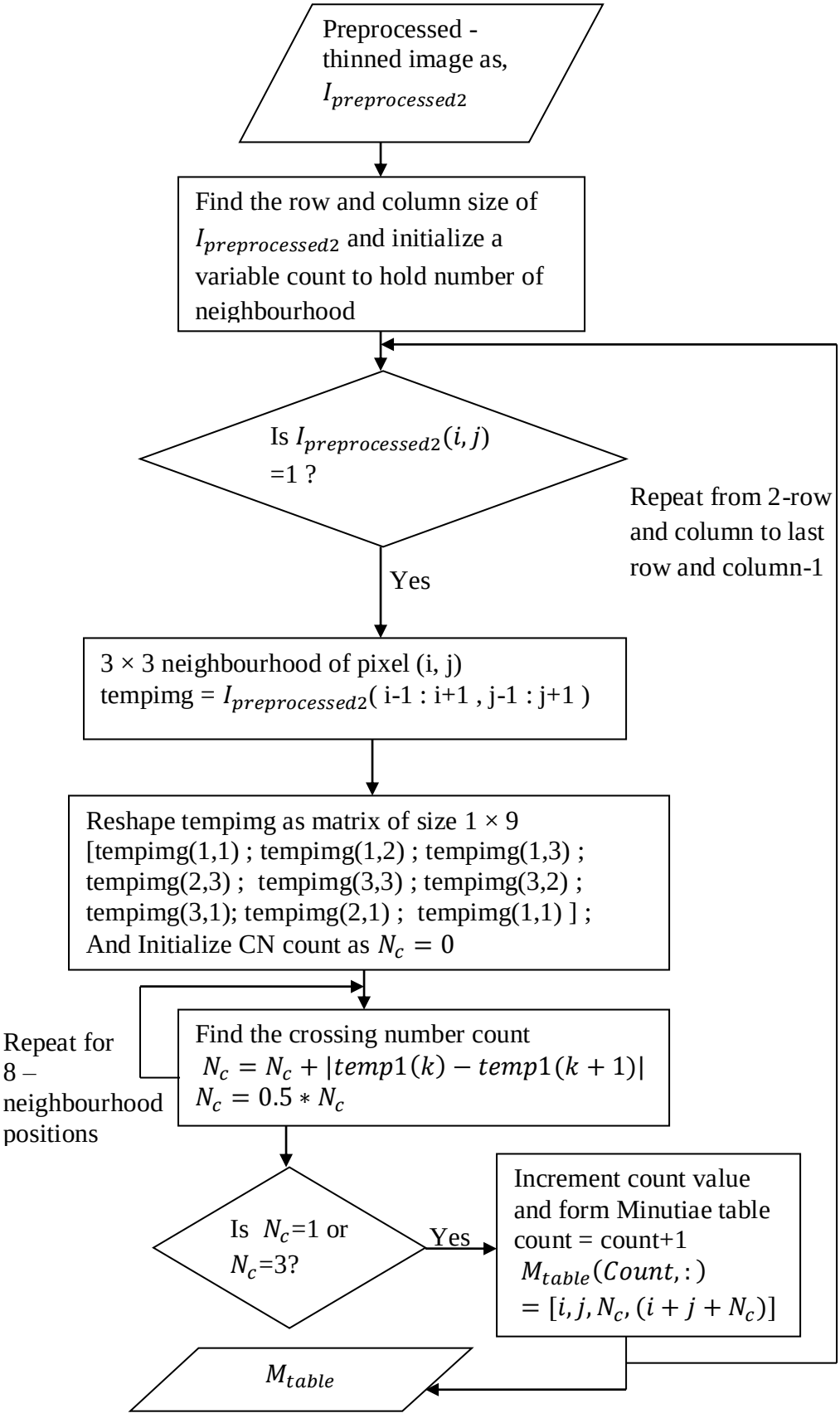
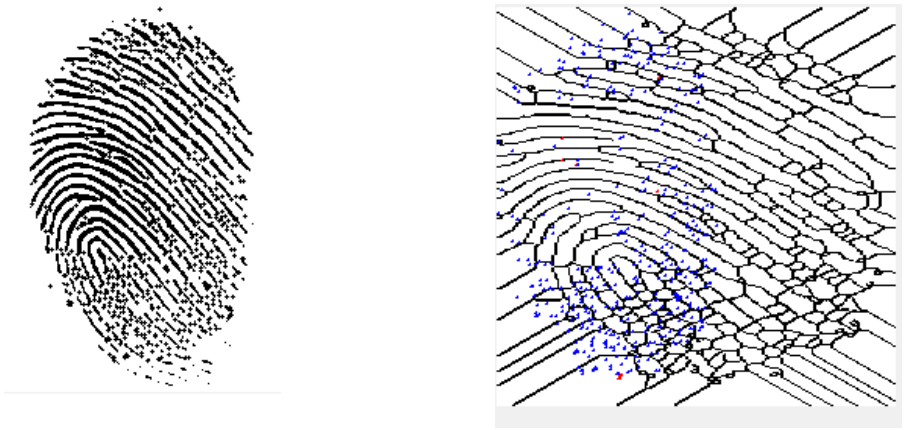



**Figure 4.6:** Flowchart for Minutiae extraction based on crossing number

### 4.3.4 Analysis of Minutiae extraction based on Crossing Number

To analyze and test Minutiae extraction based on crossing number, FVC ongoing 2002 benchmark datasets are used. Figure 4.7 shows ridge and bifurcation for the 101_1.tif image. A ridge ending is shown in red color and bifurcations are in green color. Time complexity of this process is Big-Oh ($n^2$)



(a) Minutiae point on the image (b) Minutiae points on the skeleton

**Figure 4.7:** Minutiae points on image and skeleton

### 4.4 Post processing- Processing Minutiae Table

After applying fingerprint image preprocessing on raw fingerprint, which includes filtering, enhancement, binarization, and segmentation thinned image or skeleton is formed. Further skeleton or thinned image is preprocessed to remove white areas occupied by the noise. Again preprocessed thinned image is further post-processed to remove some false minutiae from minutiae table and which is generated through crossing number theory. One greater reason for post-processing is to reduce the wide variety of minutiae points by disposing of false minutiae structures (Maltoni et al., 2003). The post-processing algorithm used in this study is based on Akram et al., 2008, here w × w window neighborhood is considered for each minutia in minutiae table. The size of the w is calculated on the basis of the following statement,

w = 2d + 1, where d is considered as local ridge distance.

In this study, we consider d as 1 unit. The window, w = 2×1+1 = 3. Average ridge distance in each region or from every pixel is usually referred as local ridge distance and it is an integer value due to round off calculation. The fingerprint image minutiae ridge ending and

bifurcation is first analyzed from the thinned image and in this study which is thinned preprocessed image.

The minutiae extracted through crossing number based theory may include some spurious minutiae structure, which should be eliminated to maximum extent or full with the aid of post-processing the preprocessed thinned image. If the 3×3 window is considered, then m along the branch of the window in all 8-directions and test whether any other ending in terms of pixel value 0→1 is not found then consider that pixel as true ridge.

**4.4. 1 Post processing Algorithm-Description**

The post-processing algorithm takes three arguments as Skeleton image after preprocessing, I_preprocessed2, Minutiae table, M_table, and window size represented as param in our study (Krishna Prasad, K., & Aithal P. S., 2018b). The output of this algorithm is final Minutiae table represented as final_M_table. This Minutiae Table contains five columns. The first column contains a serial number. The second column contains minutiae x position, third column minutiae y position and fourth ridge ending or bifurcation as code 1 or 3 and the fifth column contains the sum of a second, third and fourth column. Initially, some variables are declared and initialized with some values as follows. This algorithm is explained based on window size 3 × 3.

window = param / 2

If window variable value is not integer then round off it. For example in this study param value is 3 means, after round off window value will be 1. Create two matrixes, Rw and Clmn, of size 3 × 1 for holding indices of nonzero elements in the matrix.

Rw = zeros (3, 1), Clmn = zeros (3, 1)

Add two rows and columns for $I_{preprocessed2}$ image by padding value 0. Next find the total number of values or rows in $M_{table}$. Use a variable, count, to hold index position for final_$M_{table}$ maxval = size ($M_{table}$ ), count =0

$I_1$=$I_{preprocessed2}$ after padding 2 row and 2 column with value 0

Move along the minutiae table, $M_{table}$ from 1 row or position to last row or position. Use a variable part1 of size 3 × 3 to hold pixel values of the $I_1$ image, corresponding to $M_{table}$ minutiae pixel position.

part1= $I_1$( $M_{table}$ (i$^{th}$ row) to $M_{table}$ (i$^{th}$ row) + 2, $M_{table}$ (i$^{th}$ column) to $M_{table}$ (i$^{th}$ column) + 2 ) Here i, represents $M_{table}$ index from first position to till last position.

Because we have padded 2 row and 2 column on both sides of the $I_1$ the minutiae pixel position occupies central position of the window. All those pixel positions which are having

value 1 around the neighborhood of central pixel are referred as connected with a candidate or central pixel.

Initially, part1 is multiplied by -2 so that in the window all elements which are having value 1 become, -2. Next, we initialize central or candidate pixel with value -1.

partI = -2 * partI ;

partI (Window+1 , Window+1 ) = -1 ; // Here window value is 1 because the param value is 3. The Window size is 3 × 3. So it refers in this context, candidate pixel with value, PartI (2, 2). Next again another variable is created as temppart1 with size w × w with initial value zero.

temppart1 = w × w sized matrix with initial value 0.

This temppart1 will be copied with a value of part1 and candidate pixel will be assigned with value zero. Next, find the number of connected branches of candidate pixel by identifying non-zero window element pixel position and store it on Rw and Clmn as mentioned above.

[Rw, Clmn] = find (non-zero index position of temppart1 in row and column matrix)

The above statement simply returns no of connected branches of candidate minutiae pixel. Next, we check whether candidate pixel is minutiae ending or bifurcation. If $M_{table}$ 3, column value 1 means its ridge ending, and 3 means ridge bifurcation, which is based on crossing number based theory. If there exists, only one edge out of the all edges of the windows of candidate pixel, with the transition as, 0→1 and count=1, then it's considered as true ridge ending. If the candidate pixel is ridge bifurcation then check for transition 0→1, 1→2, and 2→3, then and the count is 1 for each transition then its valid ridge bifurcation, while evaluating all edges of the candidate minutiae pixel.

**4.4.2 Post Processing of Minutiae Table- Algorithm**

Input: $I_{preprocessed2}$, $M_{table}$, Output: final_$M_{table}$

Parameters: $I_{preprocessed2}$, $M_{table}$, Window size (param)

1. Initialize a variable window as, window = round (param / 2) //take integer value
2. Declare a variable Rw and Clmn to holds indices of nonzero elements in the matrix, Rw(3,1) with initial value 0, Clmn (3,1) with initial value 0
3. Initialize a new image as $I_1$=$I_{preprocessed2}$ after padding 2 row and 2 column with value 0
4. Find the size of $M_{table}$ as, size($M_{table}$ ) // $M_{table}$-Minutiae Table
5. Initialize a variable Count to hold total number of rows of $M_{table}$ , Count = 0
6. **for all** values of $M_{table}$ **do**

Extract w × w sized window from $I_1$

Initialize a temporary variable part1 as

part1= $I_1$( $M_{table}$ (i$^{th}$ row) to $M_{table}$ (i$^{th}$ row) + 2, $M_{table}$ (i$^{th}$ column) to $M_{table}$ (i$^{th}$ column) + 2 )

Multiply part1 by -2, Part1 = -2 * Part1

Initialize part1 candidate pixel value as -1, part1 ( window+1 , window+1 ) = -1

Create a temporary variable as temppart1 with size w × w with initial value zero to hold window value and copy part1 to temppartI

temppart1 ( param , param ) dimension with value 0.

tempPart1( Window to Window+2 , Window to Window+2 ) = part1( Window to Window+2 , Window to Window+2 )

Initialize temppart candidate pixel value to zero.

temppart1 ( Window+1 , Window+1 ) = 0 ;

find (non-zero index position of temppart1 in row and column matrix) and assign to Rw and Clmn

Check **if** candidate pixel is ridge ending or bifurcation, if it is 1 then ridge ending, if, 3 then ridge bifurcation

if ( Table(i, 3)= =1 )

Create a window Test with value zero of size w× w

Test (param, param) with value 0

Find the maximum value of non-zero index position of Rw or simply Size of Rw as, Max= size (Rw)

Traverse from first position of Rw to Max or last position

**for each value** of Rw **do**

Check the connected branch of Part1 with candidate minutiae pixel or simply check for value, -2.

if ( PartI( Rw(z) , Clmn(z) ) = = -2 )

Reassign Test window with value 1 Test( Rw(z) , Clmn(z) ) = 1 ;

**end if**

**end for**

Check whether candidate pixel has only one connected edge or border by calling extract_ring method

borders = extract_ring ( Test )

Initialize a variable to hold count for ridge ending to ensure that it has only one connected edge

T01 = 0

Traverse from first position of the border to last position minus one

**for each value** of border-1 **do** //all the w × w size-1 borders

Check, **if** (Borders(p)= 0) & (Borders(p+1)= 1) )

increment count T01 → T01 = T01 + 1

**end if**

**end for**

Ensure that T01 has only one connected edge

Check, **if** ( T01 = 1 )

Increment final_$M_{table}$ index by one

Count = Count + 1 ;

Load candidate minutiae pixel in final_$M_{table}$

final_$M_{table}$ (Count, 1) = $M_{table}$ ( i , 1 ) // row index of candidate pixel

final_$M_{table}$ (Count, 2) = $M_{table}$ ( i , 2 ) //column index of candidate pixel

final_$M_{table}$ (Count, 3) = $M_{table}$ ( i , 3 ) //type of ridge (ending or bifurcation)

final_$M_{table}$ (Count, 4) = $M_{table}$ ( i , 4 ) //sum of row, column, and type of ridge

**end if**

**else** part of candidate ridge type, means bifurcation

check that candidate minutiae pixel has at least three connected branches

**if** size(Rw(1))>=3 && size(Clmn(1))>=3

Name first 3 connected branch with candidate minutiae pixel as 1, 2, and 3 edges or branches (Minimum 3 branches are required if its bifurcation)

Part1( Rw(1) , Clmn(1) ) = 1

Part1 ( Rw(2) , Clmn(2) ) = 2

Part1 ( Rw(3) , Clmn(3) ) = 3

Assign Part1 to temporary variable Test1

Test1 = Part1

Check whether candidate pixel has three connected edge or border by

calling for all three marked edges

Borders = extract_ring ( Test1 )

Initialize a variable to hold count for ridge bifurcation to ensure that it has exactly three connected ridges means 6 points while traversing along all connected points

T01 = 0

Traverse from first position of the border to last position minus one for marked edge-1, edge-2 and edge-3

**for each value** of border-1 **do** //all the w × w size-1 borders

**if** (Borders(p)=0) & (Borders(p+1) =1) (Borders(p) =0) & (Borders(p+1)=2) (Borders(p) =0) & (Borders(p+1) =3))

increment count T01 → T01 = T01 + 1

**end if**

**end for**

Ensure that T01 has only three connected edge

**if** ( T01 = = 3 )

Increment final_$M_{table}$ index by one

count = count + 1

Load candidate minutiae pixel in final_$M_{table}$

final_$M_{table}$ (Count, 1) = $M_{table}$ ( i , 1 ) // row index of //candidate pixel

final_$M_{table}$ (Count, 2) = $M_{table}$ ( i , 2 ) //column index of //candidate pixel

final_$M_{table}$ (Count, 3) = $M_{table}$ ( i , 3 ) //type of ridge (ending //or bifurcation)

final_$M_{table}$ (Count, 4) = $M_{table}$ ( i , 4 ) //sum of row, column, //and type of ridge

**else** part of if ( T01 = = 3 )

**if** size(Rw(1))<3 && size(Clmn(1))<3

continue with next iteration

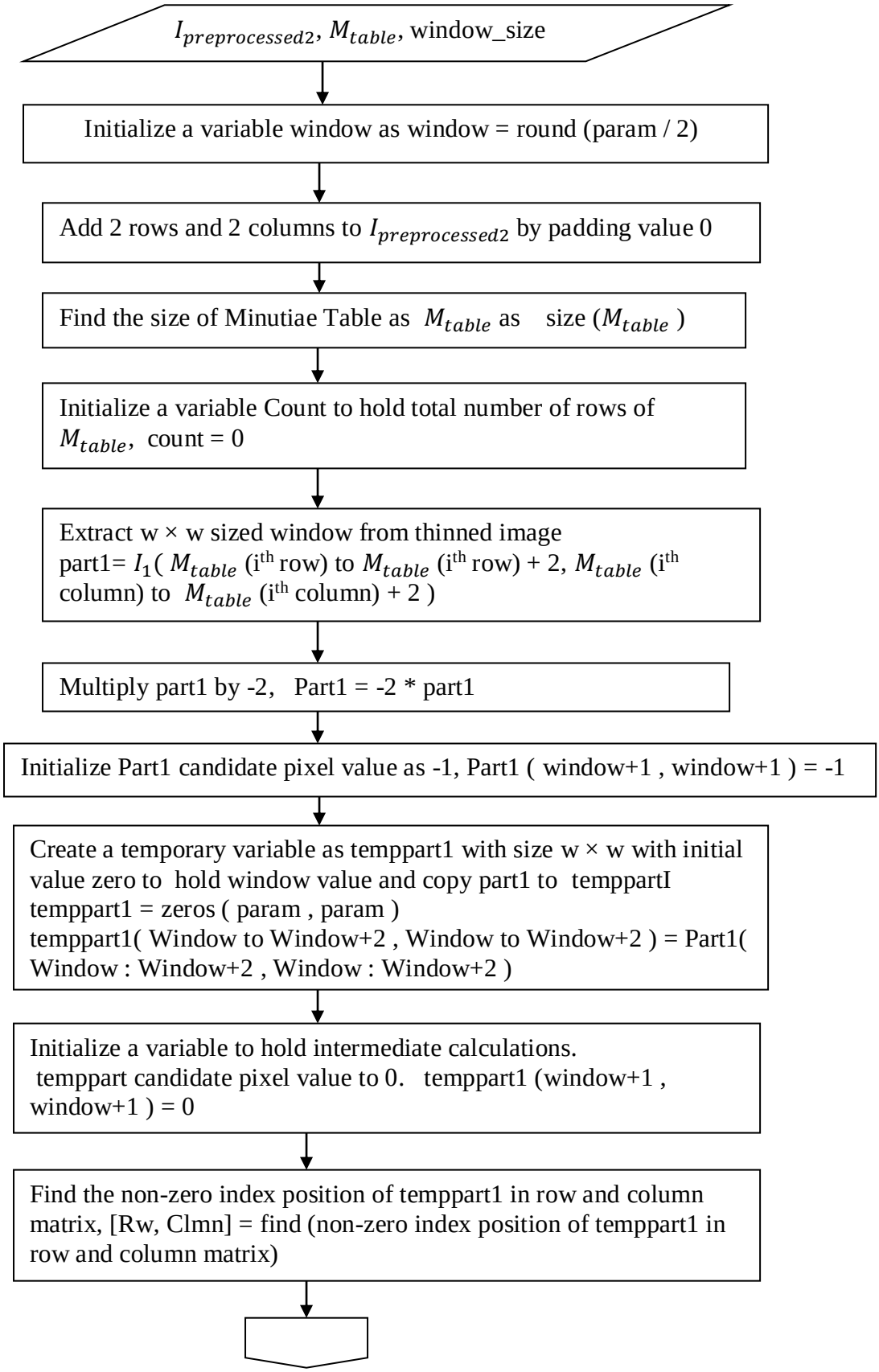
**end if**

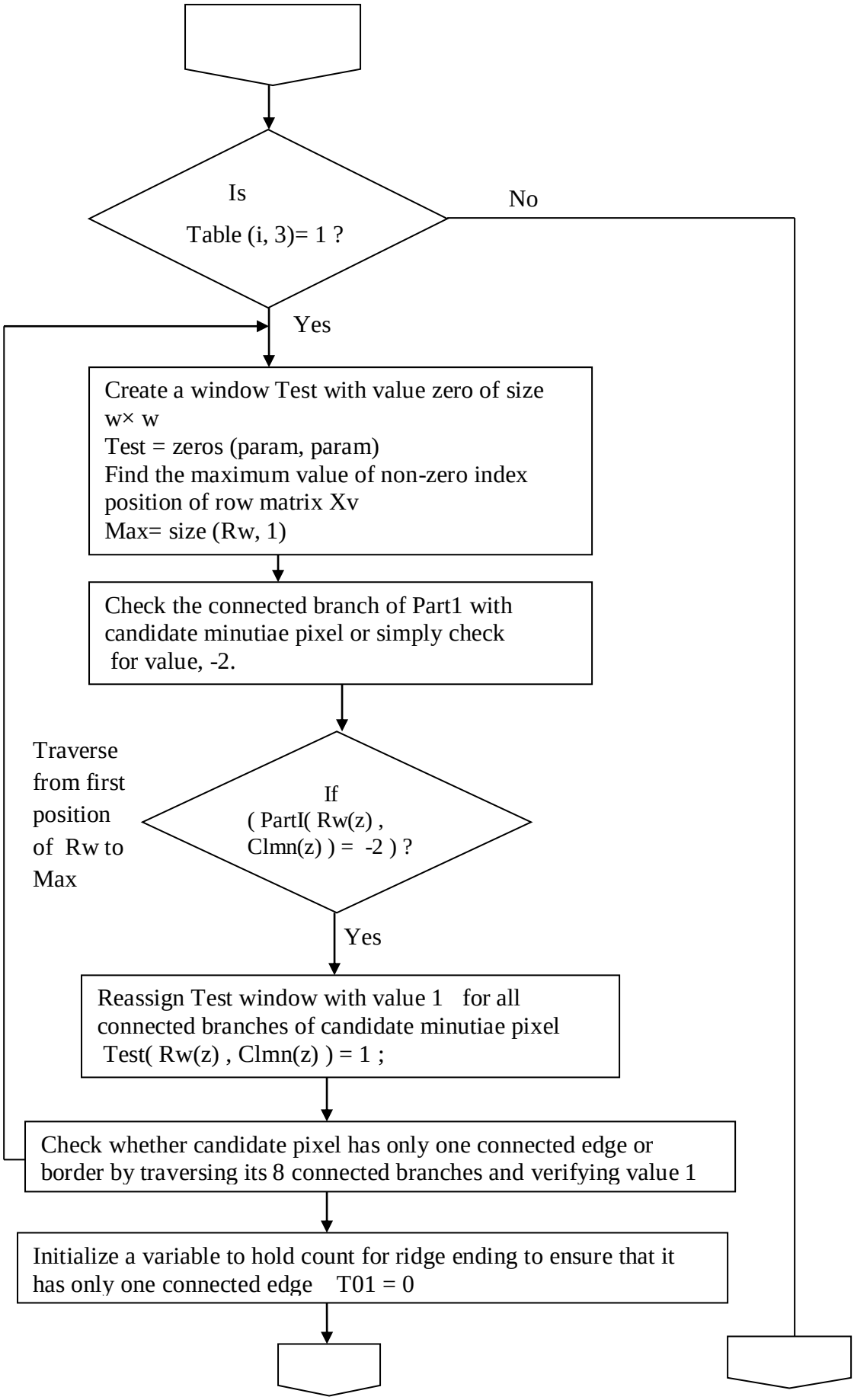
**end if**

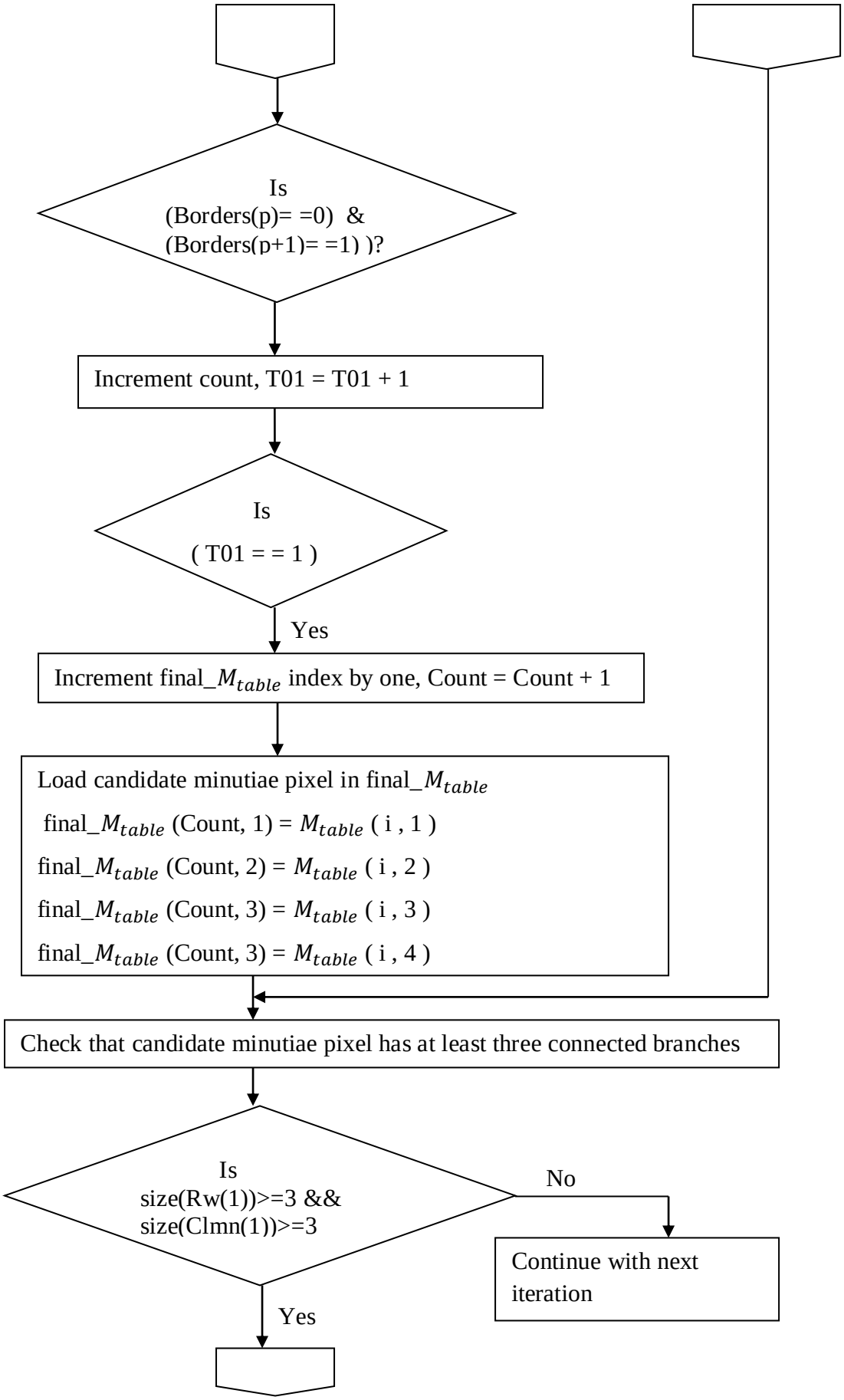
**end for**

### 4.4.3 Post Processing of Minutiae Table- Flowchart and Workflow

The Flowchart and workflow is explained using Figure 4.8 and 4.9 respectively.




Is
Table (i, 3)= 1 ?
No
Yes
Create a window Test with value zero of size w× w
Test = zeros (param, param)
Find the maximum value of non-zero index position of row matrix Xv
Max= size (Rw, 1)
Check the connected branch of Part1 with candidate minutiae pixel or simply check for value, -2.
Traverse from first position of Rw to Max
If
( PartI( Rw(z) , Clmn(z) ) = -2 ) ?
Yes
Reassign Test window with value 1 for all connected branches of candidate minutiae pixel
Test( Rw(z) , Clmn(z) ) = 1 ;
Check whether candidate pixel has only one connected edge or border by traversing its 8 connected branches and verifying value 1
Initialize a variable to hold count for ridge ending to ensure that it has only one connected edge T01 = 0


Is
(Borders(p)= =0) &
(Borders(p+1)= =1) )?
Increment count, T01 = T01 + 1
Is
( T01 = = 1 )
Yes
Increment final_$M_{table}$ index by one, Count = Count + 1
Load candidate minutiae pixel in final_$M_{table}$
final_$M_{table}$ (Count, 1) = $M_{table}$ ( i , 1 )
final_$M_{table}$ (Count, 2) = $M_{table}$ ( i , 2 )
final_$M_{table}$ (Count, 3) = $M_{table}$ ( i , 3 )
final_$M_{table}$ (Count, 3) = $M_{table}$ ( i , 4 )
Check that candidate minutiae pixel has at least three connected branches
Is
size(Rw(1))>=3 &&
size(Clmn(1))>=3
No
Continue with next iteration
Yes

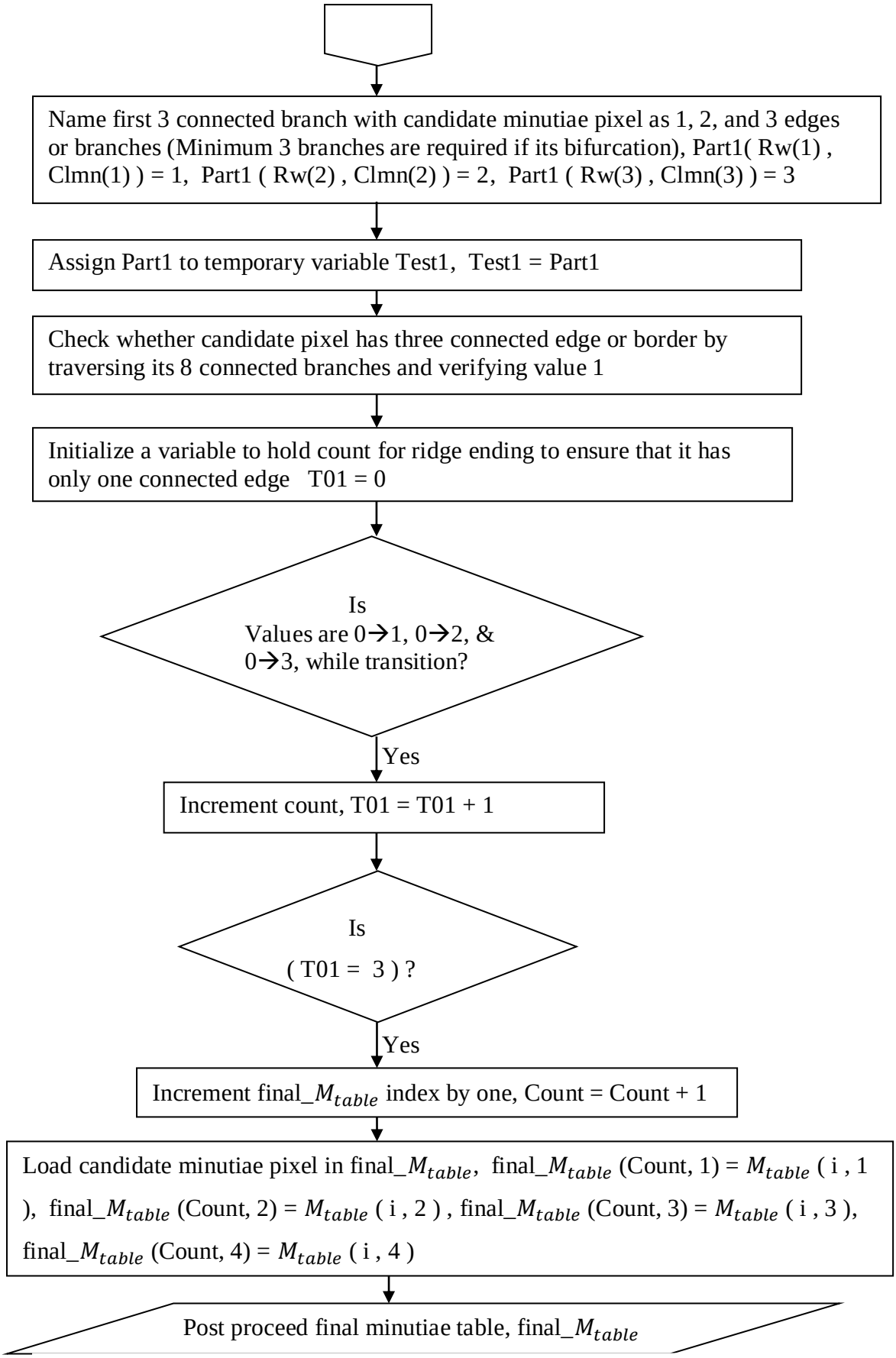



**Figure 4.8:** Flow chart for post processing of Minutiae Table

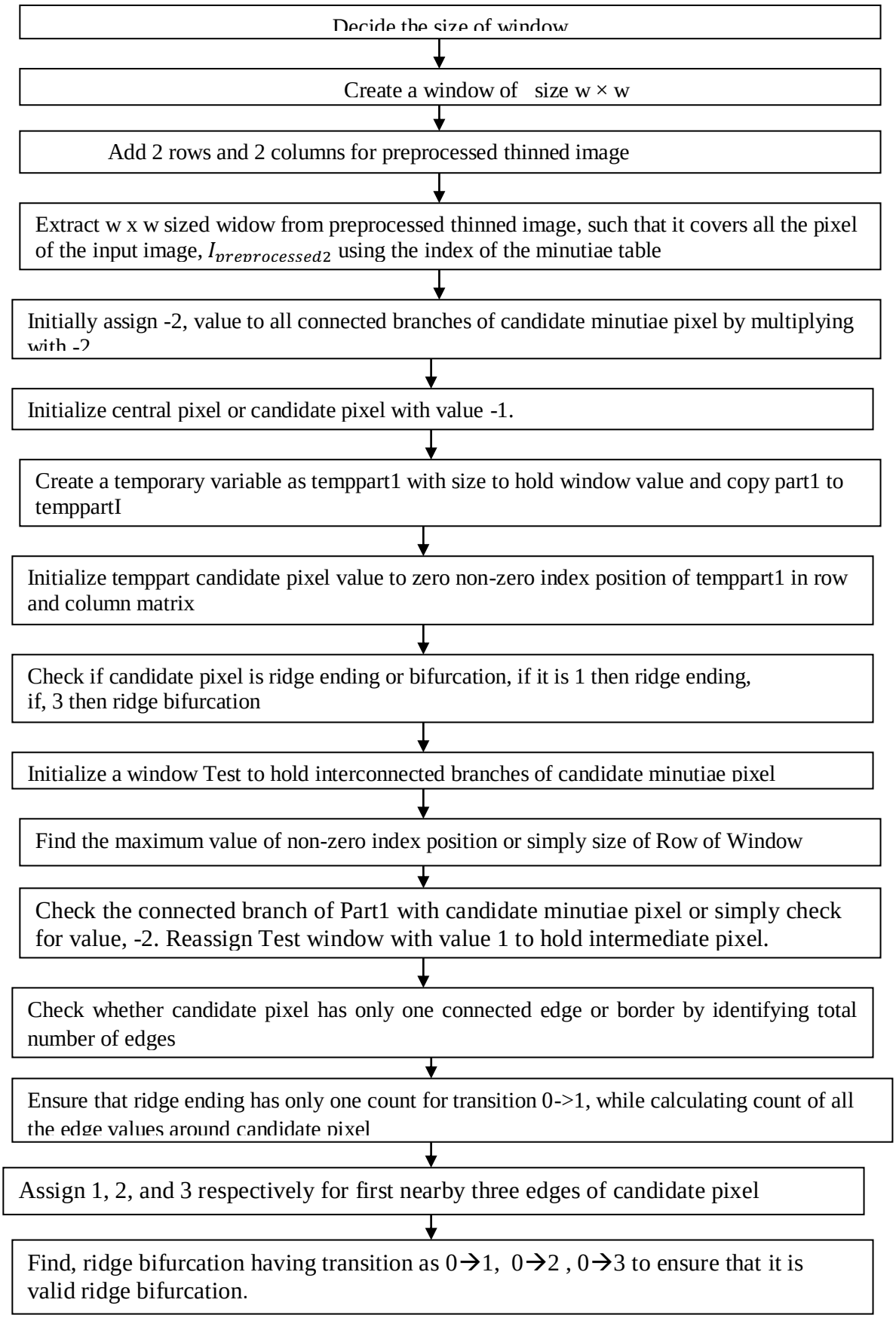



**Figure 4.9:** Workflow of Post Processing of Minutiae Table

### 4.4.4 Analysis of Post processing Minutiae Table

The Post-processing of minutiae is used to eliminate false minutiae structures occurred due to spurs, ride breaks, short ridge, holes or islands, bridges, and ladders. The postprocessing Minutiae Table algorithm stores minutiae table pixels on Final minutiae table if it is only valid ending or bifurcation, after verifying against all spurious minutiae. The process of elimination or deletions of spurious minutiae is explained below. Figure 4.10 shows few invalid minutiae ridge bifurcation obtained through FVC ongoing 2002 DB1_B benchmark dataset for, 3 × 3 size window. The gray color cell represents connected edge with respect to candidate minutiae pixel, which is in the center of the window represented in red color.

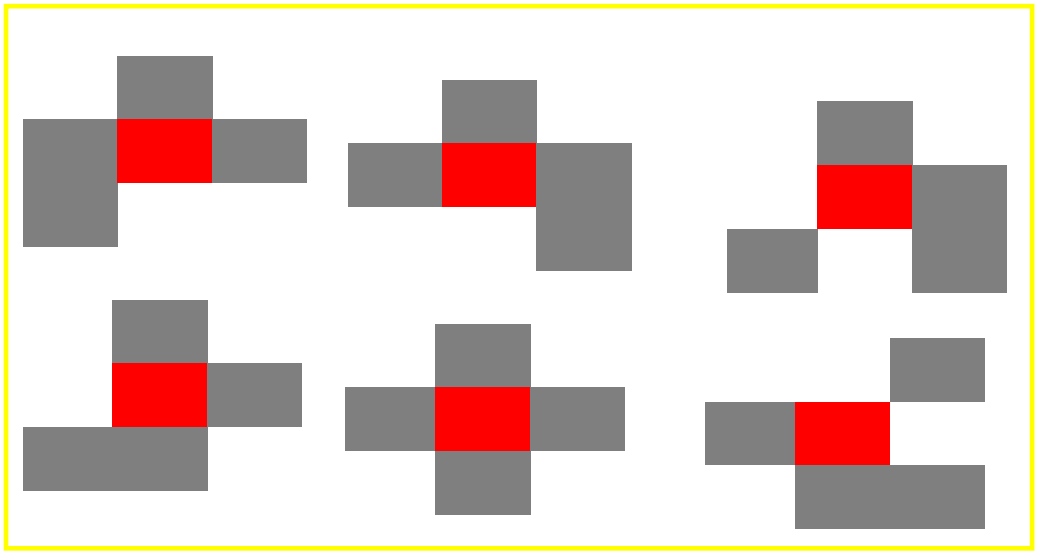


**Figure 4.10:** Invalid ridge bifurcations recognized through Post processing Minutiae Table in 3 × 3 size window

Table 4.2 shows a total number of ridge ending and ridge bifurcation pixels identified before and after post-processing operation for sample images of FVC ongoing 2002 DB1_B benchmark dataset. From the Table 4.2, it is understood that post-processing operation drastically reduces a total number of pixels in final Minutiae Table. The total number of ridge bifurcation and ending pixel is depending on the structure of thinned fingerprint image. The time complexity of post-processing minutiae table is Big-Oh $(n)$.

**Table 4.2:** Total number of ridge ending and bifurcation pixels before and after post processing operation

| Sr. No | Image name | Total number of ridge ending and bifurcation pixels before post processing operation | Total number of ridge ending and bifurcation pixels after post processing operation |
|---|---|---|---|
| 1 | 101_1 | 419 | 11 |
| 2 | 101_5 | 324 | 77 |
| 3 | 102_2 | 1015 | 55 |
| 4 | 103_3 | 623 | 32 |
| 5 | 104_4 | 450 | 52 |
| 6 | 104_7 | 811 | 582 |
| 7 | 104_8 | 488 | 02 |
| 8 | 105_8 | 829 | 67 |
| 9 | 106_6 | 693 | 54 |
| 10 | 109_3 | 819 | 18 |
| 11 | 109_8 | 879 | 26 |
| 12 | 110_3 | 666 | 18 |
| 13 | 110_8 | 900 | 23 |

## 4.5 CREATING HASH CODE USING MD5 HASH FUNCTION FROM FINAL MINUTIAE TABLE (METHOD-1)

After obtaining Final Minutiae Table (final_M_table) through post-processing phase, next to these minutiae details are further converted into a form which is suitable or compatible to convert into hash code. Here we use Message Digest 5 (MD5) hash function in order to generate hash code. The structure of final_M_table is shown in table 4.3.

**Table 4.3:** Structure of final_$M_{table}$

| Sr. No | Minutiae pixel 'x' position | Minutiae pixel 'x' position | Crossing number | Sum of 2nd, 3rd, and 4th column |
|---|---|---|---|---|
| 1 | 5 | 86 | 3 | 94 |
| 2 | 15 | 76 | 3 | 94 |
| 3 | 17 | 106 | 3 | 126 |
| 4 | 18 | 85 | 3 | 106 |
| 5 | 21 | 49 | 3 | 73 |
| 6 | 21 | 83 | 3 | 107 |
| 7 | 25 | 57 | 3 | 85 |
| 8 | 25 | 61 | 3 | 89 |
| 9 | 25 | 99 | 3 | 127 |
| 10 | 46 | 105 | 1 | 152 |

This table only shows sample values for four columns of final_M_table. Actually, an image may consist of hundreds of minutiae pixels. But in this table, only first 10 minutiae pixel

details are shown. Initially, some variables are declared and initialized. The variables are tablerowsum, tablecolsum,tableridbif, tablefetsum, ridgeendcount, bifurcationcount, num. Initially values of these all variables are zero. Later tablerowsum, tablecolsum, tableridbif, tablefetsum, ridgeendcount, bifurcationcount and num are assigned with sum of all minutiae pixel x position, sum of all minutiae pixel y position, sum of all crossing number, row sum of all elements of fourth column of the table, total of all ridge ending value, total all ridge bifurcation value and total of all ridge end count and total of all ridge bifurcation count respectively. Size of $I_{segment}$ is calculated in row and column directions and stored in variable size1 and size2. The above mentioned variables mean is calculated and stored in respective variables. Next the value of all variables are assigned to new values as shown below.

tablerowsum = tablerowsum / (size1*size2)
tablerowsummean = tablerowsum / num
tablecolsum = tablecolsum / (size1*size2)
tablecolsummean = tablecolsum / num
tableridbif = tableridbif / (size1*size2)
tableridbifmean = tableridbif / num
tablefetsum = tablefetsum / (size1*size2)
tablefetsummean = tablefetsum / num
ridgeendcount = ridgeendcount / (size1*size2)
ridgeendcountmean = ridgeendcount / num
bifurcationcount = bifurcationcount / (size1*size2)
bifurcationcountmean = bifurcationcount / num

In above variable initialization, num = ridgeendcount + bifurcationcount. All these 12 variables are passed to the MD5 hash function with a purpose to generate 32 bit hexadecimal Hash code. The above calculation ensures that all fingerprint images will generate different or unique hash code, even for a same human being different fingerprint. The process of the MD5 algorithm is disused below.

Input: Extracted Features

Output: Hash Code

1. Attach the padded bits
2. Append the length of the initial input to the result of Step-1
3. Initialize MD buffer as A, B, C, D.

A four-word buffer (A, B, C, D) was used to evaluate the message digest. Here each of A, B, C, D is a 32-bit register

4. Process message in 16-word blocks
5. Finally, we get the 32-bit hash code as output

### 4.5.1 Creating Hash code using MD5 Hash function from Minutiae Table (Method-4)

This is almost similar to Method-1 with few differences. In this Method, unlike Method-1, we don't use post-processing the minutiae. Minutiae table contains only Ridge and bifurcation code. Here also we use Message Digest 5 (MD5) hash function in order to generate hash code. The structure of final_$M_{table}$ is shown in Table 4.4.

**Table 4.4:** Structure of $Minutiae_{table}$

| Sr. No | Crossing number-Ridge Ending | Crossing number-Ridge Bifurcation |
|---|---|---|
| 1 | 1 | 3 |
| 2 | 1 | 3 |
| 3 | 1 | 3 |
| 4 | 1 | 3 |
| 5 | 1 | 3 |
| 6 | 1 | 3 |
| 7 | 1 | 3 |
| 8 | 1 | 3 |
| 9 | 1 | 3 |
| 10 | 0 | 3 |

The Table 4.4 only shows sample values for four columns of final_M_table. Actually, an image may consist of hundreds of minutiae pixels. But in this table, only first 10 minutiae pixel details are shown. Initially, some variables are declared and initialized. The variables are ridge endcount, bifurcationcount, which are initialized assigned to zero. Later these values are updated with a total of 2nd column and total of the 3rd column of Table 4.2. These two values are combined and passed to the MD5 Hash function.

## 4.6 EXTRACTING FEATURES DIRECTLY FROM SEGMENTED IMAGE (METHOD-2 & METHOD-3)

After segmentation, we extract the features without doing skeletonization process. This is mentioned in this study as Method-1 in Methodology. The use of skeletonization process for feature extraction is referred as Method-2. In Method-3 we don't use tuning based filtering algorithm except that Method-3 is similar to Method-2. In this method first, we convert the

I_segment image to double intensity image (Krishna Prasad, K., & Aithal P. S., 2018c). Four floating point numbers are created using the following statement

f=[1/3.2,1/3.4,1/3.6,1/3.8]*2*pi

Next gray thresh value of the grayscale image is calculated. Gray thresh is a threshold value between 0 and 1, and which always return a fraction value between 0 and 1. The above this value is treated as 1 and below this value is treated as 0, while converting grayscale image to binary image. In the binary image, I_binary the value 1 is considered as the background of the image and 0 is foreground or ROI of the fingerprint image. All the pixels, which are having value 1 is extracted using index position which is having value 0 in, I_binary image. The starting and ending positions of the pixel which is having value 0 are calculated using imin, jmin, imax, and jmax respectively. i and j represent row and column of the I_binary image. These variables are used to extract ROI of the image from the I_binary image. To extract minutiae details here 64 × 64 sized Gabor filter is used with 4 different frequencies. The equation for Gabor filter is given by

G (i, j) = exp(-.5*((xPrime/Sx)^2+(yPrime/Sy)^2))*cos(2*pi*f(1,fre)*xPrime)

Where xPrime = x * cos(theta) + y * sin(theta),

yPrime = y * cos(theta) - x * sin(theta),

theta=(pi*i)/8 i, can take value from 1 to 4.

Later, the convolution of the image p1 and imaginary part of G is found. p1 is a 64 × 64 sized double image obtained from I_binary. Again the convolution of the image p1 and Real part of G is also found, these two are stored in variables Imgabout and Regabout. Finally mean, standard deviation, and variance mean of Regabout is calculated. The above entire process is repeated for 4 different values of f. Total 12 real values are obtained and which is given as an input for the hash function. The hash function is generated using MD5 algorithm. The procedure for extracting features directly from segmented image using Gabor filter is shown below

Input: Segmented image, $I_{segment}$

Output: Extracted features

1. Convert segmented image to double type

   $I_{double}$ = double ($I_{segment}$)

2. Initialize three constants Sx and Sy with value 3 and L with value 4.

   Sx=3, Sy=3, L=4

3. Initialize frequency for Gabor filter

f= [1/3.2, 1/3.4, 1/3.6, 1/3.8] * 2 * pi // [where pi = 22/7]

4. Initialize a matrix p1 for Gabor filter as p1 with initialize value 1 with size 64 × 64, as, $p1_{64\times64} = 1$
5. Find a grey thresh (threshold value) for $I_{double}$
   level = graythresh ($I_{double}$)
6. Convert double image to binary image using graythresh value
   $I_{binary}$ = binary_image ($I_{double}$, level)
7. [i, j] = find (zero index position of $I_{binary}$ in row and column matrix)
8. Find the minimum and maximum position value for i and j.
   imin = min(i), imax = max(i), jmin = min(j), jmax = max(j)
9. Create a new binary image, $I_{binary1}$ which contains only value zero from $I_{binary}$
10. Initialize a constant variable rate
    rate = 64/max (size($I_{binary1}$))
11. Resize the $I_{binary1}$ as
    Resize $I_{binary1}$ (i × rate, j × rate) // where i and j are row and column dimension
12. Find the new size of $I_{binary}$
    [ i, j] = size ($I_{binary1}$)
13. Round off the value of i, and j
    i1 = round ((64-i) / 2)
    j1 = round ((64-j) / 2)
14. Reassign the value of p1
    p1 = (i1 + 1 to i1 + i, j1 + 1 to j1 + j)
15. Convert p1 to double from binary
    p1= double(p1)
16. **for each** i (from 1 to 4) **do**
    Initialize the theta value as theta = (pi × i) / 8;
    **for** x= round to nearest integer value (-Sx) to round to nearest integer value (Sx)
    **for** y= round to nearest integer value (-Sy) to round to nearest integer value (Sy)
    Rotate with respect to theta
    xPrime = x * cos(theta) + y * sin(theta)

```
        yPrime = y * cos(theta) - x * sin(theta)
        Use Gabor filter by varying frequency and angle
        G(x, y) = exp(-((xPrime/Sx)^2+(yPrime/Sy)^2))*cos(2*pi
                    *f(1,fre)*xPrime)   // ^ represents power
      end for
    end for
  Do convolution of P1 and imaginary part of G from central part
    Imgabout = conv2 (p1, double (imag (G)), 'same') // 'same' does the
                                          //convolution from the central part
    Do convolution of P1 and real part of G from central part
      Regabout = conv2 (p1, double (real (G)), 'same') // 'same' does the
                                          //convolution from the central part
     Find the mean of  Imgabout and Regabout
     imfea1(i) = mean (Imgabout)
     imfea2(i) = mean (Regabout)
     Find Standard Deviation of  Imgabout and Regabout
      stfea1(i) = standard_deviation (Imgabout)
      srfea2(i) = standard_deviation (Regabout)
     Find the mean of variance of  Regabout
      medfea2(i)=mean(var(Regabout))
  End for
  End for
features = [ imfea2, srfea2, medfea2]
```

### 4.6.1 Workflow and Flowchart for extracting features directly from segmented image

Extracting features directly from the segmented image is explained using flowchart in Figure 4.12. The input for this algorithm is a segmented image, I_segment. The final output is Extracted features. The workflow diagram is shown using Figure 4.11.

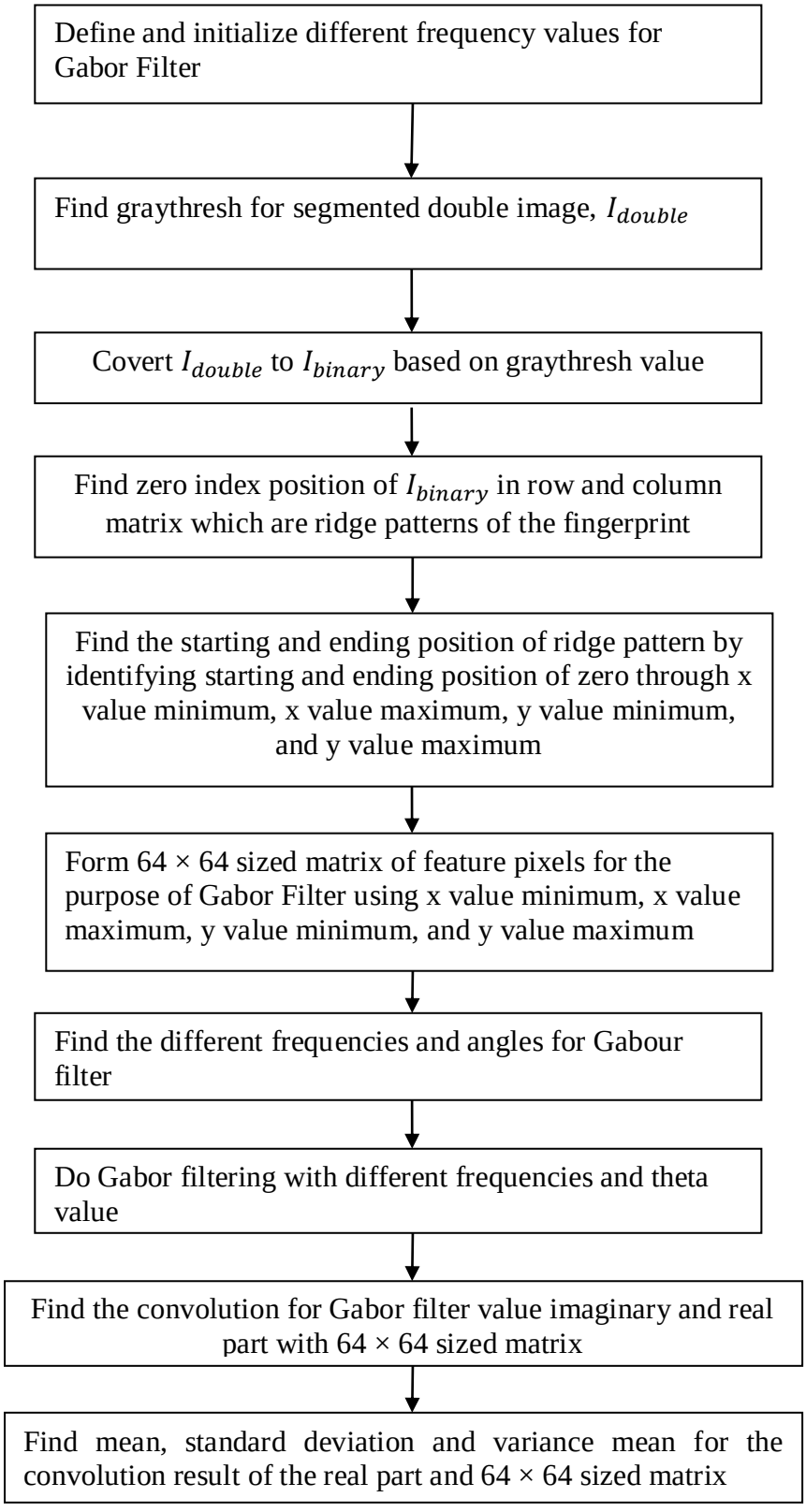
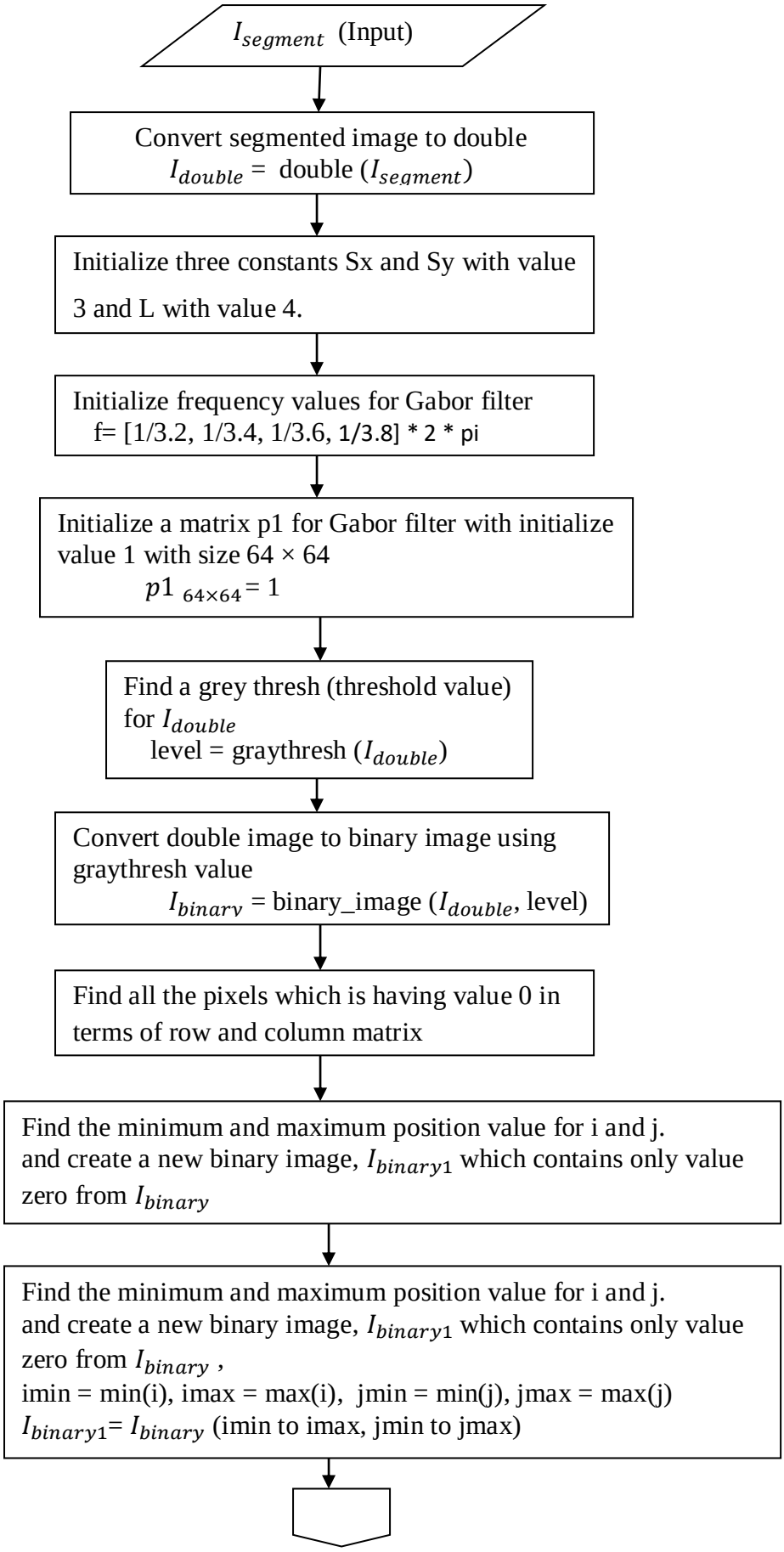



**Figure 4.11:** Workflow of Feature Extraction using Gabor Filter


$I_{segment}$ (Input)
Convert segmented image to double
$I_{double}$ = double ($I_{segment}$)
Initialize three constants Sx and Sy with value 3 and L with value 4.
Initialize frequency values for Gabor filter
f= [1/3.2, 1/3.4, 1/3.6, 1/3.8] * 2 * pi
Initialize a matrix p1 for Gabor filter with initialize value 1 with size 64 × 64
$p1_{64\times64}$ = 1
Find a grey thresh (threshold value) for $I_{double}$
level = graythresh ($I_{double}$)
Convert double image to binary image using graythresh value
$I_{binary}$ = binary_image ($I_{double}$, level)
Find all the pixels which is having value 0 in terms of row and column matrix
Find the minimum and maximum position value for i and j.
and create a new binary image, $I_{binary1}$ which contains only value zero from $I_{binary}$
Find the minimum and maximum position value for i and j.
and create a new binary image, $I_{binary1}$ which contains only value zero from $I_{binary}$ ,
imin = min(i), imax = max(i), jmin = min(j), jmax = max(j)
$I_{binary1}$= $I_{binary}$ (imin to imax, jmin to jmax)

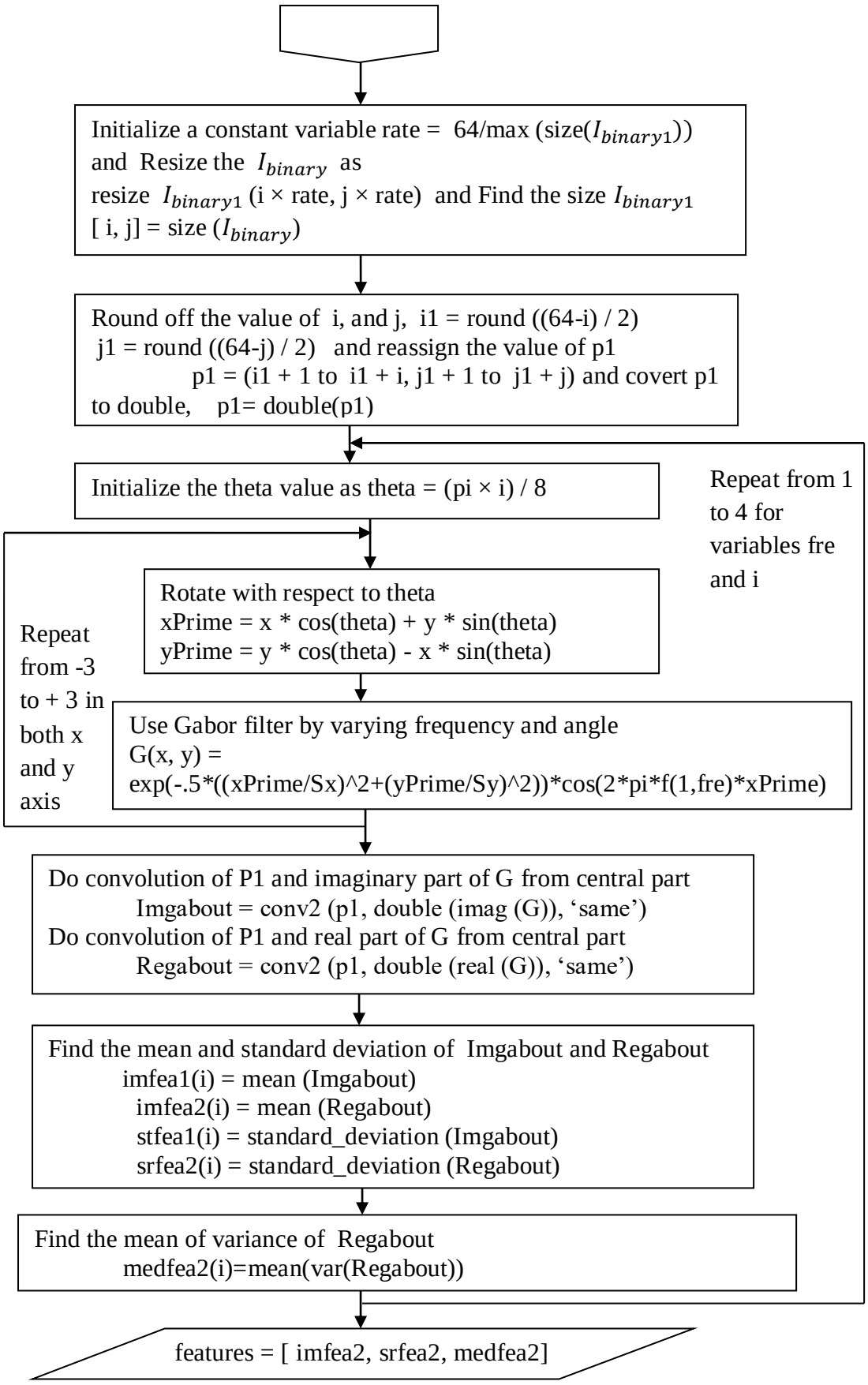



**Figure 4.12:** Flowchart for extracting features using Gabor filtering

### 4.6.2 Analysis of extracting features directly from segmented image

Extracting features directly from the segmented image based on Gabor filter uses four different values for frequency and theta, which is shown in Table 4.3. These four frequencies and Angle value help to generate a matrix of size, 7 × 7 containing total 49 real values due to Gabor filtering process. Each row of the Table 4.5 results in 3 positive or negative real numbers due to mean, standard deviation, and mean of variance calculations. Before calculating these three statistical calculation convolutions process was conducted on Gabor filter matrix of size 64 × 64 (p1) and real part of the imaginary number of Gabor value (G).

**Table 4.5:** Frequency and theta value used in Gabor Filter to extract features

| Sr. No | Frequency value | Angle (theta) value |
|---|---|---|
| 1 | 1.9635 | 0.3927 |
| 2 | 1.8480 | 0.7854 |
| 3 | 1.7453 | 0.1781 |
| 4 | 1.6535 | 1.5708 |

With the aid of Gabor filter process, each fingerprint image produces total of twelve (12) double precision values.

These large double precision values ensure that each fingerprint sample produces different hash values through MD5 hash functions.

Method-2 and Method-3 use feature extraction without skeletonization or they extract fingerprint feathers from the segmented image directly using above mentioned Gabor filter. Method-2 uses contrast adjustment filtering and Method-3 does not make use of Contrast adjustment method, which is newly proposed work of this research study.

## 4.7 FINGERPRINT HASH CODE GENERATION USING FREEMAN CHAIN CODING.

Freeman chain code is used to symbolize a boundary by means of a connected series of straight line segments of specific length and path in the predefined direction, stated by Gonzalez and Woods (1992). Typically Freeman Chain coding illustration is based on 4 or 8 connectivity of the segments (Bernard et al., 2012). The direction of each segment is coded or represented by the usage of a numbering format or scheme. A boundary code fashioned as a sequence of such directional numbers is called a Freeman chain code. The chain code of a boundary relies upon at the place to begin. Running with code numbers gives a unified way to research or analyze the form of the boundary. Chain code follows the contour in a counter-

clockwise manner and keeps tune of the directions as we go from one contour pixel to the following. Figure 4.13 (a) and 4.13 (b) represents 4-connected and 8-connected neighbor of Freeman Chain code respectively.

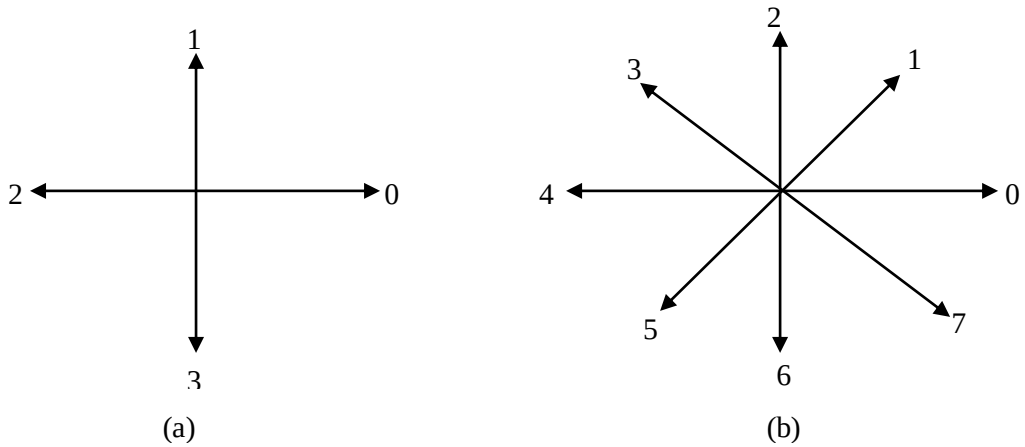



**Figure 4.13:** Neighbour Directions of Freeman Chain code

The main drawback of 4-connectivity is that we lose the diagonal factors or pixels wherein those pixels are very useful in most of the image processing programs. An example of 4-connected Freeman Chain code is shown in Figure 4.14.

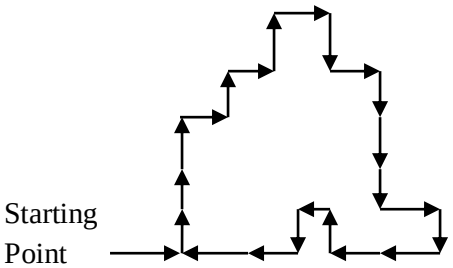



**Figure 4.14:** Freeman Chain code Example for 4-connected neighbour

So, in order to overcome the` drawback of 4-connectivity here, we use 8-connectivity. In 8-connected neighbor, every code is taken into considerations. In 8-connected neighbor, the angular direction is in multiples of 450, that we have to pass or move from one contour pixel to the next. If we take into account Figure 4.14, we can calculate freeman chain code for 4-connectivity as follows.

Freeman Chain code for Figure 4.14 is 111010103033303221322. The first difference of Freeman Chain code for Figure 4.14 is 100313133130013303113O. The first difference of Freeman Chain coding for 4-connected neighbor is explained using Figure 4.15. The first difference value is calculated by counting a number of separating directions in an anti-clockwise direction from the starting point to ending point.

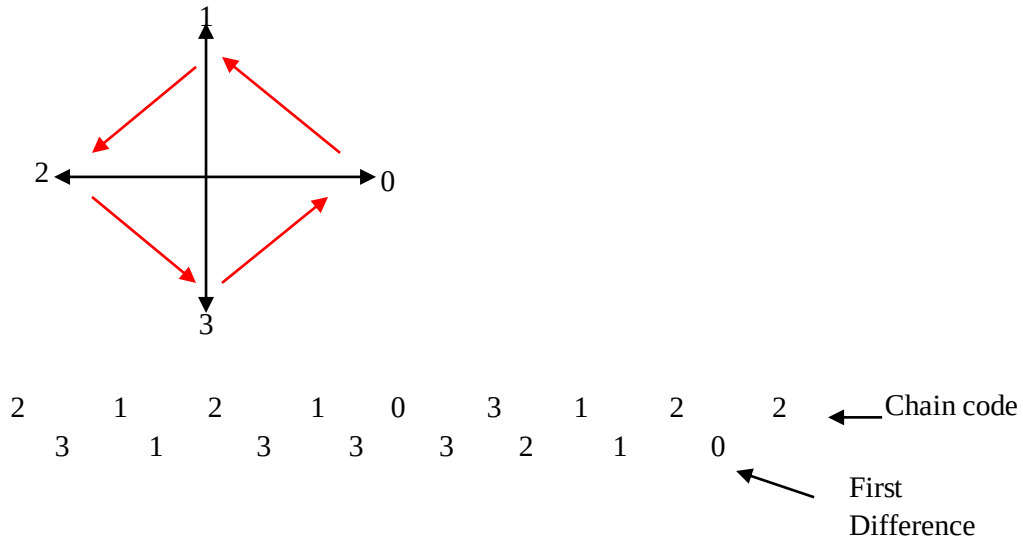



**Figure 4.15:** Freeman Chain code first Difference calculation-example

In 8-connectivity neighbor, we have code from 0 to 7. Consider group of four binary digit as shown below

- 0010
  0100
  0011

The Freeman Chain code first checks for non zero points, in a binary number which is 1. So in the first row starting from left 3 bit is 1. Next bit is 1 from this point three-bit position, which is in the 2nd row. Next non zero value is the five-bit position from the second non-zero bit, which is in the third row. Next non zero bit is very next bit and which is also in the third row. If you observe 8 connected neighbors the direction from the first non zero bit to second is in the direction 5. From second non zero bit to third in the direction of 7. From third non zero bit to fourth in the direction of 0. So the Chaincode of 8-connected neighbor is 570.

Here initially FVC ongoing 2002 benchmark dataset is considered for testing the hash code. The benchmark dataset image is binarized and Freeman Chain code of the image is calculated for each pixel. Before calculating Freeman Chain code it finds boundary starting x and y value. Also, the first difference value of the chain code is calculated. The entire there parameters are considered and 32-bit length hash code is generated. Distinct Euclidean distance value summation, mean value and standard deviation values are considered for generating Hash code. After converting fingerprint image to binary image we have to take one's complement of the binary image. So that all minutiae points will be represented using

binary bit 1. Find all exterior, interior, parent and child boundary of the fingerprint binary image. Boundary_pixel_cell array returns all the pixel positions involved in a boundary. This function returns an array of boundary pixel values. Each element of the array is a matrix of size n × 2 dimensions. Where n represents a number of rows involved in forming boundary points and column are always 2, which represents x and y value of each point. Each boundary matrix is passed as an argument for Freeman Chain coding function.

Freeman Chain code function returns starting x and y position of the boundary, Freeman Chain code, the First difference value of the Freeman Chain code. Initially, if more than one argument is sent to Freeman Chain code function, then it returns an error message that too many arguments. Freeman Chain code Function then checks whether an argument matrix column value is 2. This means that each point should have two values corresponding to x and y pixel positions values respectively. If not this will return an error message that input dimension mismatched. Next, it checks for open contour or open boundary. If the first and last point of the boundary value is same then it is considered an open contour. In this case, Freeman Chain code boundary stating x and y value will be equal to first point pixel value. Both Freeman Chain code and First difference value will be zero. If the first and last point of the boundary is not same, then find the difference x and y value, by subtracting the first point from the second point. Find difference for all the points which makes the boundary pixels. The transition from current pixel to the next pixel is computed from the connectivity diagram shown in Figure 4.13 (b) and as shown in Table 4.6. Setting up mapping mechanisms between pixel value differences in 8-connectivity directions is controlled by the following statement

idx([1 2 3 5 7 9 10 11]) = [5 4 3 6 2 7 0 1]

idx corresponds index value of code value and unique value is obtained by doing a simple calculation as follows

diffB_map = 4*row_diff + col_diff + 6

**Table 4.6:** Transition Table of Freeman Chain code

| Row difference | Column Difference | Direction |
|---|---|---|
| 0 | +1 | 2 |
| 0 | - 1 | 6 |
| - 1 | +1 | 3 |
| - 1 | - 1 | 5 |
| +1 | +1 | 1 |
| +1 | -1 | 7 |
| -1 | 0 | 4 |
| +1 | 0 | 0 |

Here diffB_map variable corresponds to each point pixel value difference that is involved in forming boundary pixels. These diffB_map values indexed into direction map using below statement and which produces chain code value as chain_code_value = idx(diffB_map)

Finally, first difference value of chain code is obtained, by the following procedure

1. Subtract each chain code value from Chain code end value
2. Add number 8 to Step-1
3. Take Modulus value of step-2 and 8 i.e. mod (Step-2, 8)

### 4.7.1 Procedure for fingerprint Hash code generation using Freeman Chain code

The procedure for Fingerprint Hash code generation using Freeman Chain code is shown using Figure 4.16 (Krishna Prasad, K., & Aithal P. S., 2018d).

1. Input Grayscale fingerprint image, read (input_image)
2. Convert input image into 256 × 256 sized two-dimensional image
   resized_image = image_resize (input_image, [256, 256])
3. Contrast Adjustment using $\tau$-Tuning Based Filtering (As discussed in 3.3)
   contrast_adjusted_image = $\tau$-Tuning Based Filtering(resized_image)
4. Convert 256 × 256 sized grayscale image into binary image
   binary_image = convert_to_binary(contrast_adjusted_image)
5. Perform One's complement of the binary_image
   binary_image = one's complement(binary_image)
6. Find the Exterior boundaries of the binary image and boundaries of holes inside this exterior Boundary as, boundary_pixel_array = boundary_pixel(binary_image)
7. Find the row length of boundary_pixel_array
   m = length (boundary_pixel_array ) [where m is row length]
8. Find Freeman Chain code for each element of the boundary_pixel_array
   **for each** element of boundy_pixel_array **do**
   freeman_chain_code= freeman_chain_code (i) // i, index to each element
   **end for**
9. Obtain Row and column coordinates for the starting pixel of the boundary from Step-8, start_idx = freeman_chain_code. start_idx
10. Obtain Freeman Chain code value for each boundary from Step-6
    chain_code = freeman_chain_code. chain_code
11. Obtain Freeman Chain code first difference value for each boundary from Step-6
    firstdiff = freeman_chain_code. firstdiff
12. Compute summation of Step-7, Step-8, and Step-9
13. Divide all 3 values of Step-10 by m.
14. Pass the value of Step-11 as parameter for MD5 Hash function
    hash_value = MD5_DataHash(combine_value)

**Figure 4.16:** Procedure for Fingerprint Hash code generation using Freeman Chain code

### 4.7.2 Flowchart of Hashcode Generation using Freeman Chain Code

The Hashcode Generation using Freeman Chain Code is explained using a flowchart in Figure 4.17.

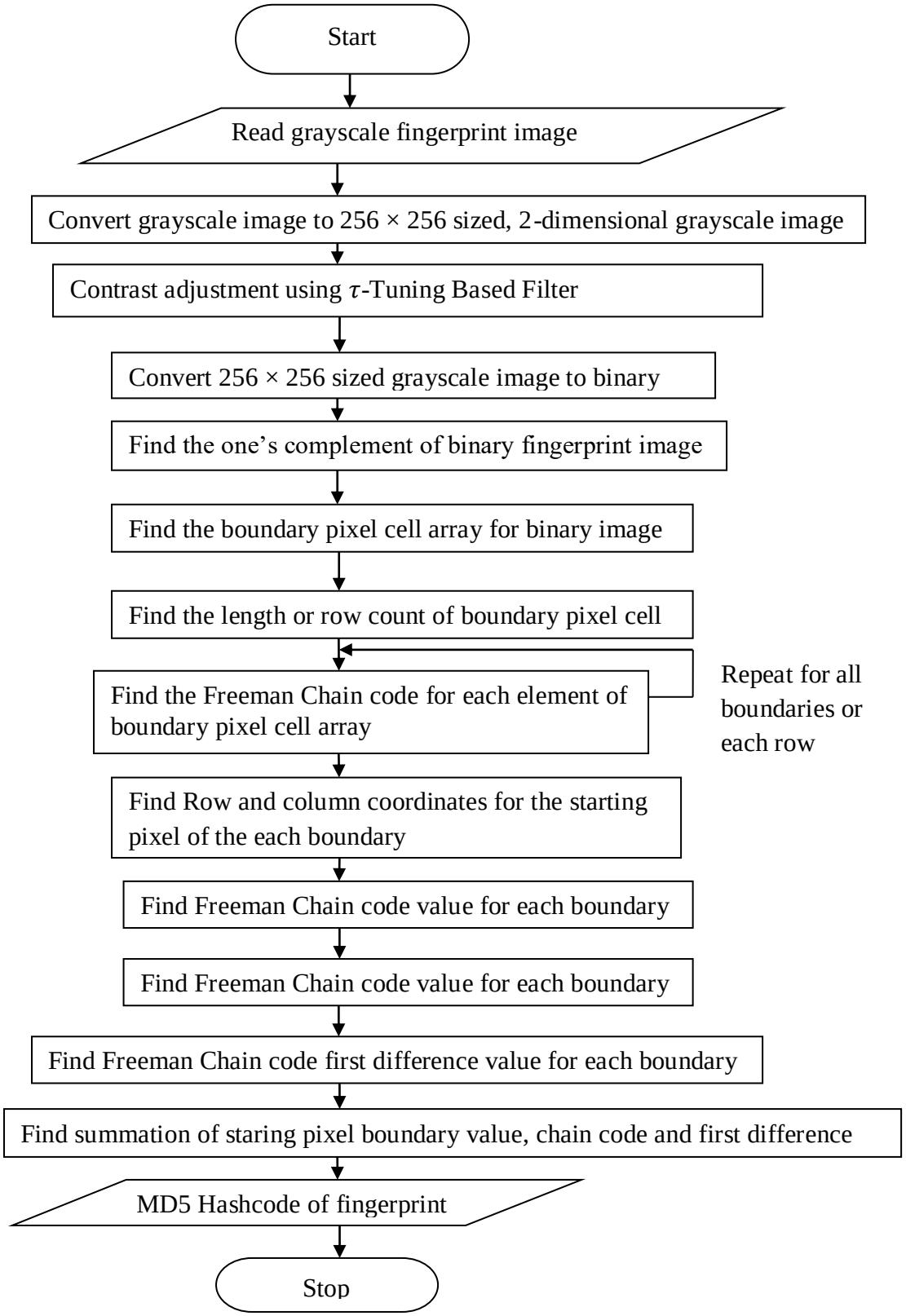



**Figure 4.17:** Flowchart of Hash code generation using Freeman Chain **code**

With an intention to make the MD5 Hashcode more robust and to get the advantage of salting Freeman Chain code summation of boundary starting x and y position, Chain code value and first difference value are divided by a total number of boundary value and all values are combined as a string and passed to the MD5 algorithm.

## 4.8 FINGERPRINT HASH CODE GENERATION USING EUCLIDEAN DISTANCE (METHOD-6)

In this study, we calculate Euclidean distance for a binary fingerprint image, which is a straight line distance from a pixel with value zero to the pixel with value non-zero, which is one in a binary image using Euclidean norm. The Euclidean distance is calculated for all the pixels of the binary fingerprint image. The two points k and l, in two-dimensional Euclidean spaces and k with the coordinates (k1, k2), l with the coordinates (l1, l2). The line segment with the endpoints of k and l will form the hypotenuse of a right-angled triangle. The space among factors k and l is defined as the square root of the sum of the squares of the differences among the corresponding coordinates of the points. In a two-dimensional Euclidean geometry Euclidean distance between two points k = (kx, ky) and l = (lx, ly) is given as follows;

$$d(k, l) = \sqrt{(lx - kx)^2 + (ly - ky)^2}$$

For example, consider a 3×3 sized matrix with values as follows

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

The Euclidean distance for each point is calculated as follows

$$\begin{bmatrix} 1.4142 & 1.0000 & 1.4142 \\ 1.0000 & 0 & 1.0000 \\ 1.4142 & 1.0000 & 1.4142 \end{bmatrix}$$

The most natural or common matrix for finding distance matrix in the binary image is Euclidean distance (Das et al., 1987, Yamada, 1984, & Borgefors, 1986). Due to the lack of efficient algorithms in the field of Euclidean distance led to the development of many types of research in this field in order to define, elaborate and also to use some other methods to find the distance using other methods like the city block, chessboard or chamfer (Borgefors, 1986, Danielsson, 1980, & Yamashita & Ibaraki, 1986). The Euclidean distance transform is global operation and the calculation of Euclidean distance is most common and simple operation and amount of calculation required is always directly proportional to the size of the entire image because this is calculated for every pixel.

Initially, FVC ongoing 2002 benchmark dataset is considered for testing the hash code. The benchmark dataset image is binarized and Euclidean distance of the image is calculated for each pixel. The distinct values of the Euclidean distance matrices values are considered and 32-bit length hash code is generated. Distinct Euclidean distance value summation, mean value and standard deviation values are considered for generating Hash code.

### 4.8.1 Procedure of Hashcode Generation using Euclidean Distance

This section explains step by step procedure to develop Hashcode by making use of Euclidean distance matrix on a binary fingerprint image (Krishna Prasad, K., & Aithal P. S., 2017i). The procedure for Hash code generation using Euclidean distance is shown in Figure 4.18.

1. Input Grayscale fingerprint image
   read (input_image)
2. Convert input image into 256 × 256 sized two-dimensional image
   resized_image = image_resize (input_image, [256, 256])
3. Contrast Adjustment using $\tau$-Tuning Based Filtering (As discussed in 3.3)
   contrast_adjusted_image = $\tau$-Tuning Based Filtering(resized_image)
4. Convert 256 × 256 sized grayscale image into binary image
   binary_image = convert_to_binary(resized_image)
5. Perform One's complement of the binary_image
   binary_image = one's complement(binary_image)
6. Find the Euclidean distance of the image
   euclidean_image = Euclidean_distance(binary_image)
7. Find the distinct value of the Euclidean distance
   distinct_eucllidean_value = distinct_value(euclidean_image)
8. Find the distinct value summation
   **for each** distinct_eucllidean_value **do**
   euclidean_sum = distinct_eucllidean_value (i) //i, index to each distinct //element
   **end for**
9. Find the mean of the distinct Euclidean value
   euclidean_mean = mean(distinct_eucllidean_value)
10. Find the standard deviation of the distinct Euclidean value
    std_deviation = standard_deviation(distinct_eucllidean_value)
11. Combine the value of (8), (9), and (10)
    combine_value = combine(euclidean_sum, euclidean_mean, std_deviation)
12. Pass the value of (11) as parameter for MD5 Hash function
    hash_value = MD5_DataHash(combine_value)

**Figure 4.18:** Procedure for Hash code Generation using Euclidean Distance

### 4. 8.2 Flowchart of Hashcode Generation using Euclidean Distance

The procedure used in Figure 4.18 is explained using flowchart in Figure 4.19. With an intention to make the MD5 Hashcode more robust and to get the advantage of salting

Euclidean distance sum, mean, and standard deviation are combined and passed to the MD5 algorithm.

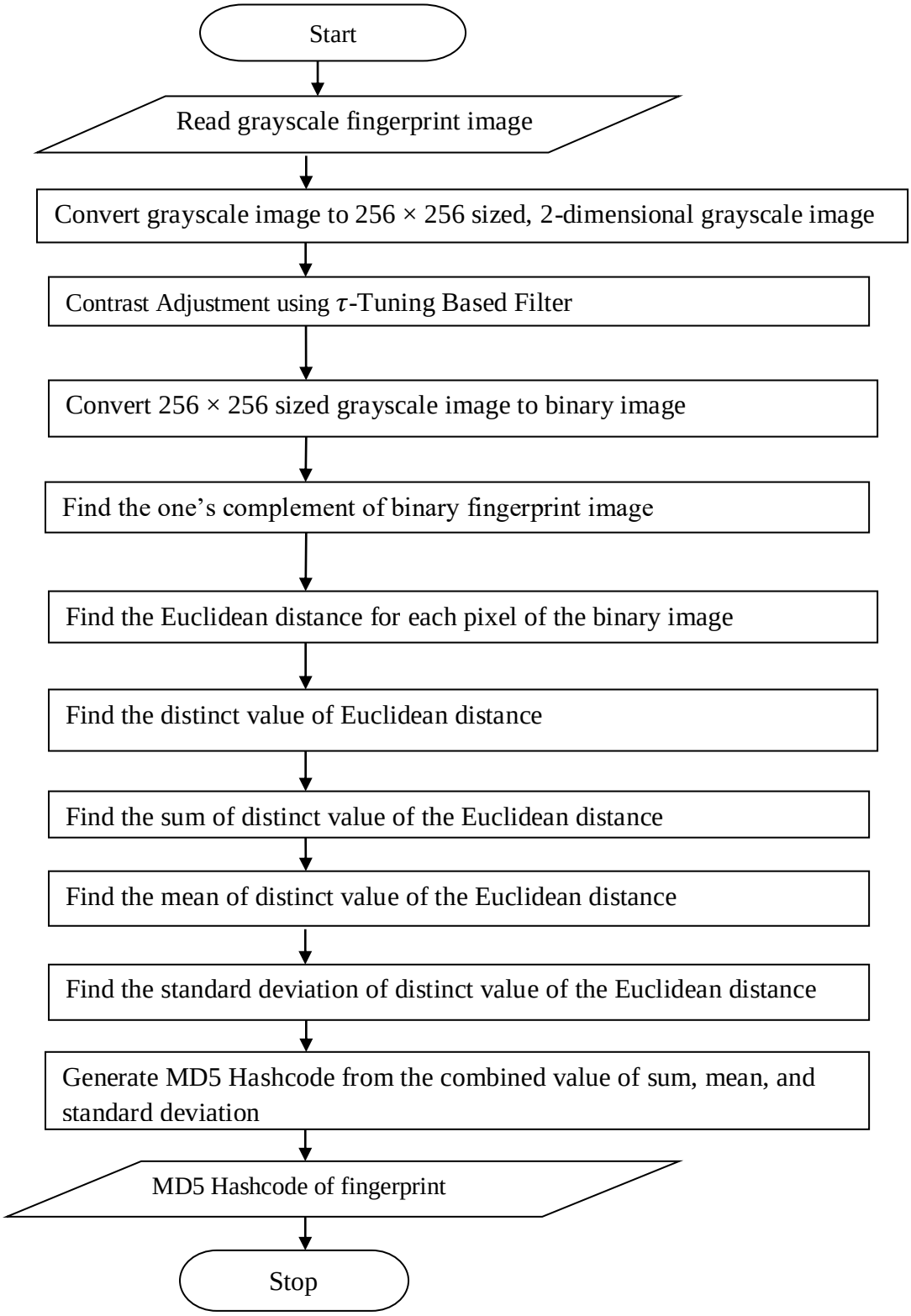



**Figure 4.19:** Flowchart of Hash code generation using Euclidean Distance

## 4. 9 DATABASE DESIGN

In this study for test purpose, we use WampServer. In WampServer we use MySQL database to create database and database table. This study becomes only framework for security mechanisms in fingerprint verification systems. If the system is implemented through server and hash matching is done at server side by encrypting features, then it will improve the security. Storage space required is also very less because hash code takes very less space compared to original fingerprint template structure. For test purpose, FVC ongoing 2002 benchmark datasets are used. The design of the Database, in MySQL command prompt, is shown below.

MySQL> create database fingerprint1;

MySQL> use fingerprint1;

MySQL> create table trainhash1 (id number (10), hash varchar (100));

Table 4.7 shows the trainhash1 table values for the benchmark dataset FVC ongoing 2002 DB1_B, dataset image 101_1 to 101_8 using the method without skeletonization process (Method-1). Each user will be having 8 fingerprint images.

**Table 4.7:** Hash value for image DB1_B 101.tif using Method-1

| id | Hash |
|---|---|
| 1 | 6b0cb74f5f8773667bf633a232b7ed12 |
| 1 | 34b40e9b5888aba96b2cef5c1a8f80e5 |
| 1 | 966db620d38d4f4ef2784fc84f6d95f7 |
| 1 | 3ab5c91b098c92383205bac43d6bb234 |
| 1 | 70225273d8b8a5d2c4ac44884d22d84a |
| 1 | 4881fbf214265358a6dd5473032d2926 |
| 1 | 00992803ad7c036a1d0a773e839ee791 |
| 1 | ced83b3a7a84676ac72e0a62a5d33479 |

If the test sample hash code matches with already stored registered user fingerprint's hash code, then the user is treated as Authenticated user or else unauthenticated user. This research work acts as a framework for real fingerprint verification systems to increase security. Table 4.8 shows the trainhash1 table values for the benchmark dataset FVC ongoing 2002 DB1_B, dataset image 101_1 to 101_8 using non-skeletonisation process (Method-2). Each user will be having 8 fingerprint images.

**Table 4.8:** Hash values for image DB1_B 101.tif using Method-2

| id | Hash |
|---|---|
| 1 | d579254fa5831c03e60e18729fbc710b |
| 1 | 27024ce2cdd3dbdfa8d689adb7abc36c |
| 1 | 23a8d9d5cb9b4eb62dab62bb4a67e30c |
| 1 | 51398c3f65804111d281ba3e9f62e084 |
| 1 | 3db3a5b0777e10d97b49851c4e71fe49 |
| 1 | d7d4a52858c98fb16e37d9613242ca36 |
| 1 | d2901a0ae4e697d2ca2b9122e7bd2a1e |
| 1 | 9f164d2dfaa2dff871208789d9056098 |

Table 4.9 shows the trainhash1 table values for the benchmark dataset FVC ongoing 2002 DB1_B, dataset image 101_1 to 101_8 using non-skeletonisation process and without using contrast adjustment filtering (Method-3). Each user will be having 8 fingerprint images.

**Table 4.9:** Hash values for image DB1_B 101.tif using Method-3

| id | Hash |
|---|---|
| 1 | 6b0cb74f5f8773667bf633a232b7ed12 |
| 1 | 34b40e9b5888aba96b2cef5c1a8f80e5 |
| 1 | 966db620d38d4f4ef2784fc84f6d95f7 |
| 1 | 3ab5c91b098c92383205bac43d6bb234 |
| 1 | 70225273d8b8a5d2c4ac44884d22d84a |
| 1 | 38e88574ce4e29b5d5ed227f0b7c8355 |
| 1 | 00992803ad7c036a1d0a773e839ee791 |
| 1 | ced83b3a7a84676ac72e0a62a5d33479 |

Table 4.10 shows the trainhash1 table values for the benchmark dataset FVC ongoing 2002 DB1_B, dataset images 101_1 to 101_8 using skeletonization process without pixel location values (Method-4). Each user will be having 8 fingerprint images.

**Table 4.10:** Hash values for image DB1_B 101.tif using Method-4

| id | Hash |
|---|---|
| 1 | 88dfd45f54a0eb12ea86304b05839930 |
| 1 | 218e4710abab1df6f9de4d62255162a0 |
| 1 | f35144c3020e5b409d0cdf20856eda15 |
| 1 | 496332e85fdaf1c41c63e587a3ecd29c |
| 1 | 9dc3aea7b8e816463cf22f482256bdc8 |
| 1 | 7a5922f1660b47a494f497b4cea6f745 |
| 1 | d06612e4af7f6d1a91951416144c7356 |
| 1 | 65a1844eeaa282f3f6a6e9879b92fec8 |

Table 4.11 shows the trainhash1 table values for the benchmark dataset FVC ongoing 2002 DB1_B, dataset image 101_1 to 101_8 using Freeman Chain code (Method-5). Each user will be having 8 fingerprint images.

**Table 4.11:** Hash values for image DB1_B 101.tif using Method-5

| id | Hash |
|---|---|
| 1 | 81981d7bd4cce1582d8b2b7504c26a50 |
| 1 | a99611a0d96a1c61f3959811ef124e39 |
| 1 | 036873c293d1c167fff2ffcdf7c170ee |
| 1 | 4ca11dc4b4d34742e3984a6860de9f35 |
| 1 | 76a6ddd5554db7f62c09002b47656019 |
| 1 | 8643dba9e05955186a853bfc0f98c49a |
| 1 | de58fc3ceb2c6dd18b13fa63135fc0ec |
| 1 | e5dfa310f4597b5135e67dbdf0d321e3 |

Table 4.12 shows the trainhash1 table values for the benchmark dataset FVC ongoing 2002 DB1_B, dataset image 101_1 to 101_8 using Euclidean distance code (Method-6). Each user will be having 8 fingerprint images.

**Table 4.12:** Hash values for image DB1_B 101.tif using Method-6

| id | Hash |
|---|---|
| 1 | e06c186b309ba7351d716b519d7c73b2 |
| 1 | e51abc67aa9ca5395a65a788cba88a0a |
| 1 | aa79a59951cce403bf3aaded33d38bf3 |
| 1 | 565b3d8c305f29cb32888777ac0131c1 |
| 1 | abc94dbee77bbea4fa09cae0437b20e6 |
| 1 | 58e165b5848805c9b7becccbccd508cb |
| 1 | 0bf588d95473eebd72d44ae3d5e6be30 |
| 1 | e255b46593bf8b5c2ac162cd13511632 |

## 4.10 CHAPTER SUMMARY

In this chapter, we have discussed Fingerprint minutiae feature Extraction using the Skeletonized image and without using the Skeletonized image. The six Methods used in this study mainly focuses on four different methods like minutiae feature extraction from the thinned image, feature extraction using Gabor filtering, Feature extraction using Freeman Chain code, and Feature extraction using Euclidean distance. Method-1 and Method-4 almost similar with location details and without location details of minutiae ridge ending and ridge bifurcation pixel. Method-2 and Method-3 are only having a difference that earlier uses tuning based contrast adjustment algorithm, whereas later one does not use. All the six methods make use of an MD5 algorithm to generate Hash code. Next chapter discusses performance evaluation of hash code generation methods.

**********

# CHAPTER FIVE

# *Performance Evaluation of Fingerprint Hash Code Generation Methods*

| Contents | Page No. |
|---|---|

## 5.1 INTRODUCTION

The advancement in Automatic Fingerprint Identification or Verification System (AFVS) has motivated to evaluate new standards of fingerprint matching algorithm. One of the critical, fingerprint matching is minutiae based-ridge ending and bifurcation. Securing biometrics databases from being compromised is an important area of biometric security study task that ought to be conquered in an effort to assist the vast use of biometrics primarily based authentication. The creation of hash code from the minutiae points of the fingerprint image is an innovation to protect the biometric templates and original fingerprint image. The hash-based device or system should adhere to the subsequent extra requirements:

- Similar fingerprints must have comparable hash values means hash values should be distinct.
- Exclusive fingerprints or two fingerprints should no longer have comparable hashes means even same person different finger of the same hand should produce different hash codes.
- Partial fingerprints also must be matched if sufficient minutiae points are presented.
- Hash code should be invariant to translation and rotation while capturing through fingerprint sensing devices.

In this research study, an alternative approach for fingerprint hash code generation is proposed based on six methods, all of which uses MD5 algorithm, which is mentioned below;

- Hash code based on Minutiae points including ride ending and bifurcation with thinning, preprocessing and post-processing.
- Based on contrast adjustment and segmentation, Gabor filtering, and without thinning process.
- Based on Segmentation, Gabor filtering without using Contrast adjustment filtering and thinning process.
- Minutiae points-ridge ending and bifurcations without its location values by making use of thinning and preprocessing process.
- Based on Freeman Chaincode values by making use of segmentation and binarized image.
- By making use of Euclidean distance of binary image with the aid of segmentation.

The effect of these alternative approaches for fingerprint recognition systems based on modified filtering, minutiae table and using hash code are studied and examined with

distinctive fingerprints taken from benchmark datasets. Numerous performance metrics were used in order to evaluate and know the quality and efficiency of the alternative approach. We have proposed an alternative approach or technique a technique for fingerprint biometric facts that is similar to password encryption and hashing and entails steps like inputting raw fingerprint, segmentation, feature extraction and hash code generation. These steps are common in all four methods mentioned above.

Based on the performance analysis of all six methods an alternative model is proposed for multifactor authentication which makes use of on Fingerprint hash code, Password and OTP combined mainly focusing on internet-based online transactions and mobile-based safe transactions. This method is not suitable for ATM machines and Ordinary Attendance maintenance system.

### 5.2 DATASETS

The datasets used for this study is from Fingerprint Verification Competition (FVC) ongoing 2002 benchmark datasets DB1_B, DB2_B, DB3_B, and DB4_B. Each dataset consists of 10 different fingerprint images and 8 impressions for each fingerprint labeled from 1 to 8. These datasets consist, a total of 3520 (880×4) fingerprints, but out of which only 40 fingerprints are available as a free resource for research testing purposes under the name of four datasets as DB1_B, DB2_B, DB3_B, and DB4_B. These 320 fingerprints are used in this study for test purpose. These datasets consist of image sizes of 388 pixels by 374 pixels (142 Kpixels) with resolution of 500 dpi, 296 pixels by 560 pixels (162 Kpixels) with resolution of 569 dpi, 300 pixels by 300 pixels (88 Kpixels) with resolution of 500 dpi, and 288 pixels by 384 pixels (108 Kpixels) with resolution of about 500 dpi for DB1_B, DB2_B, DB3_B, and DB4_B respectively. First two datasets are captured through optical sensor and DB3 and DB4 are captured through the capacitive sensor and SFinGe v2.51 sensor respectively. The table 5.1 list outs description of FVC 2002 Benchmark datasets.

**Table 5.1:** FVC 2002 Benchmark datasets descriptions

| Dataset Name | Dataset labels | Sensor Type | Image Size | Resolution |
|---|---|---|---|---|
| DB1_B | 101_1.tif to 101_8.tif<br>.....<br>110_1.tif to 110_8.tif | Optical sensor | 388 pixels by 374 pixels (142 Kpixels) | 500 dpi |
| DB2_B | 101_1.tif to | Optical | 296 pixels by 560 | 569 dpi |

| | | | | |
|---|---|---|---|---|
| | 101_8.tif<br>.....<br>110_1.tif to<br>110_8.tif | sensor | pixels (162 Kpixels) | |
| DB3_B | 101_1.tif to<br>101_8.tif<br>.....<br>110_1.tif to<br>110_8.tif | Capacitive sensor | 300 pixels by 300 pixels (88 Kpixels) | 500 dpi |
| DB4_B | 101_1.tif to<br>101_8.tif<br>.....<br>110_1.tif to<br>110_8.tif | SFinGe v2.51 sensor | 288 pixels by 384 pixels (108 Kpixels) | About 500 dpi |

Figure 5.1 shows sample images of a fingerprint taken randomly from different datasets of FVC ongoing 2002 datasets.

DB1_B-101_1.tif

DB2_B-104_8.tif

DB3_B-103_6.tif

DB4_B-105_3.tif

**Figure 5.1:** Sample images of FVC 2002 Datasets

## 5.3 VARIOUS METHODS USED FOR FINGERPRINT HASH CODE GENERATION BASED ON MD5 ALGORITHM

For the purpose of finding performance and efficiency of the hash function based fingerprint matching, we have used four methods in this study. All the methods in common use segmentation and hash code. Hash function or code based fingerprint verification system follows uniqueness property of fingerprint image, means it generates unique or different hash code for each fingerprint image. All the 8 impressions of each fingerprint of individual user produce unique hash code. The four methods are explained below;

**Method-1:**

In this method, raw fingerprint image or image taken from datasets of FVC ongoing 2002 is initially contrast adjusted using $\tau$- Tuning Based Filtering Algorithm (proposed algorithm). The later image is converted into double type image from the uint8. In second step double type image is converted into binary image and image is segmented based on Surfeit clipping based segmentation algorithm. In third step image skeletonization or thinning process is performed based on Edge Prediction. In fourth step skeletonized image is preprocessed initially and fingerprint features-ridge ending and ridge bifurcations are extracted based on counting number based theory. Again these features are post-processed to remove false minutiae. In the fifth step, these ridge ending and bifurcations are displayed in tabular format and are called as Minutiae table. In final step from these tables features hash code is generated using the MD5 hash algorithm.

The time complexity of Method-1 can be calculated by adding time complexity of all processes or techniques used in order to develop hash code using Method-1. The time complexities of different techniques are shown below in Table 5.2.

**Table 5.2:** Time complexity of different techniques involved in Method-1

| Sr. No | Process/ Techniques | Time Complexity |
|---|---|---|
| 1 | Contrast Adjustment Algorithm | O $(n^2)$ |
| 2 | Surfeit based Segmentation Algorithm | O $(n^2 \log n^2)$ |
| 3 | Edge Prediction based Skeleton Formation | O $(kn^2)$ k lies between 1 and m or n but less than or equal to m or n. |
| 4 | Preprocessing-1 | O $(n^2)$ |
| 5 | Preprocessing-2 | O $(n^2)$ |
| 6 | Minutiae extraction | O $(n^2)$ |
| 7 | Postprocessing | O $(n)$ |
| | Method-1 (Total or greatest of 1 to 7) | $\cong$O$(n^3)$ |

**Method-2:**

As like Method-1, initially image is taken from datasets of FVC ongoing 2002 and contrast adjusted using $\tau$- Tuning Based Filtering Algorithm (proposed algorithm). The later image is converted into double type image from the uint8. In second step double type image is converted into binary image and image is segmented based on Surfeit clipping based segmentation algorithm. Unlike Method1, here thinning or skeletonization process is not performed. Instead of that from the skeletonized image fingerprint features are extracted using Gabor filtering techniques and finally, Hash code is generated using an MD5 hash algorithm like Method-1. The time complexities of different techniques involved in Method-2 are shown in Table 5.3.

**Table 5.3:** Time complexities of different techniques involved in Method-2

| Sr. No | Process/ Techniques | Time Complexity |
|---|---|---|
| 1 | Contrast Adjustment Algorithm | O $(n^2)$ |
| 2 | Surfeit based Segmentation Algorithm | O $(n^2 \log n^2)$ |
| 3 | Method-1 (Total from 1 to 2 or Greatest of two ) | $n^2 + n^2 \log n^2$ |

**Method-3:**

This method is exactly similar to Method-2, but here initial Contrast Adjustment filtering and conversion of the image from uint8 to double type is discarded or ruled out. Like Method-2 here also fingerprint features are extracted using Gabor filtering techniques and finally Hash code is generated using an MD5 hash algorithm like Method-1. The time complexity of Method-3 is shown in Table 5.4.

**Table 5.4:** Time complexity of Method-3

| Sr. No | Process/ Techniques | Time Complexity |
|---|---|---|
| 1 | Surfeit based segmentation | O $(n^2 \log n^2)$ |
| 2 | Method-1 | O $(n^2 \log n^2)$ |

The Time complexity of feature extraction is less than O (n), so we neglect the time complexity of this process.

**Method-4:**

Method-4 is almost same as Method-1. In Method-1 we extract the ridge ending and bifurcation along with its location details. The location details are nothing but pixel position in the pre-processed thinned image. Here we skip post processing because in fingerprint hash

code post-processing does not affect the performance of matching efficiency. Time complexities of different techniques involved in Method-4 are shown in Table 5.5.

**Table 5.5:** Time complexity of different techniques involved in Method-4

| Sr. No | Process/ Techniques | Time Complexity |
|---|---|---|
| 1 | Contrast Adjustment Algorithm | O ($n^2$) |
| 2 | Surfeit based Segmentation Algorithm | O ($n^2 \log n^2$) |
| 3 | Edge Prediction based Skeleton Formation | O ($kn^2$) k lies between 1 and m or n but less than or equal to m or n. |
| 4 | Preprocessing-1 | O ($n^2$) |
| 5 | Preprocessing-2 | O ($n^2$) |
| 6 | Minutiae extraction | O ($n^2$) |
| | Method-1 (Total or greatest of 1 to 7) | $\cong$ O($n^3$) but less than Method-1. |

**Method-5**

Method-5 is based on Freeman chain coding. Freeman chain code extracts all possible boundaries for an image. Which gives starting x and y positions as x0 and y0. This works based on 8 or 4 connected points with respect to a central pixel. The 8 points are represented from 0 to 7 with is a particular format. In order to generate Hash code, we use the first difference of chain code value for all boundaries of the image. These values are unique to each fingerprint. This method makes use of segmentation process. The time complexity of Method-5 is shown in Table 5.6.

**Table 5.6:** Time complexity of Method-5

| Sr. No | Process/ Techniques | Time Complexity |
|---|---|---|
| 1 | Contrast Adjustment Algorithm | O ($n^2$) |
| 2 | Feature extraction using Freeman chain coding | O(n), Lies between n and $n^2$or > O(n) |
| | Method-1 (Total or greatest of 1 to 7) | $n^2$+n |

**Method-6**

Method-6 is based on Euclidean distance matrices of a binary image. In this, it calculates distance from each pixel to its nearest neighbor pixel with value 1 or not equal to zero. The unique distance value, mean and standard deviation are combined to form hash code. This method also makes use of segmentation process. The time complexity of Method-5 is shown in Table 5.7.

**Table 5.7:** Time complexity of Method-6

| Sr. No | Process/ Techniques | Time Complexity |
|---|---|---|
| 1 | Contrast Adjustment Algorithm | O ($n^2$) |
| 2 | Feature extraction using Euclidean Distance | O (n), Less than Method-5 |
| | Method-1 (Total or greatest of 1 to 7) | O($n^2$) |

The time complexities of all six Methods are listed in Table 5.8. The ascending order of time complexity of all six methods is Method-6, Method-5, Method-3, Method-4, Method-2, and Method-1. The highest and lowest time complexities are for Method-6 and Method-1 respectively. The graphical representation of Time complexities of all six methods is shown in Figure 5.2.

**Table 5.8:** Comparison of Time complexities of all Six Methods

| Sr. No | Method Name | Time |
|---|---|---|
| 1 | Method-1 | ≅O($n^3$) |
| 2 | Method-2 | O($n^2 \log n^2$) [$n^2 \log n^2 + n^2$, for small values) |
| 3 | Method-3 | O($n^2 \log n^2$) less than Method-2 |
| 4 | Method-4 | ≅O($n^3$) < Method-1. |
| 5 | Method-5 | O($n^2$) [$n^2$ + n, for small values) |
| 6 | Method-6 | O($n^2$) < Method-5. |

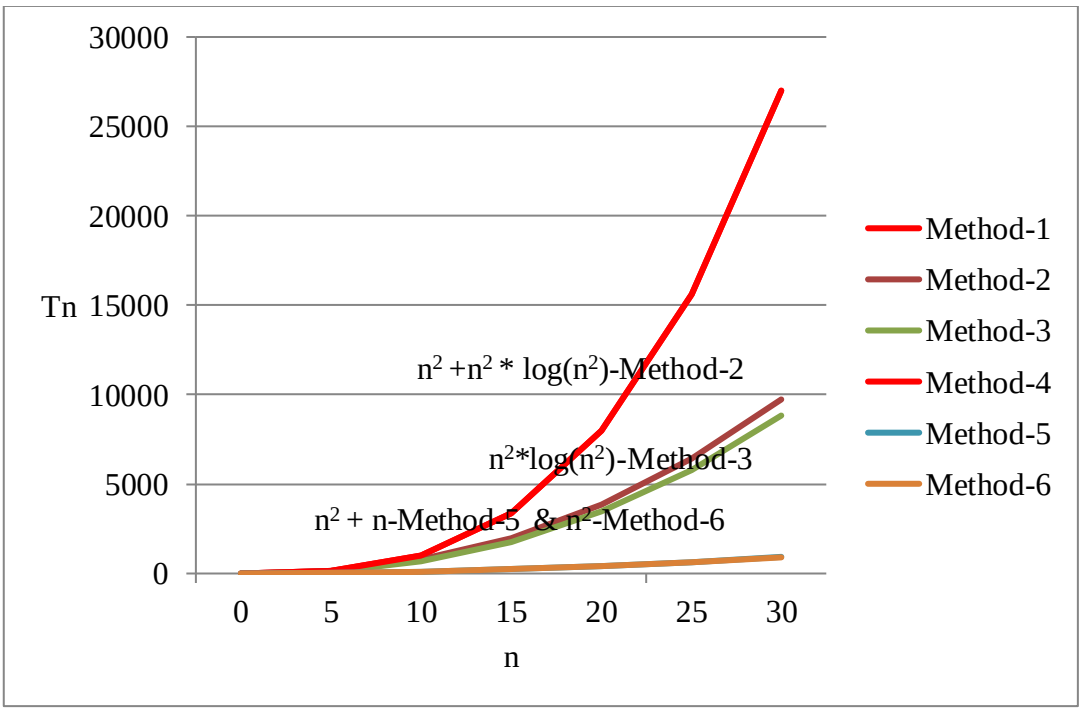



**Figure 5.2:** Graphical Representation of time complexities of all six Methods used in this study

The different techniques used in all six methods are listed out using table 5.9. ☑ The symbol indicates particular technique is used and ☒ Symbol indicates particular technique is not used.

**Table 5.9:** Different techniques used in various methods of fingerprint hash code Generation based on MD5 Algorithm

| Method Name / Techniques | Method-1 | Method-2 | Method-3 | Method-4 | Method-5 | Method-6 |
|---|---|---|---|---|---|---|
| Image resize (256 × 256) | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| Contrast Adjustment using $\tau$- Tuning Based Filtering | ☑ | ☑ | ☒ | ☑ | ☒ | ☒ |
| Conversion from uint8 to double | ☑ | ☑ | ☒ | ☑ | ☒ | ☒ |
| Segmentation based on Surfeit clipping | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| Thinning based on edge prediction | ☑ | ☒ | ☒ | ☑ | ☒ | ☒ |
| Preprocessing | ☑ | ☒ | ☒ | ☑ | ☒ | ☒ |
| Post processing | ☑ | ☒ | ☒ | ☑ | ☒ | ☒ |
| Minutiae Table | ☑ | ☒ | ☒ | ☑ | ☒ | ☒ |
| Minutiae Table with only ride ending and bifurcation details | ☒ | ☒ | ☒ | ☑ | ☒ | ☒ |
| Minutiae Table with ride ending, ridge bifurcation, and location details | ☑ | ☒ | ☒ | ☑ | ☒ | ☒ |
| Gabor Filtering | ☒ | ☑ | ☑ | ☒ | ☒ | ☒ |
| Freeman Chaincode | ☒ | ☒ | ☒ | ☒ | ☑ | ☒ |
| Euclidean Distance | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ |
| Hash coding based on MD5 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |

## 5.4 FINGERPRINT HASH CODE PERFORMANCE EVALUATION MATRICES

All the new or alternative research study of fingerprint verification or recognition system must be tested to know efficiency and effectiveness in differentiating decision between authenticated person and imposter. Before implementing the algorithm or new approach in real-time applications, we need to evaluate its performance using different factors. All these 6

methods are not suitable for authentication purpose because fingerprint, when produced from any type of sensors, give some changes in terms of translations and rotations. Even though above all mentioned methods does not support this features means these are variant to translations and rotations, still fingerprint hash code is not used for authentication and security purpose due to other variations in fingerprints like fingerprints may be swollen or wet or dry due to varying weather conditions or small damages in fingerprints. Even one-bit changes cause a difference in hash code. There are some fingerprint hash codes available in the literature, which is used for verification purpose with slight or small translation and rotation invariant. All these methods make uses of multiple or series of hash code for comparison purpose. This hash code works along with another type of security measures like a password or OTP it will be very robust or effective. Hash code can be used as one factor in multifactor authentication and which usually acts as a key identifier. The performance factors vary from algorithms to algorithm. Even though the only hash code does not support authentication we just compare hash code with all performance factors of fingerprint verification/identification system. This can be part of authentication process so we just include this performance factors.

The most common or general matrices used to quantify the fingerprint biometric system are;

- False Match Rate (FMR)
- False Non-Match Rate (FNMR)
- Receiver Operating Characteristic (ROC)
- Equal Error Rate (EER)
- Failure to Enroll Rate (FTER)
- Failure to Capture Rate (FTCR)
- Accuracy of the system
- Elapsed Time

### 5.4.1 False Match Rate (FMR) or False Acceptance Rate (FAR)

FAR is the likelihood of the Fingerprint Verification System incorrectly classifies the input pattern to a non-matching hash code inside the database. It measures the percentage of invalid inputs, which might be incorrectly classified. In this study in order to calculate FAR, the first sample or impression of each fingerprint of individual user are compared with every other remaining impression or samples of all individual users. So in this study first impression or first sample, the 101_1.tif image is compared with all other 319 fingerprint images. For

Convince purpose in each fingerprint datasets, DB1_B, DB2_B, DB3_B, and DB4_B first 40 fingerprint images are considered as Authenticated and last 40 fingerprint images are considered as Un-authenticated form the total available 80 fingerprint images.

$$\text{FAR} = \frac{Number\ of\ imposter\ Fingerprint\ Accepted}{Total\ Number\ of\ Imposter\ Fingerprints}$$

As each of the 320 fingerprint images produces different hash code or all hash codes are distinct or unique, there is no chance of accepting any imposter fingerprint. All the four methods produce unique hash code for all fingerprint images. So total there will be 1280 hash codes. This shows that FAR in all six methods will be zero.

$$\text{FAR} = \frac{0}{Total\ Number\ of\ Imposter\ Fingerprints} = 0$$

The MD5 hash algorithm produces different hash code even small changes in terms of letters or small fractional differences. This ensures that there is no possibility of having two fingerprints same hash code.

### 5.4.2 False Rejection Rate (FRR) or False Non-Match Rate (FNMR)

FRR is the probability that the fingerprint biometric framework unable to identify a match between the authentic person and a coordinating hash code in the database. Unless and until the input fingerprint given to this system varies at the time of training and testing phase, there is no chance of False Rejection Rate. All the authenticated user or person is properly identified through hash code with one condition that both training and testing phase fingerprint should be identical.

### 5.4.3 Receiver Operating Characteristic (ROC)

The ROC plot is a visual representation of the exchange off between the FAR and the FRR. Normally all matching algorithm makes a decision based on the threshold value. Threshold value indicates how close the difference in score value of the template and sample should be. This threshold sometimes called as sensitivity. When threshold reduces FNMR also reduces but FAR may increase. On the other hand when threshold increases FAR decrease but FRR increases. In this study, there is no scope on Receiver Operating Characteristic (ROC) because here threshold value is not used for matching purpose and also both FAR and FNMR are zero.

### 5.4.4 Equal Error Rate (EER)

EER is the ratio at which both acceptance and rejection mistakes are identical. The value of the EER can be easily generated from the ROC curve. The ERR is a short way to compare the accuracy of the system with exceptional or different ROC curves. An ideal system considers a system with very lowest EER rate. This system produces zero EER rate. Unless and until input fingerprint varies there is no acceptance and rejection mistake.

### 5.4.5 Failure to Enroll Rate (FTER)

FTER is the unsuccessful attempt made to enroll in database or template of an Automatic Fingerprint Identification System by the input. FTER occurs due to low quality or substandard input. The system generates a hash code, even if there is very minute or little minutiae details-ridge ending and bifurcation are present. Failure to enroll rate is also very minimum or zero.

### 5.4.6 Accuracy of the system

This is calculated based on following formula

1-((FAR+FRR)/2)

The accuracy of the system is 1, because FAR and FRR are zero.

### 5.4.7 Failure to Capture Rate (FTCR)

Inside programmed frameworks or Automatic system, the likelihood that the system neglects or unable to distinguish a biometric input when introduced accurately is referred as Failure to capture rate. All the input are accepted or captured by the system if a little minutiae detail is present in the image. All six methods Performance evaluation Matrices results are shown in Table 5.10.

**Table 5.10:** Performance Evaluation Matrices Results

| Sr. No | Performance Evaluation Matrices | Value | Interpretation |
|---|---|---|---|
| 1 | False Match Rate (FMR) or False Acceptance Rate (FAR | 0 | This ensures that there is no possibility of having two fingerprints same hash code. |
| 2 | False Rejection Rate (FRR) or False Non-Match Rate (FNMR) | 0 | Unless and until the input fingerprint given to this system varies at the time of training and testing phase, there is no chance of False Rejection Rate. |

| | | | |
|---|---|---|---|
| 3 | Receiver Operating Characteristic (ROC) | No Scope | Threshold value is not used for matching purpose and also both FAR and FNMR are zero. |
| 4 | Equal Error Rate (EER) | 0 | EER is the ratio at which both acceptance and rejection mistakes are identical and equal to zero |
| 5 | Failure to Enroll Rate (FTER) | 0 | Even partial minutiae details produces Hash code |
| 6 | Accuracy of the system | 1 | FAR and FRR are zero |
| 7 | Failure to Capture Rate (FTCR) | 0 | All the input is accepted or captured by the system if a little minutiae detail is present in the image. |

### 5.4.8 Elapsed Time

The speed refers the time taken by the system to enroll as well as authenticate or reject. In technology term, this can be referred as Elapsed time or time utilized by the new algorithm or model in to enroll and match. Elapsed time is calculated on following configuration system, and which are given in Table 5.11.

**Table 5.11:** Configuration of The System for finding Elapsed Time

| Sr. No. | Parameters | System Configuration |
|---|---|---|
| 1 | Model | Compaq 435 |
| 2 | Processor | AMD E-350 processor 1.60 GHz |
| 3 | Installed Memory | 3 GB (2 GB usable) |
| 4 | System Type | 32-bit Operating System |
| 5 | Operating System | Windows 7 Starter |
| 6 | Software | MATLAB 2015a 32-bit |

Table 5.12 shows elapsed time of the training phase for Method-1 under the above mentioned system. In training phase, usually, we store the template in the database. But in this study, we store hash code instead of a template. Hash code occupies very less memory space compared to the template. Method-1 is based on Minutiae details of the fingerprint image, which includes ridge endings and ridge bifurcations and their locations in terms of pixels positions where these minutiae details exist. The elapsed time of the testing phase for Method-1 under the mentioned system is approximately 0.6 seconds more than training phase. This can vary slightly depending on the size of the database. In any fingerprint verification systems, there will be training and testing phase. In testing phase other than training phase steps it includes comparing and matching sample fingerprint hash code with the already stored hash code in

the database. If a match is found then that image is fingerprint biometric details of authenticated user or else unauthenticated user.

Table 5.12: Elapsed time of the training phase for Method-1

| Method Name | Image name | Elapsed Tine (in seconds) | Average |
|---|---|---|---|
| Method-1 | 101_1 | 48.470198 | 85.809198 |
| | 101_5 | 60.491718 | |
| | 102_2 | 56.248801 | |
| | 103_3 | 83.940243 | |
| | 104_4 | 119.014163 | |
| | 104_7 | 52.786410 | |
| | 104_8 | 221.429194 | |
| | 105_8 | 65.443958 | |
| | 106_6 | 55.507943 | |
| | 109_3 | 100.329180 | |
| | 109_8 | 94.389282 | |
| | 110_3 | 78.436837 | |
| | 110_8 | 79.031646 | |

Table 5.13 shows execution time of the training phase for Method-2. Method-2 is based on Gabor Filter of the fingerprint image. Gabor filter is used to extract features from the segmented image. The execution time of the testing phase is same for all four methods, which are about 0.6 seconds and 0.44 seconds more than training phase.

**Table 5.13: Elapsed time of the training phase for Method-2**

| **Method Name** | **Image name** | **Elapsed Tine (in seconds)** | **Average** |
|---|---|---|---|
| Method-2 | 101_1 | 9.433374 | 6.1170 |
| | 101_5 | 5.912853 | |
| | 102_2 | 5.997807 | |
| | 103_3 | 5.789369 | |
| | 104_4 | 5.884570 | |
| | 104_7 | 5.919527 | |
| | 104_8 | 5.721385 | |
| | 105_8 | 5.910486 | |
| | 106_6 | 5.626518 | |
| | 109_3 | 5.873990 | |
| | 109_8 | 5.908076 | |
| | 110_3 | 5.870832 | |
| | 110_8 | 5.672772 | |

Method-3 is exactly similar to Method-2, but here initial filtering and conversion of the image from uint8 to double type are discarded or ruled out. Like Method-2 here also fingerprint features are extracted using Gabor filtering techniques and finally Hash code is

generated using the MD5 hash algorithm. Table 5.14 shows elapsed time of the training phase for Method-3.

**Table 5.14:** Elapsed time of the training phase for Method-3

| Method Name | Image name | Elapsed Tine (in seconds) | Average |
|---|---|---|---|
| Method-3 | 101_1 | 4.073368 | 2.9547 |
| | 101_5 | 2.866404 | |
| | 102_2 | 2.836739 | |
| | 103_3 | 2.838646 | |
| | 104_4 | 2.795661 | |
| | 104_7 | 2.948594 | |
| | 104_8 | 2.904648 | |
| | 105_8 | 2.837218 | |
| | 106_6 | 2.826639 | |
| | 109_3 | 2.872899 | |
| | 109_8 | 2.859486 | |
| | 110_3 | 2.897389 | |
| | 110_8 | 2.888153 | |

Method-4 is almost similar to Method-1. Here while considering minutiae details-ridge ending and ridge bifurcation, location details of minutiae are not considered. Total count of ridge ending and ridge bifurcation in each fingerprint image is different or it's unique. By considering this property Hash code is developed. So small change in orientation of the image does not affect in hash code variations. This property is very important while considering real-time applications, because while capturing fingerprint image through sensors, always input image orientation may not be same. Table 5.15 shows elapsed time of the training phase for Method-4.

Method-5 is based on Freeman chain coding. Freeman chain code extracts all possible boundaries for an image. Which gives starting x and y positions as x0 and y0. This works based on 8 or 4 connected points with respect to a central pixel. The 8 points are represented from 0 to 7 with is a particular format. In order to generate Hash code we use x0 and y0 position, chain code value for all boundaries of the image, and the chain code first difference value. These values are unique to each fingerprint. This method makes use of segmentation process. This method is invariant to translation. If we translate the image also hash code does not change. Initially, the fingerprint is resized to 256 × 256 sized images and then normalized. Table 5.16 shows elapsed time of the training phase for Method-5. Table 5.16 shows elapsed time of the training phase for Method-5.

**Table 5.15:** Elapsed time of the training phase for Method-4

| Method Name | Image name | Execution Tine (in seconds) | Average |
|---|---|---|---|
| Method-4 | 101_1 | 47.864448 | 84.037799 |
| | 101_5 | 58.578443 | |
| | 102_2 | 54.409824 | |
| | 103_3 | 77.683423 | |
| | 104_4 | 116.227812 | |
| | 104_7 | 52.218293 | |
| | 104_8 | 218.873006 | |
| | 105_8 | 64.357929 | |
| | 106_6 | 54.840099 | |
| | 109_3 | 99.497319 | |
| | 109_8 | 93.487273 | |
| | 110_3 | 76.325792 | |
| | 110_8 | 78.127733 | |

Method-6 is based on Euclidean distance matrices of a binary image. In this it calculate distance from each pixel to its nearest neighbour pixel with value 1 or not equal to zero. The unique distance value, mean and standard deviation are combined to form hash code. This method also makes use of segmentation process.

**Table 5.16:** Elapsed time of the training phase for Method-5

| Method Name | Image name | Execution Tine (in seconds) | Average |
|---|---|---|---|
| Method-5 | 101_1 | 6.374650 | 5.226603 |
| | 101_5 | 5.106057 | |
| | 102_2 | 4.323511 | |
| | 103_3 | 5.135806 | |
| | 104_4 | 5.209417 | |
| | 104_7 | 7.147446 | |
| | 104_8 | 5.599593 | |
| | 105_8 | 5.764250 | |
| | 106_6 | 4.662723 | |
| | 109_3 | 5.569806 | |
| | 109_8 | 4.730140 | |
| | 110_3 | 4.061247 | |
| | 110_8 | 4.078556 | |

Table 5.17 shows elapsed time of the training phase for Method-6.

**Table 5.17: Elapsed time of the training phase for Method-6**

| Method Name | Image name | Elapsed Tine (in seconds) | Average |
|---|---|---|---|
| Method-6 | 101_1 | 3.268564 | 3.015870 |
| | 101_5 | 3.081479 | |
| | 102_2 | 3.086628 | |
| | 103_3 | 2.968837 | |
| | 104_4 | 3.045837 | |
| | 104_7 | 3.050931 | |
| | 104_8 | 2.831525 | |
| | 105_8 | 3.068100 | |
| | 106_6 | 2.820155 | |
| | 109_3 | 3.055488 | |
| | 109_8 | 3.049432 | |
| | 110_3 | 3.051967 | |
| | 110_8 | 2.827368 | |

The elapsed time varies slightly depending on the image. If fingerprint image having noise or little minutiae details then the execution time increases little bit. Table 5.18 shows average elapsed time for training phase combined for all the six methods.

**Table 5.18:** Average Elapsed time of training phase for all six Methods

| Sl. No | Method name | Average Elapsed time (In seconds) |
|---|---|---|
| 1 | Method-1 | 85.809198 |
| 2 | Method-2 | 6.1170 |
| 3 | Method-3 | 2.9547 |
| 4 | Method-4 | 84.037799 |
| 5 | Method-5 | 5.226603 |
| 6 | Method-6 | 3.015870 |

From the Table 5.18, it's clear that Method-3 and Method-6 take more or less same time and variations come due to variations in images. Testing phase takes little bit more time than training phase. Testing depends on the size of the database.

The Table 5.19 shows different requirements of the good fingerprint Hash code. The Table 5.19 contains few rows and columns, in which rows represent different requirements of fingerprint Hash code, which include distinct Hashes, distinct hashes for different fingers of the same person, the Hash code generated from partial minutiae, and salting in an MD5 hash generation. Salting is a random input or value added to original value to make the hash function more secure. The one more requirements of the Hash code is translation and rotation invariant, which not given emphasis on this study because Hash code are used as

identity key or index key and not used entirely or solely for security purpose. So in this study, we ignore this feature. The column of the Table 5.19 contains all the six methods that we have used in this study. The values of the tables contain Boolean values as yes and no. Yes is represented using☑ symbol and No is represented using ☒ symbol. The generated Hash code should not be compromised by the intruder. To achieve this parameter used for generating Hash code should be very strong. The factors used for measuring the quality of salting are double precision numbers as a parameter for Hash code, a total number of characters or string length, and the generated hash code should not be in the online MD5 decrypting database.

**Table 5.19:** Different Requirements of Good Fingerprint Hash code Methods

| Dataset name | Requirements | Method-1 | Method-2 | Method-3 | Method-4 | Method-5 | Method-6 |
|---|---|---|---|---|---|---|---|
| DB1_B 2002, DB2_B 2002, DB3_B 2002, and DB4_B 2002, | Distinct Hashes | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| | distinct hashes for different fingers of the same person | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| | Hash code generated from partial minutiae | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| | Translation and rotation invariant | ☒ | ☒ | ☒ | ☒ | ☒ | ☒ |
| | Double precision numbers as parameter for Hash code | ☒ | ☑ | ☑ | ☒ | ☒ | ☒ |
| | String length (Large) | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| | Generated hash code should not be decrypted using online MD5 Database | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |

The Method-2 and Method-3 hold all these factors, whereas Method-1, Method-4, Method-5, and Method-6 do not hold characteristics of double precession numbers. Datasets are from FVC ongoing 2002. This Dataset contains four groups as DB1_B, DB2_B, DB3_B, and DB4_B. DB2_B datasets contain some partial fingerprint images and examples for partial fingerprint image are 104_8 and 105_3. The Method-5 and Method-6 handle more efficiently partial fingerprints and thereby generates Hash code.

## 5.5 SCREENSHOTS OF FINGERPRINT HASH CODE IMPLEMENTATION USING MATLAB2015A

This section explains the different screenshots used in the implementation of fingerprint Hash code in Matlab2015a for Method-1. Figure 5.3 shows a screenshot of Loading, Select Image, Enhancement, and Segmentation Button of Method-1. Here Loading button gives details of how to initially connect with WampServer and create database and table. This also gives an explanation how to connect database from MATLAB2015a. Select Image button selects and loads the image to the system. Enhancement button gives result contrast adjustment of the fingerprint image. Segmentation button gives segmentation of the contrast adjusted fingerprint image. Figure 5.3(a) shows details of Selection of the fingerprint image and Enhancement buttons. Figure 5.3(b) shows Database connection and Segmentation buttons of preprocessing state. All these components are part of the mainGUI window used in Method-1.


**Figure 5.3 (a):** Screenshots of mainGUI Components used in Method-1: Select Image and Enhancement Buttons

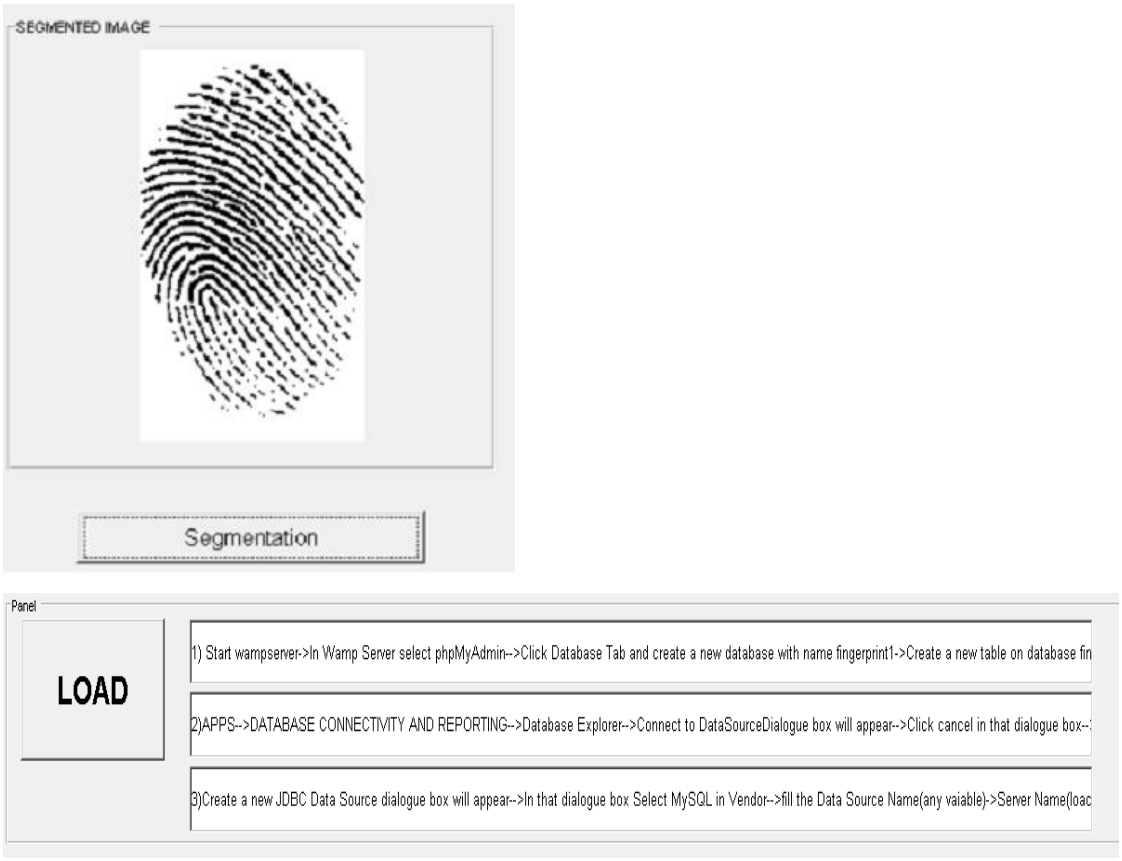
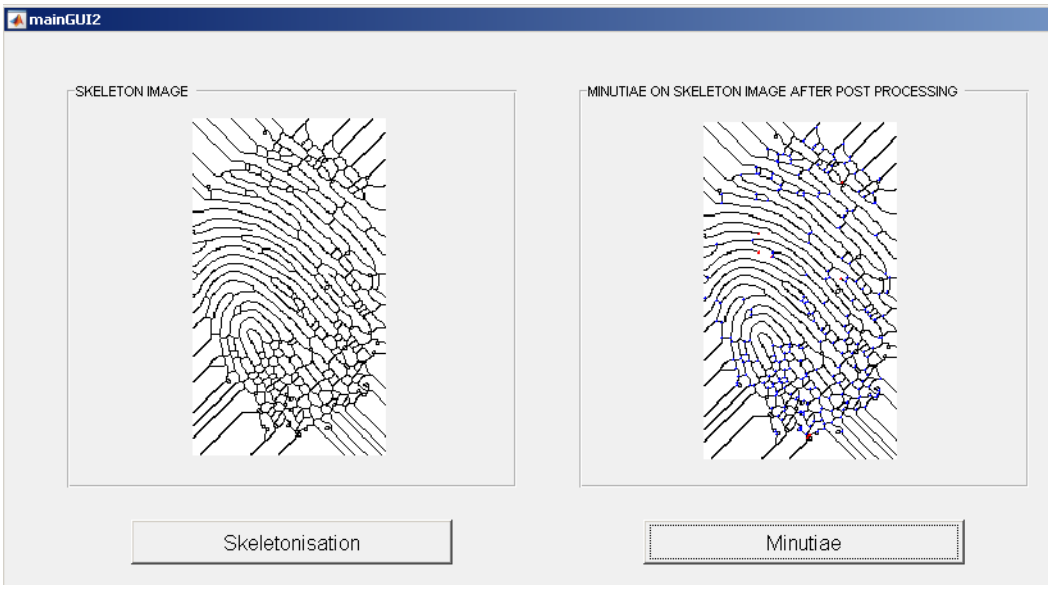



**Figure 5.3 (b):** Screenshots of mainGUI Components used in Method-1: Load, Select Image, Enhancement and Segmentation Process

Figure 5.4 shows screenshots of Skeletonisation, Minutiae (Minutiae on Skeleton image after post-processing), and Minutiae Table of mainGUI2 window. Skeletonisation process is also called as thinning, which is obtained by lowering the thickness of every line of a fingerprint pattern or ridge pattern to just a single pixel width. Minutiae are shown with ridge ending in red color and Ridge bifurcation in green color. Minutiae table contains Ridge ending and Ridge bifurcation feature with its location details. The location details contain each ridge ending and ridge bifurcation pixel x and y value.

Figure 5.5 shows Screenshots of mainGUI3, which is related to Database connection, fetching and Hash Matching process. The status shows whether Hash code is matched or not if Hash code matches then status displays authenticated person, else, un-authenticated person.




MINUTIAE TABLE

| | 1 | 2 | 3 |
|---|---|---|---|
| 1 | 5 | 86 | 3 |
| 2 | 15 | 76 | 3 |
| 3 | 17 | 106 | 3 |
| 4 | 18 | 85 | 3 |
| 5 | 21 | 49 | 3 |
| 6 | 21 | 83 | 3 |
| 7 | 21 | 91 | 3 |
| 8 | 25 | 57 | 3 |
| 9 | 25 | 61 | 3 |
| 10 | 25 | 99 | 3 |
| 11 | 26 | 66 | 3 |
| 12 | 27 | 111 | 3 |
| 13 | 29 | 67 | 3 |
| 14 | 29 | 100 | 3 |
| 15 | 30 | 56 | 3 |
| 16 | 30 | 111 | 3 |
| 17 | 31 | 57 | 3 |
| 18 | 32 | 67 | 3 |
| 19 | 32 | 107 | 3 |

**Figure 5.4:** Screenshots of mainGUI2 components used in Method-1: Skeletonisation, Minutiae and Minutiae Table

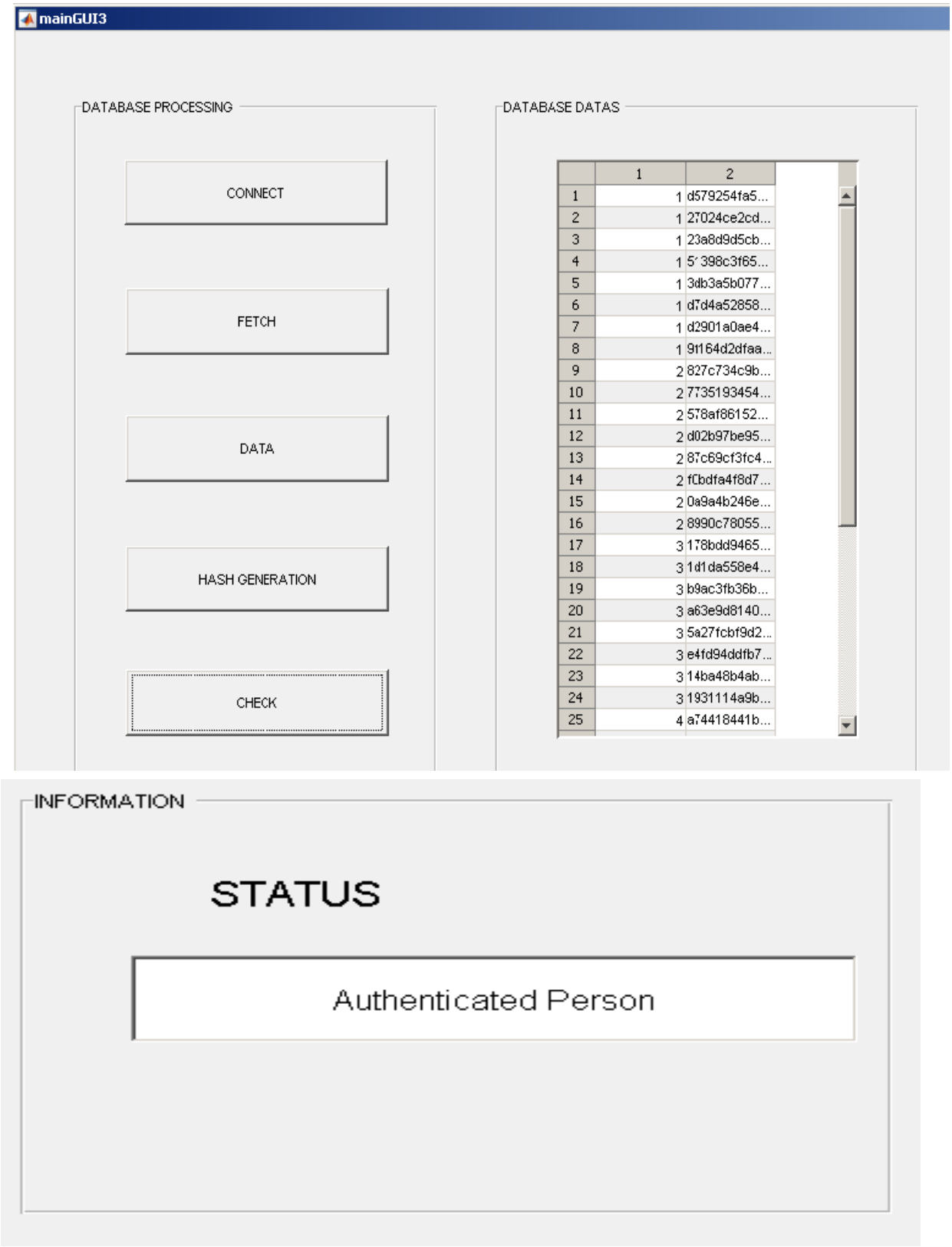



**Figure 5.5:** Screenshots of mainGUI3 components used in Method-1: Database connection, fetching, and Hash Matching, and Status

## 5.6 MULTIFACTOR AUTHENTICATION MODEL USING FINGERPRINT HASH CODE, OTP AND PASSWORD

The research study reveals that fingerprint is not so secured like secured passwords which consist of alphanumeric characters, number and special characters. Fingerprints are left at crime places, on materials or at the door which is usually class of latent fingerprints. We cannot keep fingerprint as secure like rigid passwords. Using some modern technology with copper and graphite spray it's easy to mimic fingerprint image. Fingerprints are not fully secret if passwords are leaked or hacked, it easily revocable using another password (Krishna Prasad, K., & Aithal P. S., 2018e). But in a biometric security system, which uses only biometric features, is not easy to change fingerprint key or fingerprint are static biometric, which never change much throughout the lifespan. Fingerprints are left at car, door or anyplace where every person goes and places his finger.

Fingerprint Hash code is not used for full security or authentication purpose but it can be combined with other security elements like password or OTP in order to enhance security. Fingerprint Hash code acts as the key, which can uniquely identify every person. So it can be replaceable with user-id or username and can work along with text-based or picture based or pattern based passwords. The fingerprint hash code is not constant with biometric sensors or readers. There are many types of research are carried out translation and rotation invariant fingerprint hash code generation but even small or pixel changes cause difference in Hash code.

Based on the different Methods of Fingerprint Hash code generation, it reveals that fingerprint hash code does not suit exclusively for authentication or security purpose. But it uniquely identifies an individual person or human being through a Hash code key. This research work proposes an alternative method of authentication using Fingerprint Hash code, OTP and Passwords. Figure 5.6 shows Dataflow Diagram of Multifactor Authentication model used in this study.

Initially on the client side using an interface user loads fingerprint image into the system. At first Finger image, foreground feature is extracted from the background using segmentation Later, using Gabor filtering fingerprint image features are extracted. These features are encrypted and sent to the server. As soon as these features arrive at the server in encrypted form, the server receives that and request for One Time Password from OTP generator. OTP generator is a module or function, which is located at server machine. Time synchronized OTP is sent to the registered mobile phone user. Client system prompts a message to enter

OTP, which is received to the registered mobile phone of the user. The user enters that OTP through the client interface and this OTP is compared with server generated OTP at the server side.

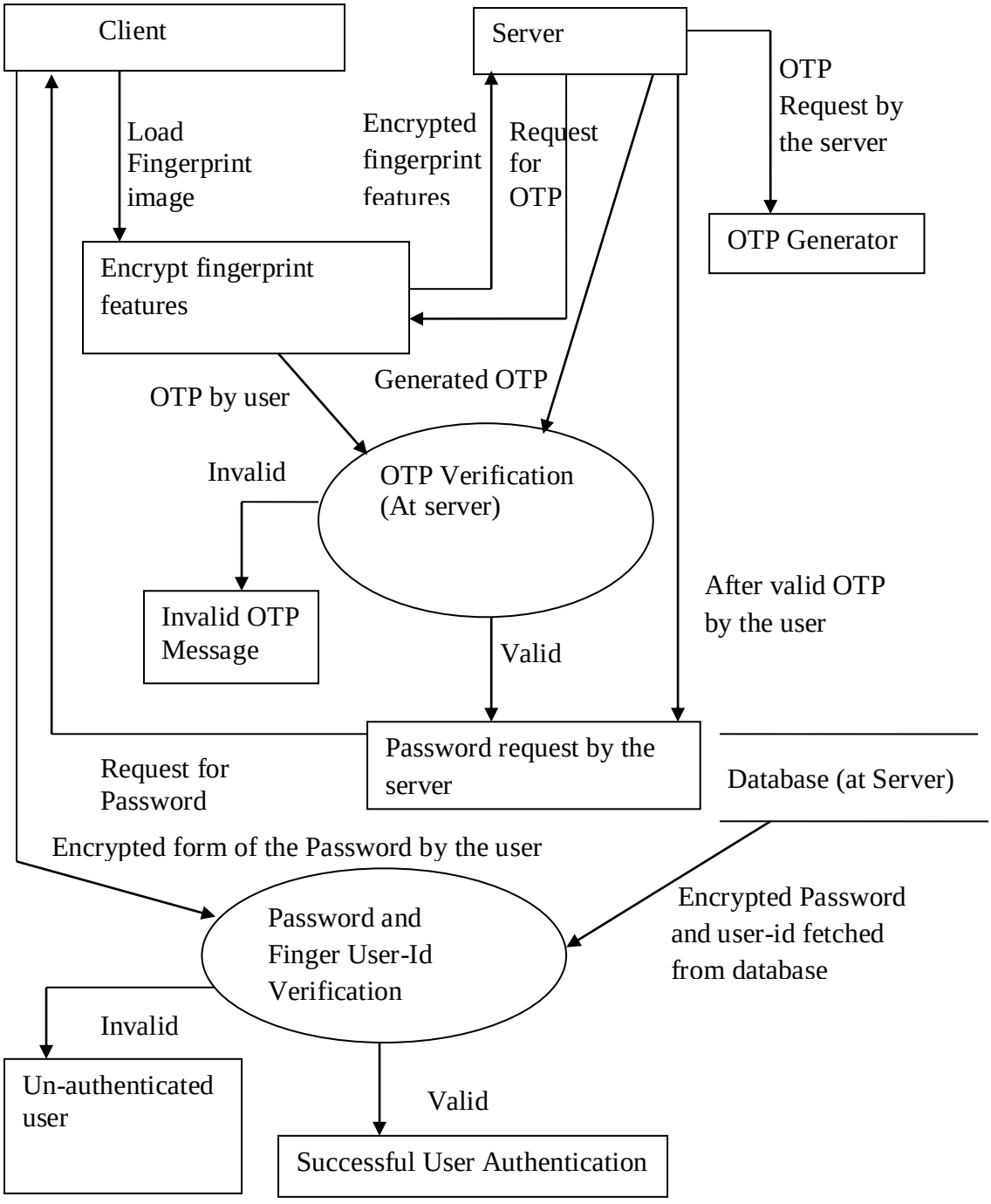



**Figure 5.6:** Dataflow Diagram of Proposed Multifactor Authentication

If OTP is verified, server requests for the password, the user enters the password through the client-side interface and entered password reaches to the server. The server verifies the user entered a password with the already stored password in its database. In the database, the

password is stored in encrypted format. The password which is stored in the database in encrypted form and finger user-id hash code is encrypted one again to enhance security. So if an intruder gets stored hash codes from the database, still authentication cannot become successful. If both password and Fingerprint Hash code match then the user is considered as an authenticated user. In other words authentication process successfully completes when OTP, Password and Fingerprint Hash code matches. If anyone out of Fingerprint Hash code or Password does not matches user is considered as an unauthorized user. If OTP not matches then the user is blocked from further steps in the authentication process. In this research study, this is not implemented as server and client in different machines. The model of this approach is implemented on the same machine using MATLAB 2015a.

### 5.6.1 One Time Password Generator

In this research work One Time Password Generator is responsible for generating OTP. This is a function located on the server. In this study, Time synchronized OTP is generated by combining some features. The procedure for generating OTP is explained using Figure 5.7.

1. Generate the Hash code for input fingerprint using MD5 Hash Function.
2. Extract system Date and Time.
3. Extract seconds separately.
4. Consider only integer part of the seconds.
5. A- 4 × 4 sized matrix of random number is generated.
6. Date and Time are converted into string data type.
7. Random matrix is concatenated with Date and Time string.
8. Hash code of the input fingerprint image is concatenated with result of 7.
9. Hash code is generated for combined string obtained from Step-8.
10. A random number is generated between1 to 32.
11. If the random number is in between 1 to 8 (including both) then extract first 8 characters of the Hash code of size 32 characters generated in Step-8.
12. If the random number is in between 9 to 16 (including both) then extract next 8 characters (from position 9 to 16) of the Hash code of size 32 characters generated in Step-8.
13. If the random number is in between 17 to 24 (including both) then extract next 8 characters (from position 17 to 24) of the Hash code of size 32 characters generated in Step-8.
14. If the random number is in between 24 to 32 (including both) then extract next 8 characters (from position 24 to 32) of the Hash code of size 32 characters generated in Step-8.

**Figure 5.7:** Procedure for gemerating One Time Password (OTP)

## 5.7 SCREENSHOTS OF MULTIFACTOR AUTHENTICATION MODEL

In this research work, Multifactor Authentication model is not implemented as a client-server concept, but its model is implemented using MATLAB2015a. In order to extract the features of the fingerprint image, Gabor filtering is utilized. Figure 5.8 shows screenshots of fingerprint feature extraction by utilizing segmentation process. This is treated as a client-side process. In client-side user fingerprint image is loaded into the system.

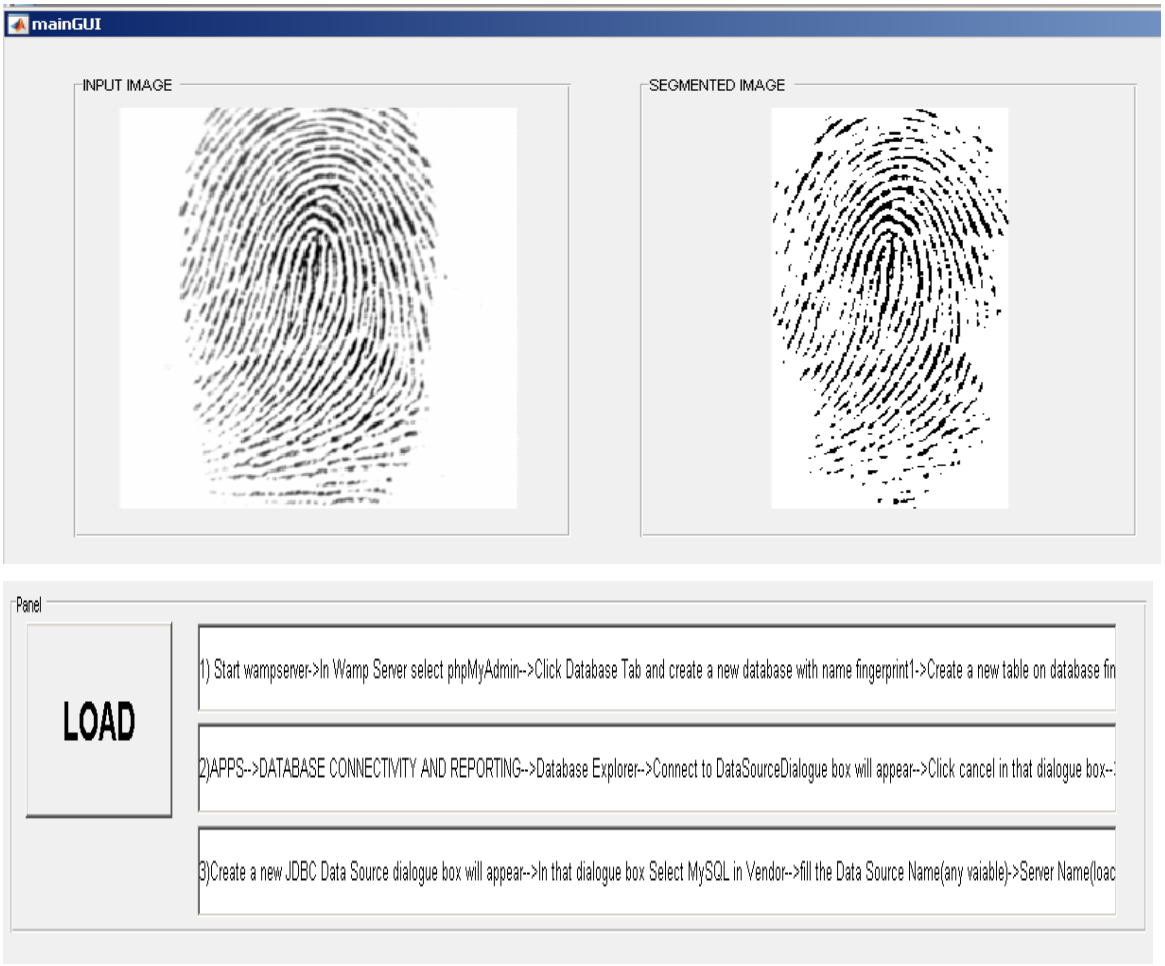



**Figure 5.8:** Screenshots of fingerprint feature extraction using segmentation Process (Client-side processing)

Initially, the image is segmented and foreground region of the image is extracted from background region. Next fingerprint features are extracted. These features are converted into some double precision number using Gabor filtering. These values are encrypted and sent to the server for generating Hash code.

Server-side processing includes Hash generation, OTP generation, OTP verification, Password Verification, and Fingerprint Hash verification. As soon as server receives

fingerprint features in encrypted form, the server decrypts it and generates Hash code. This Hash code is used to generate OTP along with some other details. Figure 5.9 shows input dialog box for OTP.

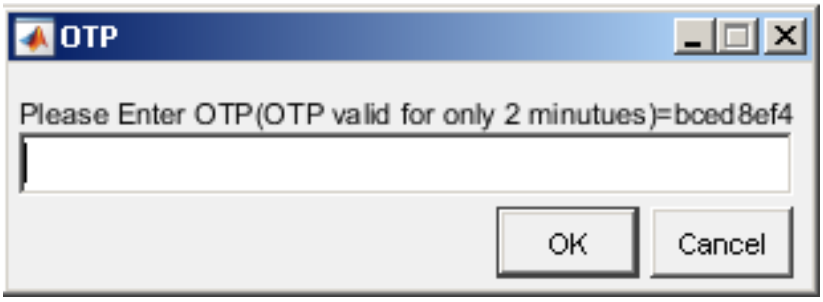



**Figure 5.9:** Screenshots of OTP with 2-Minutes of life span

As soon as Client receives the OTP, the user enters OTP through client interface and it is passed to the server back for verification, If OTP matches, server prompts a password for a client, and the user enters the password. Figure 5.10 shows the password message.

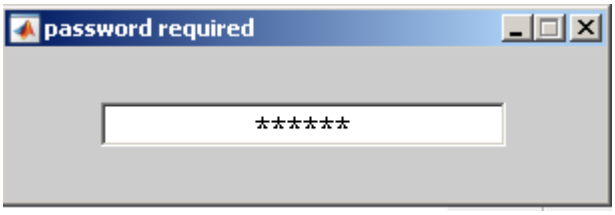



**Figure 5.10:** Screenshots of Password

Once user entered password reaches to the server, the server verifies the password with database and if verification becomes a successful user is authenticated. Figure 5.11 shows the status of authentication.

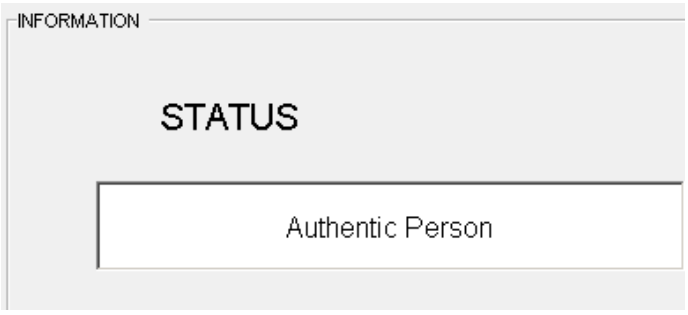



**Figure 5.11:** Screenshots of Status used in Multifactor Authentication Model

Table 5.20 shows screenshots of database values. Id represents the Hash value of the user fingerprint and hash column represents password. In the database, table password is stored in cryptographic Hash function. In the worst case, if an intruder hacks the database, he/she

cannot understand password, because which is already stored in the Hash form in the database.

**Table 5.20:** Fingerprint-id and Password (hash) stored in Database

| Id | Hash |
|---|---|
| 6b0cb74f5f8773667bf633a232b7ed12 | 63e7c5b52f995c466de97c7e1b13c45a |
| a0e5550770d0b6f72ca7f0afc1d0509a | 46aa16250c809e993ccde5d5cababe12 |
| 2b4e687bf015532ba5ec6a0403d90935 | 2bc98e659d9627bca74ef482a953af5d |
| f1a14a44898a2eb2272aa76fe4ed8295 | 176f93ff4c5bb289decdfc2d9f8297a2 |
| 3b5a17d8092dbf0b23f71c2031dc2161 | 6ee1bca71a01ebba0f63fd076402f14f |
| 4fbfe255d3610c804092653f9b4f61f6 | 5c98d6ca3f5d51048c98112cab8cb3b6 |
| a542a749b79cfd482c4a45f4912f49ff | a843da9c81b63495736d1af10435227b |
| b8454d515e6f0a8893a5c97019e303ab | e2e638ac139b6da754e0a0e0533e65d7 |
| c44837ccf2bf4903057c8b1678963fd5 | 1191e3745ad3aa05f405015cb4b88974 |
| 27f649b4d979e9b13ee5c412ab0d05a3 | ebdd5c0b31050a546260fd849093f11d |

## 5.8 CHAPTER SUMMARY

In this chapter, we have discussed and analyzed all six Methods used in this study with different performance evaluation matrices. We have calculated overall time complexity of the six Methods. Method-1 and Method-6 are having highest and least time complexity. The elapsed time was maximum for Method-1 and minimum for Method-3. By considering the time complexity, Elapsed Time, and salting strength we have considered Method-3 was best and used for generating Hash code for Multifactor Authentication Model using the Hash code, OTP and Password. Even though Method-3 has little bit more time complexity compare to Method-5 and Method-6, its salting strength is very good due to the use of 12 double precision numbers. The new authentication model uses static one time captured fingerprint image for identity purpose and OTP and password are used for security purpose. We used a simple algorithm for generating a random OTP which is time synchronized.

**********

# CHAPTER SIX

# *Factors and Elemental Analysis of Multifactor Authentication Model through ABCD Framework*

**Contents** **Page. No**

## 6.1 INTRODUCTION

Automated fingerprint identification System (AFIS) is composed of various strategies like preprocessing, enhancement, segmentation, thinning, function extraction, post-processing, minutiae orientation, and alignment. Fingerprint Hash code acts as the key, which could uniquely distinguish all people. So it could be replaceable with person-id or username and might work along with text-primarily based or picture primarily based or pattern primarily based passwords. The fingerprint hash code isn't always steady with biometric sensors or readers. There are many styles of research are done translation and rotation invariant fingerprint hash code generation but even small or pixel adjustments purpose a distinction in hash code.

The ABCD Framework is used to analyze a new model with advantages, benefits, constraints, and disadvantages in a systematic way. The whole framework is split into various issues, the area which new model is targeted. Various key properties and affecting elements of the new model may be diagnosed and analyzed under each issue identified earlier. Later some of the important constituent element for every identified issue is diagnosed and analyzed. This approach to evaluation is straightforward and additionally gives a guiding principle to become aware of and take a look at the effectiveness of the new model in this context. As per ABCD analysis various determinant issues related to Multifactor Authentication Model for Verification/Authentication purpose are (1) Security issues, (2) User-friendly issues, (3) Input issues, (4) Process issues, (5) Performance Evaluation matrix issues.

Here we compare Multifactor Authentication Model based on Fingerprint Hash code, OTP, and Password with different existing systems of the same kind of slightly different systems or any system which makes use of biometric or password or username or OTP for authentication. The different system considered in this study are the traditional user-d, password-based internet/mobile banking system, Apple iPhone X face recognition system, HDFC OTP Checkout for online transactions, and Indian Aadhaar card registration process. These comparisons help to understand where this model stands in terms of its features compare to the existing systems.

## 6.2 ABOUT ABCD FRAMEWORK

Many techniques are available in the literature, to investigate the individual characteristics, system traits, and effectiveness of an idea or concept, the effectiveness of a method to know its merits and demerits and also business value in the society. The individual traits or

organizational effectiveness & techniques in a given surrounding may be studied the usage of SWOT analysis, SWOC evaluation, PEST analysis, McKinsey7s framework, ICDT version, Portor's 5 force model and so on. Recently a new model is introduced to these analysis areas called ABCD analysis framework (Aithal et al., 2015), which is used for analyzing business concept, business system, new technology, new model, new idea/concept etc. In the qualitative evaluation the use of ABCD framework, the new idea or new system or new strategy or new generation or new model or new concept is further analyzed studied or analyzed using critical constituent elements. In the quantitative evaluation, the use of ABCD framework (Aithal, 2016) can be used to assign appropriate score or rating for each critical constituent elements, which is calculated through empirical research. The final score is calculated and based on the score the new idea or new system or new strategy or new generation or new model or new concept can be accepted or rejected. Consequently, ABCD evaluation framework may be used as a research tool in these regions and is easy but systematic study or analyzing method is essential for business concept or systems or models or ideas or strategy evaluation (Krishna Prasad, K., & Aithal, 2017c; Aithal et al., 2016a). ABCD analysis framework can be used for analyzing private universities (Aithal et al., 2016b), New National Institutional Ranking System (Aithal et al., 2016c), Dye-doped Polymers for Photonic Applications (Aithal, S., & Aithal, P. S., 2016), Annual research productivity (Aithal et al., 2016d) and On-line Campus Placement Model (Shenoy & Aithal, 2016) and also many more.

## 6.3 ABCD ANALYSIS OF FINGERPRINT HASH CODE, PASSWORD AND OTP BASED MULTIFACTOR AUTHENTICATION MODEL

Multifactor Authentication Model used in this research work can be analyzed using ABCD Analysis (Krishna Prasad, K., & Aithal P. S., 2018f). The complete framework is divided into various issues, the area which new model is focused. Various key properties and affecting the area of the new model may be identified and analyzed under each area of issues identified before.

Later some of the critical constituent element for each identified issue is recognized and analyzed and which is shown in Figure 6.1. This method of analysis is simple and also offers a guideline to identify and examine the effectiveness of the new model in this context. As per ABCD analysis various determinant issues related to Multifactor Authentication Model for

Verification/Authentication purpose are: (1) Security issues, (2) User-friendly issues, (3) Input issues, (4) Process issues, and (5) Performance Evaluation matrix issues.

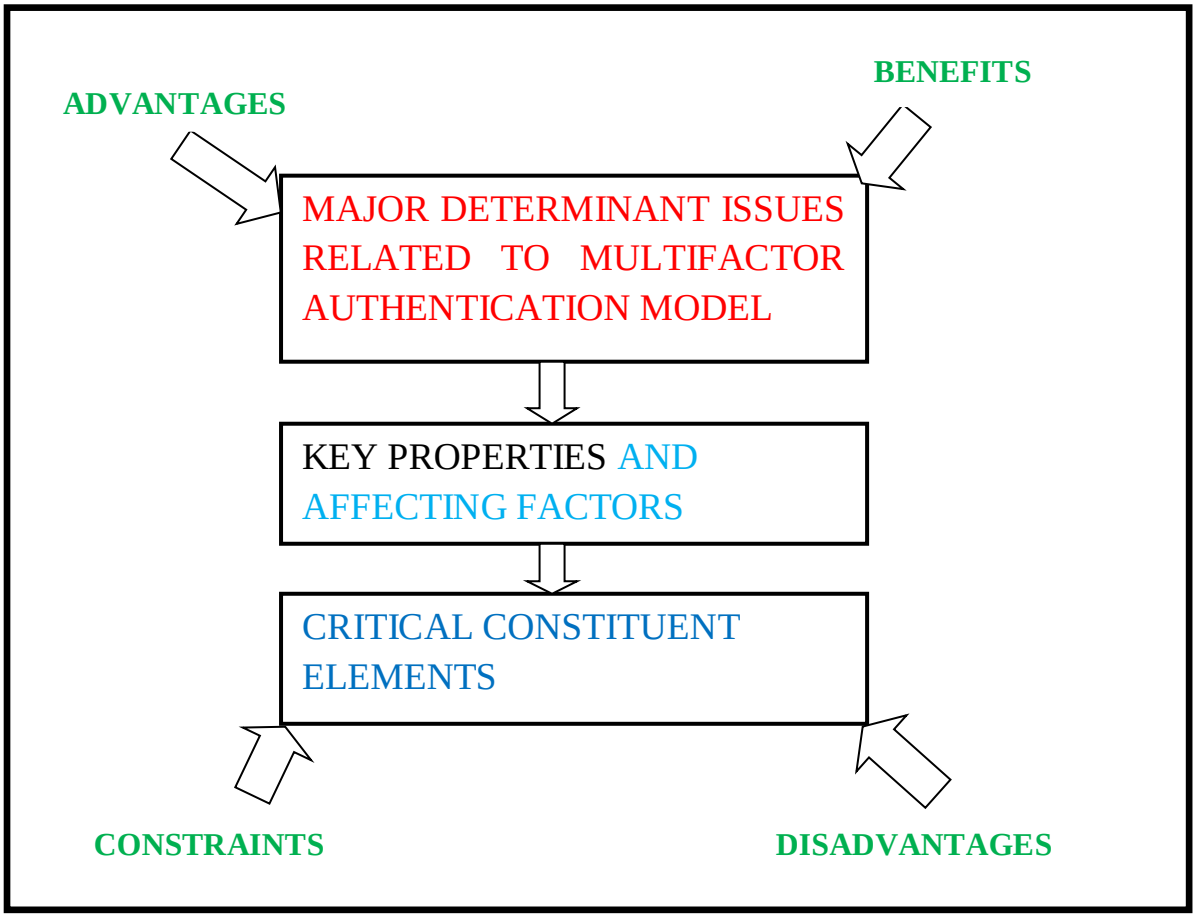



**Figure 6.1:** Block diagram of Issues affecting the Fingerprint Hash code, Password, OTP based Multifactor Authentication Model

(1) Security Issues

Security is very important in the Authentication process. An ideal security refers that a system which is impossible for an intruder to break or impossible for the unregistered user to access the system. In Authentication process, security refers safeguarding the user personal data used for authentication process, which includes, Fingerprint Hash code, Password, One Time Password (OTP). The affecting factors of Security issues include Fingerprint Hash code, Password, and OTP under key properties or levels like user level, network level, and Database or template level are determinant factors under the constructs Advantages, Benefits, Constraints, and Disadvantages of the new model.

(2) User-friendly Issues

The user-friendliness of Multifactor Authentication Model signifies that user should able to get access to the system effortless or easily without remembering anything or very minimum amount of data. The affecting factors under key properties like Response time, Access time, Automatic Process, Speed, and Availability are determinant factors under the constructs Advantages, Benefits, Constraints, and Disadvantages of the new model.

(3) Input Issues

Input ensures that registered user should able to get access to the system or authenticated with very less or no input or automatically. The affecting factors under key properties like Minimum Possession, Least input, Input Selectivity, Ubiquitous Data, Reliability, Usability, Efficiency, Input security and execution time are determinant factors under the constructs Advantages, Benefits, Constraints, and Disadvantages of the new model.

(4) Process Issues

Process Issues ensures that user should able to complete authentication process without any fault, fast and completely. The affecting factors under key properties like Atomicity, Consistency, Isolation, Availability, effort free, and High durability are determinant factors under the constructs Advantages, Benefits, Constraints, and Disadvantages of the new model.

(5) Performance Evaluation matrix issues

This refers all the performance evaluation matrices normally used for the authentication system. The affecting factors under key properties like False Acceptance Rate, False Rejection Rate, Equal Error Rate, Failure to enroll rate, Accuracy Rate, and Execution are determinant factors under the constructs Advantages, Benefits, Constraints, and Disadvantages of the new model. Each determinant issue has sub-issues called key properties used for analyzing the advantages, benefits, constraints and disadvantages, the four constructs of the framework. The factors affecting the various determinant issues of Multifactor Authentication Model for each key issue under four constructs are derived by a qualitative data collection instrument namely, focus group method. The Table 6.1 shows analysis of Fingerprint Hash code, password, and OTP-Multifactor Authentication Model for Verification purpose under four constructs as Advantages, Benefits, Constraints, and Disadvantages.

**Table 6.1:** Analysis of Fingerprint Hash code, Password, and OTP-Multifactor Authentication Model for Verification purpose

| Determinant Issues | Key properties | Advantages | Benefits | Constraints | Disadvantages |
|---|---|---|---|---|---|
| Security Issues | User-level security (For Biometric Image-Hash code) | Easy to secure using personal devices like mobile phone, Laptop, USB drive, and private cloud drive | increases demand for Cloud Drive, Mobile, Pen drive, and laptop | High Security of the Cloud Drive, USB device, Laptop, and Mobile Phone is questionable | Acceptance by the user |
| | Network Level Security | Non-reversible, Non-Revocable Hash code, | Customer faith increases, Can attract new customer | tampering of data | Network failure due to some uncontrollable circumstances |
| | Database or Template Security | Single Hash value is used for comparing, Nonrevertible Hash code | Efficient memory use, Database is easily manageable | Database table requires values in Hash form | Database failure, Server failure |
| User-friendly Issues | Response time | Increased rate of growth of authentication process | Increased customer pool | Requires high configuration system and efficient algorithms | Hardware and Software cost |
| | Access time | User Instantaneous authentication | Reduced Queuing, Reduced waiting process | Requires good network, memory and processor | Hardware and software cost |
| | Speed | Increased Authentication request per unit time | Increased customer satisfaction, retention and acquiring new customers becomes easy | Requires high configured system and reduced time complexity | Hardware and software cost, High bandwidth network, |
| | Automatic process | Minimum prior | Increased customer | Ability to make | Utilization of hardware and |

| | | | | | |
|---|---|---|---|---|---|
| | | information of the system required | satisfaction, | difference between registered and unregistered user, processing power | software resources are too high complex backend design of the user interface |
| | Availability | Ubiquitous authentication | Reduced request queue | Dedicated server and network | 24 × 7 working server |
| Input Issues | Minimum Possession | minimum knowledge parameters required for authentication | User get authenticated anywhere without carrying anything | Capacity of the system to differentiate between registered user and intruder with minimum data | Lack of information |
| | Least input | Simple User authentication from customer point of view | Reduced I/O operation | Requirement of unique and robust parameter for user Authentication | Lack of information |
| | Input Selectivity | Reduced error in inputting | Increased Customer comfort and satisfaction | User ability to identify correct image | Negligence of the user in selection of input |
| | Ubiquitous input | Ubiquitous Authentication process | Increased user satisfaction | Requirement for high configuration system and network availability | Misuse of Authentication system, More intruder will try to break the system |
| | Reliability | Improved consistency of the system | Improved user satisfaction | Operating cost | Significant startup and Maintenance cost |
| | Usability | One parameter for multipurpose like fingerprint | Reduced parameter requirement for | The ability of the software to make a distinction | Intruder or un-registered user tries to get multipurpose |

| | | | | | |
|---|---|---|---|---|---|
| | | image | authenticati on | between the different context of the same parameter | parameter used in the authentication process. |
| | Efficiency | Increased number of requests | Accurate results, error- free output | Quality of the input | Inability to handle error prone or partial input |
| | Security | User personal data protection | Trust and faith over system increases | Uniqueness, permanence, Universality, and revocability | Cost of the system become high. |
| | Execution time | Increased growth rate in authentication | Trust and faith over system increases | Requires a good time and space complexity algorithm | Requirement of Good configuration system increases cost |
| Process Issues | Atomicity | Authentication process Rollback or Commit at the time of system failure | Authenticati on failure is very rare or practically zero. | Need of good fault tolerance techniques. | Requires separate programme for database protection /safeguards |
| | Consistency | Ensures the consistent state at the time of system failure | Authenticati on process ensures consistency, | Need of good fault tolerance techniques. | Database management and safe guarding requires extra efforts and cost |
| | Isolation | Authentication process gets isolation property | Enhanced user trust and satisfaction | Need of good lock-based concurrency control system | Database management and lock-based concurrency control requires extra cost |
| | Availability | Ubiquitous authentication | Reduced request queue | Dedicated server and network | 24 × 7 working server |
| | Effort free | User freely and easily interacts with authentication system | User enjoys working with system, Increased user trust and satisfaction | Requires navigational and narrative user interface, Input should be selective rather than | Complex design of user interface and programme increases cost |

| | | | | | |
|---|---|---|---|---|---|
| | | | | entering | |
| | Durability | Changed Password and Biometric-ID durable for long time | Revocability can be done easily, if password or id is compromised | Need of good fault tolerance techniques. | Database management and safeguarding requires extra efforts and cost |
| Performance Evaluation matrix issues | False acceptance rate | Ability of the system to differentiate registered and unregistered user can be tested. | Improved biometric matching and identification rate | The fingerprint unique property | Not useful to identify performance of non-biometric factors. |
| | False Rejection Rate | Ability of Authentication system to identify registered user can be improved | Biometric Matching rate and registered user identification can be improved | Unique fingerprint feature should be used for registered user identification | Not useful to identify performance of non-biometric factors |
| | Equal Error Rate | Ability of Authentication system to identify rejection and acceptance rate can be easily studied | Biometric Matching rate , registered user, and un-registered user identification error can be improved | Unique fingerprint feature should be used for registered and unregistered user identification | Not useful to identify performance of non-biometric factors like password |
| | Failure to enrol rate | The capacity of the authentication system in identifying person when some specific features are missing can be studied easily | Biometric matching rate, enrol rate failure can be improved | Sophisticated feature enhancement techniques are essential | Not useful to identify performance of non-biometric factors |
| | Accuracy Rate | The overall matching performance and accuracy | Overall quality of matching can be | Sophisticated filtering, feature enhancement | Not useful to identify performance of non-biometric |

| | | | | | |
|---|---|---|---|---|---|
| | | can be easily studied | studied, analyzed, and improved | techniques are essential Good false rejection and acceptance rate are compulsory | factors |
| | Execution time | The rate of users get authenticated increases per unit time. | Trust and faith over system increases | Requires a good time and space complexity algorithm | Requirement of Good configuration system increases cost |

### 6.3. 1 Critical Constituent Elements as per ABCD Model

The important constituent factors of determinant issues are listed beneath the four constructs - advantages, benefits, constraints and disadvantages of the ABCD model and tabulated in Tables 6.2 to 6.5.

**Table 6.2:** Advantages of Multifactor Authentication Model for Verification purpose

| Sl. No | Issue | Factors affecting | Critical Constituent Elements |
|---|---|---|---|
| 1 | Security Issues | Mobile/Smart Phone | Structure of locking pattern |
| | | | Password strength |
| | | USB-pen Drive | Password strength of third-party software |
| | | | Usage of USB (Public/ Private) |
| | | Laptop | Password strength |
| | | Private cloud drive | Security strength of cloud drive |
| | | | Accessibility strength of image by programme/software |
| | | Non-reversible Hash code in network level | Strength of cryptographic programs/ Hash code in network level |
| | | Revocable Hash code | Ability or how fast the system having capacity to change password and finger-id when compromised |
| | | Non-reversible Hash code in network level | Strength of cryptographic programs/ Hash code in template level |
| 2 | User friendly issues | Increased rate of growth of authentication process | Conversion time required to convert fingerprint image to hash-id |
| | | | Time required for fetching password and decrypting |
| | | | Network speed for OTP |

| | | | |
|---|---|---|---|
| | | | Speed of Matching function |
| | | Increased Authentication request per unit time | Ability of concurrent authentication |
| | | | Efficiency of Hash code matching rate |
| | | Minimum prior information of the system required | The ability of the system to authenticate without prompting anything or with minimum input (only by selection or automatic) |
| | | Ubiquitous authentication in user friendly issue | The system used for authentication |
| | | | Availability of network |
| 3 | Input Issue | Minimum Knowledge parameters | The ability of the system to authenticate without prompting or without accepting more input from the user. (only password) |
| | | Simple User authentication from customer point of view | Number of Input |
| | | | Narration used in the interface |
| | | Reduced error in inputting | The way the input are provided to the system (Selection rather than entering) |
| | | Ubiquitous Authentication process in input | The device used for authentication process |
| | | | Availability of network |
| | | Consistency of the system | Reliability of the system |
| | | | The working efficiency of the system |
| | | Multipurpose parameter | The ability of the unique fingerprint features to make different actions in different instances |
| | | Increased number of requests | The execution time of the system |
| | | | Features or quality of input |
| | | User personal data protection | Security mechanisms used in authentication process |
| | | | Security used for protecting input |
| | | Increased growth rate in authentication due to input | The structure of the input |
| | | | Execution time of the algorithm used (time complexity) |
| 4 | Process Issues | Authentication process Rollback or Commit at the time of system failure | Strength of RDBMS |
| | | | RDBMS transaction atomicity property |
| | | Ensures consistent state at the time of system failure | Strength of RDBMS |
| | | | RDBMS transaction consistent property |
| | | Authentication process gets isolation property | Strength of RDBMS |
| | | Ubiquitous authentication in | RDBMS transaction atomicity |

| | | | |
|---|---|---|---|
| | | process issue | property |
| | | | The device used for authentication process |
| | | | Availability of network |
| | | User freely and easily interacts with authentication system | Simple user interface |
| | | | Navigational and narrative interface |
| | | Changed Password and Biometric-ID durable for long time | Management and maintenance of Database |
| | | | Safeguarding of database |
| 5 | Performance Evaluation matrix issues | Ability of the system to differentiate registered and the unregistered user can be tested. | The fingerprint image unique feature |
| | | | Quality of the fingerprint image |
| | | | False Acceptance Rate |
| | | Ability of Authentication system to identify registered user can be improved | The fingerprint image unique feature |
| | | | Quality of the fingerprint image |
| | | | False Rejection Rate |
| | | Ability of Authentication system to identify rejection and acceptance rate can be easily studied | The fingerprint image unique feature |
| | | | Quality of fingerprint image |
| | | | Difference of Acceptance and Rejection Rate |
| | | The capacity of the authentication system in identifying person when some specific features are missing can be studied easily | The fingerprint image unique feature |
| | | | Quality of the fingerprint image |
| | | | Ability of the system to convert hash code from partial fingerprint image |
| | | The overall matching performance and accuracy can be easily studied | The fingerprint image unique feature |
| | | Increased growth rate in authentication due to performance issue | Quality of the fingerprint image |
| | | | Rejection rate |
| | | | Acceptance rate |
| | | | The structure of the input |
| | | | Execution time of the algorithm used (time complexity) |

**Table 6.3:** Benefits of Multifactor Authentication Model for Verification purpose

| Sl. No | Issue | Factors affecting | Critical Constituent Elements |
|---|---|---|---|
| 1 | Security Issues | Increases demand for Cloud Drive, Mobile, Pen drive, and laptop | Usage of cloud drive for authentication process |
| | | | Usage of mobile phone for authentication process |

| | | | |
|---|---|---|---|
| | | | Usage of pen drive for authentication process |
| | | | Usage of Laptop for authentication process |
| | | Increased customer faith and attracts new customer | Security in all aspects of network |
| | | | Simple and easy way to input |
| | | | Time taken for authentication process |
| | | Efficient memory use, Database is easily manageable | One hash code for comparison and matching |
| | | | Cryptographically Encrypted Hash code |
| | | | Nonreversible Hash code |
| 2 | User-friendly issues | Increased customer pool | Quality of multifactor authentication model |
| | | | Response time |
| | | | Simple method of inputting |
| | | | Speed of authentication process |
| | | Reduced Queuing and Reduced waiting process | Good access time |
| | | | Simple method of inputting |
| | | | Speed of authentication process |
| | | Increased customer satisfaction, retention and acquiring new customers becomes easy | Good Access time |
| | | | Good Response time |
| | | | Simple method of inputting |
| | | | Speed of authentication process |
| | | Increased customer satisfaction, | Automatic process |
| | | | Good Access time |
| | | | Good Response time |
| | | | Simple method of inputting |
| | | | Speed of authentication process |
| 3 | Input Issue | Ubiquitous authentication with minimum possesition of data | The device used for authentication process |
| | | | Availability of network |
| | | Reduced I/O operation | Minimum number of input |
| | | | Quality of input |
| | | Increased Customer comfort and satisfaction | Automatic process |
| | | | Selection input method |
| | | | Good Response time |
| | | | Simple method of inputting |
| | | | Speed of authentication process |
| | | Reduced parameter requirement for authentication | Multipurpose usability of single input |
| | | | Type of input |
| | | Accurate results, error-free output | Reliability of the system |
| | | | Efficiency of the input |
| | | | Quality of input |

| | | | |
|---|---|---|---|
| | | Trust and faith over system increases | Increased security |
| | | | Increased execution time |
| | | | Reliability of the system |
| | | | Efficiency of the input |
| | | | Type and quality of input |
| | | | Security used for protecting input |
| 4 | Process Issues | Authentication failure is very rare or practically zero. | Strength of RDBMS |
| | | | RDBMS transaction atomicity property |
| | | | Ability of the system to handle crashes or failures |
| | | Ensures a safe state at the time of system failure | Strength of RDBMS |
| | | | RDBMS transaction consistent property |
| | | | Ability of the system to handle crashes or failures |
| | | Enhanced user trust and satisfaction | Strength of RDBMS |
| | | | RDBMS transaction atomicity property |
| | | | Protected and private authentication process |
| | | | Isolation transaction property of DBMS |
| | | Reduced request queue | Availability of authentication system |
| | | | Availability of network |
| | | | Speed of authentication |
| | | Increased user trust, happiness, and satisfaction | Simple user interface |
| | | | Navigational and narrative interface |
| | | | Speed of authentication |
| | | | Effort free input and process |
| | | Revocability can be done easily if password or Finger-id is compromised | Fast fingerprint-id change option |
| | | | Fast password change option |
| | | | Hash code representation of fingerprint features and password |
| 5 | Performance Evaluation matrix issues | Improved biometric matching and identification rate | The fingerprint image unique feature |
| | | | Quality of the fingerprint image |
| | | | Ideal false acceptance rate or simply zero. |
| | | Biometric Matching rate and registered user identification can be improved | The fingerprint image unique feature |
| | | | Quality of the fingerprint image |
| | | | Ideal False Rejection Rate or simply zero |
| | | Biometric Matching rate, | The fingerprint image unique |

| | | | |
|---|---|---|---|
| | | registered user, and un-registered user identification error can be improved. | feature |
| | | | Quality of fingerprint image |
| | | | Ideal Difference between Acceptance and Rejection Rate |
| | | Biometric matching rate, enroll rate failure can be improved | The fingerprint image unique feature |
| | | | Quality of the fingerprint image |
| | | | The capacity of the system to generate Hash code when partial minutiae details are present in fingerprint image. |
| | | Overall quality of matching can be studied, analyzed, and improved | The fingerprint image unique feature |
| | | | Quality of the fingerprint image |
| | | | Rejection rate |
| | | | Acceptance rate |
| | | Trust and faith over system increases | The structure of the input |
| | | | Execution time of the algorithm used (time complexity) |
| | | | Over performance of the system |

**Table 6.4:** Constraints of Multifactor Authentication Model for Verification purpose

| Sr. No | Issue | Factors affecting | Critical Constituent Elements |
|---|---|---|---|
| 1 | Security Issues | High Security of the Cloud Drive, USB device, Laptop and Mobile Phone is questionable | Security architecture used in Cloud Drive |
| | | | Third party software security architecture used in USB devices |
| | | | Password strength used in Laptop login process |
| | | | Mobile phone pattern lock rigid structure and strength of password |
| | | Good network architecture | Connectivity and security |
| | | | Redundancy |
| | | | Standardisation |
| | | | Disaster recovery |
| | | | Growth |
| | | Cryptographically Hash representation of fingerprint image | The fingerprint feature used for Hash code generation |
| | | | The strength of Hash code. |
| | | | The rate of difficulty for decrypting Hash code. |
| 2 | User-friendly issues | Requires high configuration system and efficient algorithms | RAM size |
| | | | OS and its architecture (32bit 0r 64-bit) |

| | | | |
|---|---|---|---|
| | | | Processor used |
| | | | Single processor/ Multiprocessor |
| | | | Clock speed |
| | | | Time and space complexity of algorithms used. |
| | | Ability to make difference between registered and unregistered user and Processing power | The features used for identification purpose |
| | | | RAM size |
| | | | Processor used, Clock speed |
| | | | Single processor/ Multiprocessor |
| | | | Time and space complexity of algorithms used. |
| | | Dedicated server and network in User-friendly issue | All the features of server required for efficiency |
| | | | All the features of network required for efficiency |
| 3 | Input Issue | Capacity of the system to differentiate between registered user and intruder with minimum data | The quality of input |
| | | | The features used for identification |
| | | | All the features of high end configuration system |
| | | Requirement of unique and robust parameter for user Authentication | The quality of input |
| | | | The features used for identification |
| | | | The salting process used in Hash generation |
| | | User ability to identify correct image | The input selected through selection |
| | | | Understandability level of the User |
| | | Operating cost | Cost of the high-end processor |
| | | | Cost of the Authentication system |
| | | The ability of the software to make distinction between different context of the same parameter | The feature selected for multipurpose |
| | | | The strength of software |
| | | | Quality of input |
| | | Quality of the input | Number of minutiae details in fingerprint image |
| | | | The correctness of the OTP |
| | | | Right password |
| | | Uniqueness, permanence, Universality, and revocability | The features used for generating Hash code |
| | | | The database quality to achieve all template protection characteristics |
| 4 | Process Issues | Need of good fault tolerance | Strength of RDBMS |

| | | | |
|---|---|---|---|
| | | techniques. | RDBMS transaction's atomicity, consistency, and isolation property |
| | | | The fault tolerance technique used in RDBMS. |
| | | | The strength of lock-based concurrency control used in RDBMS |
| | | Dedicated server and network | All the features of server required for efficiency |
| | | | All the features of network required for efficiency |
| | | Requires navigational and narrative user interface Input should be selective rather than entering | Te explanation displayed in user interface |
| | | | Navigational control used in interface |
| | | | Input type (selection rather than entering) |
| 5 | Performance Evaluation matrix issues | The fingerprint unique property used for identification/Matching | Features used to generate Hash code. |
| | | | Quality of Hash code |
| | | | The stored Hash code in Database |
| | | Requires good time and space complexity algorithm | The algorithm used for Hash code |
| | | | Memory utilized by the algorithm |
| | | | Configuration of the system used for authentication |

**Table 6.5:** Disadvantages of Multifactor Authentication Model for Verification purpose

| Sl. No | Issue | Factors affecting | Critical Constituent Elements |
|---|---|---|---|
| 1 | Security Issues | User-level security acceptance by the user | Security architecture used in Cloud Drive, UDB drive, Laptop, and mobile. |
| | | | Inconvenience in handling these drives |
| | | | Security aspect is questionable in third party software |
| | | Network failure | Single point of failure in hardware |
| | | | Power problems or issues |
| | | | Routing problems |
| | | | Human error |
| | | Tampering of data | Un-authorized access to data |
| | | | Network failure |

| | | | |
|---|---|---|---|
| | | Database failure or server failure | Hardware failure |
| | | | File corruption |
| | | | File system damage |
| 2 | User-friendly issues | Hardware and software cost | Cost of RAM |
| | | | Cost of Processor |
| | | | Cost of the computer system |
| | | | OS cost |
| | | | Authentication system cost |
| | | Network cost | Bandwidth cost |
| | | | Data cost |
| | | High utilization of hardware and software | High utilization of memory and processor |
| | | | Space and time complexity |
| | | Complex backend design of interface | To design simple user interface for user |
| | | 24 × 7 services | High utilization of processor, and memory |
| | | | More power consumption |
| 3 | Input Issue | Lack of information | Only fingerprint image are selected |
| | | | User personal details are not taken by the system. |
| | | Negligence of the user in selection of input | Lack of concentration of the user |
| | | Misuse of authentication system / More intruder will try to break the system | Continuous availability of the system. |
| | | Significant startup and Maintenance cost | Cost of the high end processor |
| | | | Cost of the Authentication system |
| | | Intruder or un-registered user tries to get multipurpose parameter | Continuous availability of the system. |
| | | | Usability of the parameter |
| | | Inability to handle error-prone or partial input | Minutiae details are fully missing |
| 4 | Process Issues | Requires separate programme for database protection/safeguards | Management of the database |
| | | | Essentiality of the Database protection |
| | | Requires lock-based concurrency control system | For acquiring isolation property of the database transaction |
| | | Continuous availability of the server increases cost | Requirement of Ubiquitous availability of the server |
| | | | Requirement of efficiency of the system |
| | | Complex design of user interface and programme increases cost | Requirement of effort free authentication process |

| | | | |
|---|---|---|---|
| 5 | Performance Evaluation matrix issues | Acceptance rate, Rejection rate , Equal error rate, failure to enrol rate, accuracy only used for biometric performance evaluation | Performance evaluation matrices of biometric data |

## 6.4 COMPARISON OF NEW MULTIFACTOR AUTHENTICATION MODEL WITH EXISTING SYSTEMS

Here we compare Multifactor Authentication Model based on Fingerprint Hash code, OTP, and Password with different existing systems of the same kind of slightly different systems or any system which makes use of biometric or password or username or OTP for authentication (Krishna Prasad K., & Aithal P. S., 2018g). The different system considered in this study are the traditional user-d, password-based internet/mobile banking system, Apple iPhone X face recognition system, HDFC OTP Checkout for online transactions, and Indian Aadhaar card registration process. These comparisons help to understand where this model stands in terms of its features compare to the existing systems. The new model is compared with all the existing models under four constructs as Advantages, Benefits, Constraints, and Disadvantages. Table 6.6, Table 6.7, Table 6.8, and Table 6.9 shows Advantages, Benefits, Constraints, and disadvantages comparative study of new Multifactor Authentication Model with traditional username and password based Internet/Mobile Banking System respectively.

**Table 6.6:** Advantages comparative study of new Multifactor Authentication Model v/s traditional user-id and password based Internet/Mobile Banking System.

| Sr. No | New Multifactor Authentication Model | Traditional user-id and password based Internet/Mobile Banking System |
|---|---|---|
| 1 | The Nonreversible Fingerprint Hash code is used in network level | Highly secured encrypted user-id and password are used in network level |
| 2 | Fingerprint Hash-id is used for identification purpose which is in Hash or encrypted form | User-id is used for identification purpose which is in Hash or encrypted form |
| 3 | Easily revocable Fingerprint Hash-id and password which is in Hash or encrypted form | Easily revocable user-id and password which is in Hash or encrypted form |
| 4 | High template protection is ensured | High user-id and password protection is ensured in database level |
| 5 | The system having the ability to authenticate with one knowledgebase input (Hash-id by selection, OTP is entered by viewing and Password by knowledge base entry) | The system having ability to authenticate with two knowledgebase input (user-id by selection, OTP is entered by viewing and Password by knowledge base entry) |

| | | |
|---|---|---|
| 6 | Depending on the device and network Provides ubiquitous authentication | Depending on the device and network Provides ubiquitous authentication |
| 7 | Interactive and explorative user interface | Interactive and explorative user interface |
| 8 | One knowledge base parameter input | Two knowledge base parameter inputs |
| 9 | Simple User authentication from customer point of view | Simple User authentication from customer point of view but user-id also remembered along with password |
| 10 | Reduced error in inputting due to one selection type input. | Input error little more due to lack of selection input. |
| 11 | Due to Hash code user, personal data or input are secured. | Due to encrypted data user personal data or input are secured. |
| 12 | Due to RDBMS transaction property atomicity, consistency, and isolation properties are ensured. | Due to RDBMS transaction property atomicity, consistency, and isolation properties are ensured. |
| 13 | Changed Password and Biometric-id durable for a long time. | Changed Password and User-id durable for a long time. |
| 14 | All the fingerprint performance evaluation matrices like False Acceptance Rate, False Rejection Rate, Equal Error Rate, Failure to Enroll Rate, and Accuracy Rate gives good accuracy or matching rate. | User-id and Password give highest accuracy rate. |
| 15 | A Lifespan or validity of OTP is very less, say 2 minutes. | OTP used for financial transaction having more validity. |

**Table 6.7:** Benefits comparative study of new Multifactor Authentication Model v/s traditional user-id and password based Internet/Mobile Banking System.

| Sr. No | New Multifactor Authentication Model | Traditional user-id and password based Internet/Mobile Banking System |
|---|---|---|
| 1 | Security in all aspects of network and template, Simple and easy way to input, reduced execution time can become influence parameters for Increased customer faith and also can attract new customers. | Security in all aspects of network and database and reduced execution time increased customer faith and also attracted new customers. But due to password attacks, users require advanced way of authentication like biometrics. |
| 2 | Cryptographically encrypted one hash code and password only stored in the database, which makes database memory utilization very less and efficient. | Cryptographically encrypted user-id and password only stored in database, which makes database memory utilization very less and efficient. |
| 3 | Both fingerprint-id and passwords are protected by OTP means OTP is first entry type input. | OTP is used only for financial transactions. |
| 4 | Ubiquitous authentication with one knowledge base input. | Ubiquitous authentication with two knowledge base inputs. |
| 5 | Authentication failure is very rare or practically zero compare to any other biometrics-based authentication. | An authentication failure occurs when user-id, password or both becomes wrong. |

| | | |
|---|---|---|
| 6 | Revocability can be done easily if password or Finger-id is compromised. In most of the fingerprint-based authentication system, revocability of fingerprint is not so easy. | Revocability is done easily if the password is compromised. |
| 7 | Due to RDBMS transaction property, at the time of system failure. | Due to RDBMS transaction property, ensures a safe state at the time of system failure. |
| 8 | The simple, Navigational, and explorative user interface, the speed of authentication, and Effort free input and process can have chances to enhance user trust, happiness, and satisfaction. | The simple, Navigational, and explorative user interface, the speed of authentication, and Effort free input already enhanced user trust, happiness, and satisfaction. But the user needs still more security for their data and transactions. |

**Table 6.8:** Constraints comparative study of new Multifactor Authentication Model v/s traditional user-id and password based Internet/Mobile Banking System.

| Sr. No | New Multifactor Authentication Model | Traditional user-id and password based Internet/Mobile Banking System |
|---|---|---|
| 1 | Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working. | Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working. |
| 2 | Good RDBMS management and disaster recovery techniques are essential. | Good RDBMS management and disaster recovery techniques are essential. |
| 3 | Requires high configuration system and efficient algorithms for fingerprint Hash code creation and for encryption. | Requires high configuration system and efficient algorithms for user-id and password encryption. |
| 4 | Requires navigational and explorative user interface. | Requires navigational and explorative user interface, and Input should be selective rather than entry type. |
| 5 | While selecting fingerprint features for Hash code, unique features should be selected for collision-free Hash code and for effective user identification. | Unique user-id is selected for collusion free user-id and for effective user identification. |

**Table 6.9:** Disadvantages comparative study of new Multifactor Authentication Model v/s traditional user-id and password based Internet/Mobile Banking System.

| Sr. No | New Multifactor Authentication Model | Traditional user-id and password based Internet/Mobile Banking System |
|---|---|---|
| 1 | Network cost for OTP | Network cost for OTP in financial transactions. |
| 2 | Network and server Failures will shut down the Authentication process | Network and server Failures will shut down the Authentication process |
| 3 | Complex backend design of user interface | Complex backend design of user interface |
| 4 | The Negligence of the user in selection of | The negligence of the user in entering the |

| | | |
|---|---|---|
| | input and Lack of concentration of the user increases the non-matching rate in authentication process. | input and Lack of concentration of the user increases the non-matching rate in the authentication process. |
| 5 | Requirement of continuous availability of the server increases cost | Requirement of continuous availability of the server increases cost |

Table 6.10, Table 6.11, Table 6.12, and Table 6.13 shows Advantages, Benefits, Constraints, and disadvantages comparative study of new Multifactor Authentication Model with Apple iPhone X facial recognition system. Here the comparison is not more useful because of the Apple iPhone X facial recognition used for mobile locking and not for secured transaction or authentication.

**Table 6.10:** Advantages comparative study of new Multifactor Authentication Model v/s Apple iPhone X facial Recognition System

| Sr. No | New Multifactor Authentication Model | Apple iPhone X Facial Recognition System |
|---|---|---|
| 1 | Nonreversible Fingerprint Hash code is used in network level | Face recognition image are stored on the mobile phone. Authentication is done locally. |
| 2 | Fingerprint Hash code alone is not used for the purpose of authentication. Authentication is done with the aid of Fingerprint Hash code, OTP, and Password. | Face of the user image alone is used for authentication/recognition purpose. |
| 3 | Hashed fingerprint gives more security | The unhashed Face image is an easy target for Hackers. |
| 4 | Multiple inputs are necessary for authentication or matching, which includes Fingerprint Hash code, OTP, and Password | Only face image of the user is needed for Authentication/Matching/Verification purpose. |
| 5 | At least one knowledge base input is required (password) | None of the Knowledgebase input is used for Authentication/Matching/Verification purpose. |
| 6 | The system is not easily mimicable | The system is easily mimicable. |

**Table 6.11:** Benefits comparative study of new Multifactor Authentication Model v/s Apple iPhone X facial Recognition System

| Sr. No | New Multifactor Authentication Model | Apple iPhone X facial recognition system |
|---|---|---|
| 1 | Security in all aspects of network and template, Simple and easy way to input, reduced execution time can become influence parameters for Increased customer faith and also can attract new customers | Not implemented in large scale due to security failure in its infant stage only. |

| | | |
|---|---|---|
| 2 | Cryptographically encrypted one hash code and password only stored in the database, which makes database memory utilization very less and efficient. | Not used in Client-Server architecture. |
| 3 | Both fingerprint-id and passwords are protected by OTP means OTP is first entry type input. | OTP is not used for verification or matching process. |
| 4 | Ubiquitous authentication with one knowledge base input. | Ubiquitous matching with no knowledge base inputs. |
| 5 | Authentication failure is very rare or practically zero compare to any other biometrics-based authentication. | Authentication/matching failure occurs when face image is hacked by the intruder |

**Table 6.12:** Constraints comparative study of new Multifactor Authentication Model v/s Apple iPhone X facial Recognition System

| Sr. No | New Multifactor Authentication Model | Apple iPhone X facial Recognition System |
|---|---|---|
| 1 | Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working. | Not used in network, used in local system |
| 2 | Good RDBMS management and disaster recovery techniques are essential. | Not used in client-server architecture |
| 3 | Requires high configuration system and efficient algorithms for fingerprint Hash code creation and for encryption. | Requires high configuration system and efficient algorithms for processing of facial features from face image |
| 4 | Requires navigational and explorative user interface. | Not having much scope for interface because no entry type input required. Input is captured through a mobile camera. |
| 5 | Provides good security architecture through multifactor authentication model. | Good security architecture is essential |

**Table 6.13:** disadvantages comparative study of new Multifactor Authentication Model v/s Apple iPhone X facial Recognition System

| .Sr. No | New Multifactor Authentication Model | Apple iPhone X facial Recognition System |
|---|---|---|
| 1 | Network cost for OTP | Not suitable for network feature comparison. |
| 2 | Network and server Failures will shut down the Authentication process | The client-server architecture is not implemented. |
| 3 | Complex backend design of the user interfaces, user interface having not much scope due to lack of manual input. | user interface having not much scope due to lack of manual input. |
| 4 | Negligence of the user in selection of input and Lack of concentration of the user increases the non-matching rate in the authentication process. | Negligence of the user in storing face image in unsecured places causes security failure. |

Table 6.14, Table 6.15, Table 6.16, and Table 6.17 shows Advantages, Benefits, Constraints, and disadvantages comparative study of new Multifactor Authentication Model with HDFC OTP Checkout for online transactions.

**Table 6.14:** Advantages comparative study of new Multifactor Authentication Model v/s HDFC OTP Checkout for online transactions

| Sr. No | New Multifactor Authentication Model | HDFC OTP Checkout for online transactions |
|---|---|---|
| 1 | Nonreversible Fingerprint Hash code is used in network level. | Highly secured encrypted OTP is used in network level |
| 2 | The system having the ability to authenticate with one knowledgebase input (Hash-id by selection, OTP is entered by viewing and Password by knowledge base entry) | The system having the ability to authenticate without knowledgebase input. |
| 3 | Depending on the device and network Provides ubiquitous authentication | Depending on the device and network Provides ubiquitous authentication |
| 4 | Interactive and explorative user interface | Interactive and explorative user interface |
| 5 | One knowledge base parameter input | No knowledge base parameter inputs |
| 6 | Simple User authentication from customer point of view | Simple User authentication from customer point of view |
| 7 | Reduced error in inputting due to one selection type input. | More Reduced error in inputting due to lack of selection or entry types input. |
| 8 | Due to Hash code user, personal data or input are secured. | Due to encrypted data user personal data or input are secured. |
| 9 | Lifespan or validity of OTP is very less, say 2 minutes. | OTP used for financial transaction having less validity. |

**Table 6.15:** Benefits comparative study of new Multifactor Authentication Model v/s HDFC OTP Checkout for online transactions

| Sr. No | New Multifactor Authentication Model | HDFC OTP Checkout for online transactions |
|---|---|---|
| 1 | Security in all aspects of network and template, Simple and easy way to input, reduced execution time can become influence parameters for Increased customer faith and also can attract new customers | Security in all aspects of network and database and reduced execution time increased customer faith and also attracted new customers. When the mobile phone is stolen users requires advanced way of authentication like biometrics. |
| 2 | Cryptographically encrypted one hash code and password only stored in the database, which makes database memory utilization very less and efficient. | Cryptographically encrypted user-id and password only stored in the database, which makes database memory utilization very less and efficient. |

| | | |
|---|---|---|
| 3 | Both fingerprint-id and passwords are protected by OTP means OTP is first entry type input. | Only OTP is used for authentication/transaction purpose. |
| 4 | Ubiquitous authentication with one knowledge base input. | Ubiquitous authentication with OTP |
| 5 | Authentication failure is very rare or practically zero compare to any other biometrics-based authentication | An authentication failure occurs when OTP is wrong, which very rare or uncommon. |
| 6 | The simple, Navigational, and explorative user interface, the speed of authentication, and Effort free input and process can have chances to enhance user trust, happiness, and satisfaction. | The simple, Navigational, and explorative user interface, the speed of authentication, and lack of manual input already enhanced user trust, happiness, and satisfaction. But the user needs still more security for their data and transactions. |

**Table 6.16:** Constraints comparative study of new Multifactor Authentication Model v/s HDFC OTP Checkout for online transactions

| Sr. No | New Multifactor Authentication Model | HDFC OTP Checkout for Online Transactions |
|---|---|---|
| 1 | Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working. | Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working. |
| 2 | Good RDBMS management and disaster recovery techniques are essential. | Good RDBMS management and disaster recovery techniques are essential. |
| 3 | Requires high configuration system and efficient algorithms for fingerprint Hash code creation and for encryption. | Requires high configuration system and efficient algorithms for OTP encryption. |
| 4 | Requires navigational and explorative user interface. | Requires simple interface due to lack of knowledgebase input. |
| 5 | While selecting fingerprint features for Hash code, unique features should be selected for collision-free Hash code and for effective user identification. | Unique user-id is selected for collision-free user-id and for effective user identification but verification is done only through OTP. |

**Table 6.17:** Disadvantages comparative study of new Multifactor Authentication Model v/s HDFC OTP Checkout for online transactions

| Sr. No | New Multifactor Authentication Model | HDFC OTP Checkout for Online Transactions |
|---|---|---|
| 1 | Network cost for OTP | Network cost for OTP |
| 2 | Network and server Failures will shut down the Authentication process | Network and server Failures will shut down the Authentication process |
| 3 | Complex backend design of user interface | Simple backend design of user interface |
| 4 | Negligence of the user in selection of input and Lack of concentration of the user | No manual input, which reduces error in input. |

| | | |
|---|---|---|
| | increases the non-matching rate in the authentication process. | |
| 5 | Requirement of continuous availability of the server increases cost | Requirement of continuous availability of the server increases cost |

Table 6.18, Table 6.19, Table 6.20, and Table 6.21 shows Advantages, Benefits, Constraints, and disadvantages comparative study of new Multifactor Authentication Model with Indian Aadhaar card registration process.

**Table 6.18:** Advantages comparative study of new Multifactor Authentication Model v/s Indian Aadhaar card registration process

| Sr. No | New Multifactor Authentication Model | Indian Aadhaar card registration process |
|---|---|---|
| 1 | Nonreversible Fingerprint Hash code is used in network level | Highly secured encrypted OTP is used in network level |
| 2 | The system having the ability to authenticate without knowledgebase input (Hash-id by selection, OTP is entered by viewing and Password by knowledge base entry) | The system having ability to authenticate without knowledgebase input. |
| 4 | Interactive and explorative user interface | Interactive and explorative user interface |
| 5 | One knowledge base parameter input | No knowledge base parameter inputs |
| 6 | Simple User authentication from customer point of view | Simple User authentication from customer point of view |
| 7 | Reduced error in inputting due to one selection type input. | More Reduced error in inputting due to lack of selection or entry types input. |
| 8 | Due to Hash code user, personal data or input are secured. | Due to encrypted data user personal data or input are secured. |
| 9 | Lifespan or validity of OTP is very less, say 2 minutes. | OTP used for financial transaction having little bit more validity. |
| 10 | Fingerprint thumb capturing will not fail frequently for kids. | Registration process involving fingerprint thumb image captures requires many attempts for kids. |

**Table 6.19:** Benefits comparative study of new Multifactor Authentication Model v/s Indian Aadhaar card registration process

| Sr. No | New Multifactor Authentication Model | Indian Aadhaar card registration process |
|---|---|---|
| 1 | Security in all aspects of network and template, Simple and easy way to input, reduced execution time can become influence parameters for Increased customer faith and also can attract new customers | Not having scope for authentication. Its one-time registration for a single user. |

| | | |
|---|---|---|
| 2 | Cryptographically encrypted one hash code and password only stored in the database, which makes database memory utilization very less and efficient. | Cryptographically encrypted user-id and biometric only stored in the database, which makes database memory utilization more but efficient.. |
| 3 | Both fingerprint-id and passwords are protected by OTP means OTP is first entry type input. | Both fingerprint template and OTP makes authentication/transaction process. |
| 5 | Authentication failure is very rare or practically zero compare to any other biometrics-based authentication. | An authentication failure occurs when thumb minutiae details vary with a dry finger or cold weather, or finger damage or cut. |
| 6 | The simple, Navigational, and explorative user interface, the speed of authentication, and Effort free input and process can have chances to enhance user trust, happiness, and satisfaction. | Simple, Navigational, and explorative user interface, speed registration process, and lack of manual input already enhanced user trust, happiness, and satisfaction. |

**Table 6.20:** Constraints comparative study of new Multifactor Authentication Model v/s Indian Aadhaar card registration process

| Sr. No | New Multifactor Authentication Model | Indian Aadhaar card registration process |
|---|---|---|
| 1 | Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working. | Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working. |
| 2 | Good RDBMS management and disaster recovery techniques are essential. | Good RDBMS management and disaster recovery techniques are essential. |
| 3 | Requires high configuration system and efficient algorithms for fingerprint Hash code creation and for encryption. | Requires high configuration system and efficient algorithms for OTP encryption. |
| 4 | Requires navigational and explorative user interface. | Requires simple interface due to lack of knowledgebase input. |
| 5 | While selecting fingerprint features for Hash code, unique features should be selected for collision-free Hash code and for effective user identification. | Unique user-id is selected for collision-free user-id and for effective user identification but verification is done only through OTP. |

**Table 6.21:** Disadvantages comparative study of new Multifactor Authentication Model v/s Indian Aadhaar card registration process

| Sr. No | New Multifactor Authentication Model | Indian Aadhaar card registration process |
|---|---|---|
| 1 | Network cost for OTP | Network cost for OTP |
| 2 | Network and server Failures will shut down the Authentication process | Network and server Failures will shut down the registration process |

| | | |
|---|---|---|
| 3 | Complex backend design of user interface | Complex backend design of user interface |
| 4 | Negligence of the user in selection of input and Lack of concentration of the user increases the non-matching rate in the authentication process. | No manual entry type input, which reduces error in input. |
| 5 | Requirement of continuous availability of the server increases cost | Requirement of continuous availability of the server increases cost |
| 6 | The quality of the fingerprint capturing or sensing technology does not affect the system | The quality of the fingerprint capturing or sensing technology affects the system |

## 6.5 CHAPTER SUMMARY

We have studied the Multifactor Authentication Model based on Fingerprint Hash Code, Password, and OTP using ABCD analysis framework. As per ABCD analysis various determinant issues related to Multifactor Authentication Model for Verification/Authentication purpose are: (1) Security issues, (2) User-friendly issues, (3) Input issues, (4) Process issues, and (5) Performance Evaluation matrix issues. The analysis identified the affecting factors for various determinant issues under four constructs advantages, benefits, constraints, and disadvantages. The analysis shows that new model gives good security at network and database level. The Hash code is no reversible and also minimum numbers of input are used for the authentication process.

We have compared Fingerprint Hash code, OTP and Password-based Authentication Model with existing systems, which includes, the traditional user-id, password-based internet/mobile banking system, Apple iPhone X face recognition system, HDFC OTP Checkout for online transactions and Indian Aadhaar card registration process. Some of the important findings of the comparative study are mentioned below.

- One time captured static fingerprint image are not vulnerable to climate or weather condition changes compared to any other biometric-based authentication system like Indian Aadhaar Card registration process.
- The new multifactor Authentication model requires less knowledgebase input compared to traditional user-id and password based Internet/Mobile banking authentication. If the user takes care and ensures user-level security through external devices like USB drive or Private cloud drive, we can eliminate password factor from authentication process.

**********

# CHAPTER SEVEN

# *SUMMARY, CONCLUSION, LIMITATIONS AND FUTURE SCOPE*

**Contents** **Page No.**

## 7.1 INTRODUCTION

By definition, Authentication is using one or multiple mechanisms to show that you are who you claim to be. As soon as the identity of the human or machine is demonstrated, then human or machine is authorized to grant some services. The modern research study reveals that fingerprint is not so secured like secured a password which consists of alphanumeric characters, number and special characters. Fingerprints are left at crime places, on materials or at the door which is usually class of latent fingerprints. We cannot keep fingerprint as secure like rigid passwords. Using some modern technology with copper and graphite spray it's easy to mimic fingerprint image. Fingerprints are not fully secured if passwords are leaked or hacked, it easily revocable using another password. But in a biometric security system, which uses only biometric features, is not easy to change fingerprint key or fingerprint are static biometric, which never change much throughout the lifespan. Fingerprints are left at car, door or anyplace where every person goes and places his finger. Fingerprint Hash code is not used for full security or authentication purpose but it can be combined with other security elements like password or OTP in order to enhance security.

In this chapter, we discuss a summary of the research work of all six Hash code generation methods, Multifactor Authentication Model based on Fingerprint Hash code, OTP, and Password. We also list out the findings of this study. The future research directions are also discussed.

## 7.2 SUMMARY OF HASH CODE GENERATION METHODS

Biometrics is an intrinsic bodily or behavioral characteristic that may be used to discover or verify the person. The most common types of biometrics are face, speech, iris, fingerprint, gait, and signature. The fingerprint is very not unusual and popular biometric of type traits due to its universality, distinctiveness, and permanence and additionally, many advances and new researchers are to be had in this discipline. Despite the fact that AFIS is capable of recognizing a fingerprint image sample with already saved fingerprint image within the database, nevertheless, partial or latent fingerprint image suffers from the low-overall performance rate.

Fingerprint identification technology era has various blessings for much less price and non-invasive manner of acquisition and therefore is one of the maximum frequently used mechanisms. In this research work fingerprint’s high individualism and permanent nature

motivated us to choose this biometric feature as identity key, which is half secured and can be made fully secured by combining with passwords or OTP.

But the modern study reveals that fingerprint is not so secured like secured passwords which consist of alphanumeric characters, number and special characters. Fingerprints are left at crime places, on materials or at a door which is usually class of latent fingerprints. We cannot keep fingerprint as secure like rigid passwords. Using some modern technology with copper and graphite spray it's easy to mimic fingerprint image. Fingerprints are not fully secret if passwords are leaked or hacked, it easily revocable using another password. But in a biometric security system, which uses only biometric features, is not easy to change fingerprint key or fingerprint are static biometric, which never change much throughout the lifespan.

In this research work we use a fingerprint as identity or index key, even if the intruder gets that image, an intruder cannot get access rights or authorization to use the secured system, if it is implemented for some applications or services like online banking.

This research work shows mainly four characteristics which are unique to every fingerprint. This is true for even different fingerprints of same persons. The four features are mentioned below;

- Total number of Ridge ending and Ridge bifurcation (Minutiae details)
- Gabor filter frequencies and angular value will be unique for segmented image of the fingerprint (Feature extraction from segmented image using Gabor filtering)
- Freeman chain code sum of, first difference value, boundary starting x (x0) and y (y0) value and, chain code value for a binary fingerprint image
- Euclidean distance value from each pixel to nearest neighbour pixel with pixel value one for a binary fingerprint image (Euclidean distance matrix for binary fingerprint image).

In this research work, we have proposed six Methods of fingerprint Hash Code generation. All the methods use different techniques in order to form unique Hash code for each fingerprint image. Method-1 is based on fingerprint ridge bifurcation and ridge ending minutiae Feature extractions from the post processed Skeleton image of fingerprint with location details. In Method-2 Fingerprint minutiae features are extracted through Gabor filtering from the segmented image from the non-Skeletonised fingerprint image. Method- 3 is almost similar to Method-2, with one exception, which is without using contrast adjustment filtering algorithm. Method-4 is similar to Method-1 but without considering ridge

bifurcation and ridge ending location details. Method-5 is based on fingerprint feature extraction with the help of freeman chain coding from binary Fingerprint image. Method-6 is based on fingerprint feature extraction with the aid of freeman chain coding from binary Fingerprint image. All these six methods of Fingerprint Hash code generation generally having some Advantages, Benefits, Constraints, and Disadvantages, which are listed below.

*Advantages*

- Hash codes are noninvertible
- Hashcode takes very small amount of memory
- Hash code Hides original information of fingerprint image from the intruder
- All the six methods discussed in this study utilizes only one code for each fingerprint
- It is unique for each fingerprint of the same person means ten fingerprints will be having ten different Hash codes.

*Benefits*

- Hash code is used as identity-key or index-key to uniquely identify a person.
- Easily we can append salting in order to make the Hash code more robust.
- Fingerprint Hash code is a transformed function, which does not reveal original minutiae details.
- Fingerprint Hash code consumes very less time for training phase.
- Unlike another fingerprint matching, all the six methods discussed in this study do not use scoring level. It uses only binary value either matching or not matching.

*Constraints*

- Small changes in fingerprint hash code make large differences.
- All the six methods used in this study are translation and rotation variant..

*Disadvantages*

- Fingerprint hash code cannot be solely used for security or authentication purpose.
- If fingerprint image of same finger input is taken through any type of solid and robust sensors in consecutive two intervals, still fingerprint hash code generates different hash code.
- Even though developed fingerprint Hash code is invariant to translation and rotation, if the user presses hardly into one reader or sensor, or swipe the finger in a different orientation, or a cut in the finger, for a successive two capture, produces different Hash code.

## 7.3 SUMMARY OF MULTIFACTOR AUTHENTICATION MODEL

Multifactor Authentication Model using fingerprint Hash the code, Password, and OTP improve security in client-server-based applications. Multifactor Authentication Model can be effectively implemented in Internet banking and Mobile banking. This model does not require any fingerprint sensor device to capture user fingerprints. It uses a static image of the fingerprint. The Multifactor Authentication Model based on fingerprint Hash code, Password and OTP generally having some Advantages, Benefits, Constraints, and Disadvantages, which are listed below.

*Advantages*

- Fingerprint Hash code used in Multifactor Authentication model acts as identity-key or index-key to uniquely identify individual persons.
- Fingerprint Hash code, combined with Password and OTP makes authentication process robust or highly secure.
- The fingerprint image is hashed through the double folded layer and salted enough.
- The modern study reveals that fingerprint images are not secret, not revocable but in this model, because fingerprint Hash code is used as index-key, securing of the fingerprint image is not essential.
- Changes in finger depending on weather condition or a cut or wound in finger does not affect the system performance in this model.
- Security details database table consist of only two fields as Fingerprint Hash-id and double folded encrypted password.
- The user Registered Mobile number is stored separately in another table. Fingerprint hash-id can be used to identify the user mobile number stored in the registration table.

*Benefits*

- Multifactor Authentication Model can be effectively implemented in Internet banking and Mobile banking.
- This model does not require any fingerprint sensor device to capture user fingerprints. It uses a static image of the fingerprint.
- Cost and memory utilization is less compared to similar biometric fingerprint recognition systems

- Multifactor authentication model is effectively implemented in smart phones compared to any other platforms because smartphone already will be having one level of security through pattern lock or using password lock.
- In the worst case, if an intruder gets fingerprint image, it just acts as an identifier and not as security information. So intruder cannot break the system only with the fingerprint image.
- Even though fingerprint image cannot use solely in the authentication process, it can be protected in systems like laptop or desktop computer using login password.
- No need of remembering the User-id and Fingerprint Hash code just acts like email-id means even if public or intruder gets it, he/she cannot break the system.

*Constraints*

- The user should remember password and should not leak, or reveal to anyone, or write it on any where to protect it from the intruder or hacker.
- Password should be mixed with the number, alphanumeric characters or letters, Lower case and upper case letters, and special characters and the user should remember this.
- Lower mobile network coverage makes denial to the system because of not getting the OTP in time.

*Disadvantages*

- Biometric Fingerprint is less emphasised in verification or authentication process in Multifactor Authentication model.
- User cannot be verified or authenticated without remembering anything at least password information user should carry along with him/her secretly
- Multifactor Authentication Model used in this study is not suitable for the system which does not utilizes a mobile phone and computer like a biometric attendance system.
- Multifactor Authentication Model used in this study requires client-server architecture and not helpful for a standalone system.

## 7.4 FINDINGS OF THE RESEARCH

This research work carried out on Multiple Methods of Fingerprint image Hash code generation using MD5 hash algorithm by utilizing contrast adjustment, modified

segmentation, thinning or without thinning process. This research study reveals some points that are listed below.

- Similar fingerprints have comparable hash values means hash values are distinct or unique in all six methods discussed in this study.
- Same person different finger of the same hand produces different hash codes.
- Partial fingerprints with very minimum or minute minutiae also sufficient to generate Hash code.
- Hash coding can be generated by thinning or without thinning process of the fingerprint image. There is no difference in performance except execution time.
- A total number of Ridge ending and Ridge bifurcation are unique for every fingerprint.
- Gabor filter frequencies and angular value will be unique for segmented image of the fingerprint
- Freeman chain code sum of, first difference value, boundary starting x (x0) and y (y0) value and, chain code value for a binary fingerprint image are unique for fingerprint image
- Euclidean distance value from each pixel to nearest neighbor pixel with pixel value one for a binary fingerprint image is unique for fingerprint image
- All the Hash codes produced in this study are translation and rotation independent, which does not become any problem when Multifactor authentication techniques are used for security or verification purpose.
- From Hash code, original fingerprint minutiae cannot be reconstructed or simply it's noninvertible.
- Hash code effectively works as identity-key or index-key used to identify a person uniquely.
- Fingerprint Hash code gives Higher security when combined with Password or One Time Password (OTP)
- Post-processing of minutiae structure does not influence or affects the performance of Hash code.
- Fingerprints are effectively used as index-key or identity-key using a static image of the finger, without actually requiring senor or fingerprint acquisition device captured image repeatedly. The same grayscale image captured at the beginning can be used multiple times.

- Method-3 and Method-6 utilize more or less same elapsed time and small variation appears depending on minutiae structure of fingerprint image.
- Fingerprint Hash code shows very good performance matrices for fingerprint image with very minimum or zero False Match Rate (FMR), False Non-Match Rate (FNMR), Failure to Enroll Rate (FTER), Failure to Capture Rate (FTCR).
- The six Methods used for Fingerprint hash code generation produces zero EER rate, unless and until input fingerprint varies.
- The six Methods used for Fingerprint hash code generation produces zero acceptance and rejection mistake unless and until input fingerprint varies.
- When we compare the Multifactor Authentication Model used in this study with Ideal characteristics of the Authentication system, few of the characteristics are fulfilled, which include good template protection, network protection, performance evaluation matrices, minimum input etc.
- The fingerprint Hash code and Password are easily revocable, which is not in the case of translation and rotation invariant Hash code
- One time captured static fingerprint image are not vulnerable to climate or weather condition changes compared to any other biometric-based authentication system like Indian Aadhaar Card registration process.
- The new multifactor Authentication model requires less knowledgebase input compared to traditional user-id and password based Internet/Mobile banking authentication.
- If the user takes care and ensures user-level security through external devices like USB drive or Private cloud drive, we can eliminate password factor from authentication process.

## 7.5 GENERAL DISCUSSIONS AND CONCLUSION

In this study, six methods are used for generating fingerprint Hash code Based on MD5 Algorithm, which uses either Contrast Adjustment algorithm (proposed work) or Surfeit based segmentation (modified segmentation) to develop Hash code. The six Methods are as follows;

- The Method-1 uses a different process like Preprocessing, Thinning and Minutiae Extraction which includes specifically various techniques- Contrast adjustment filtering, Segmentation, Thinning or Skeletonisation, Preprocessing skeleton,

minutiae extraction, post-processing and again minutiae extraction and forming Minutiae table. Minutiae Table includes ridge ending with code 1 and ridge bifurcation with code 3 and location details (pixel x, y positions) of ridge endings and bifurcations, which are used for generating Hash code with the aid of MD5 Algorithm.

- The Method-2 includes techniques like Contrast adjustment filtering, Binarisation, Segmentation. Here two-dimensional 64 × 64 sized Gabor Filter is used to extract features directly from a segmented image without performing thinning process. The mean, standard deviation, and variance mean for the convolution result of the real part of 64 × 64 sized matrices of Gabor filter is utilized for developing Hash code with the aid of MD5 Algorithm.
- The Method-3 is similar to Method-2 but includes process only binarisation and segmentation without using contrast adjustment. Here also as like Method-2, two-dimensional 64 × 64 sized Gabor Filter is used for extracting features directly from a segmented image without performing thinning process with the aid of MD5 Algorithm.
- In contrast to Method-1, Method-4, Minutiae Table stores only Ridge ending and bifurcation without storing its location or pixel positions. In Method-1, Minutiae table stores position or location also. Fingerprint Hash code is developed based on only Ridge ending and Ridge bifurcation details without considering its location with the aid of MD5 Algorithm.
- Method-5 uses Freeman chain coding first difference value, boundary stating x and y position value, and chain code value. In a fingerprint image, it will be unique property. These details are used to generate Hash code. This includes Contrast adjustment to enhance the image contrast and brightness. This includes enhancement and binarization process. From the binary image 8-connected freeman chain code first difference is calculated for every 8 boundary values and these values are used for generating Hash code with the aid of MD5 Algorithm.
- Method-6 uses Euclidean distance value for each pixel of the binary fingerprint image. As like Method-5 here also Contrast adjustment is done to enhance the image contrast and brightness. From the binarized image Euclidean distance is measured for every pixel and these values are used to generate Hash code with the aid of MD5 Algorithm.

Based on the study of six methods of fingerprint Hash code generation, it's clear that fingerprint Hash code varies when angle or position changes while capturing input fingerprint image. In all most all types of sensors, there will be small variations in fingerprint image while capturing the same fingerprint of the same person once again or two continues sessions. Fingerprint Hash code alone is not sufficient for authentication or security purpose. Based on this information, this study suggests an alternative method for user authentication using multifactor authentication, which utilizes Fingerprint Hash code, Password, and OTP. The summary of the Multifactor Authentication model is explained below.

Initially on the client side using an interface user loads fingerprint image into the system. At first Finger image, foreground feature is extracted from the background using segmentation Later, using Gabor filtering fingerprint image features are extracted. These features are encrypted and sent to the server. As soon as these features arrive at the server in encrypted form, the server receives that and request for One Time Password from OTP generator. OTP generator is a module or function, which is located at server machine. Time synchronized OTP is sent to the registered user mobile phone. Client system prompts a message to enter OTP, which is received through the registered mobile phone of the user. The user enters that OTP through the client interface and this OTP is compared with server generated OTP at the server side.

Hash code is encrypted one again to enhance security. So if an intruder gets stored hash codes from the database, still authentication cannot become successful. If both password and Fingerprint Hash code match then a user is considered as an authenticated user. In other words authentication process successfully completes when OTP, Password, and Fingerprint Hash code matches. If anyone out of Fingerprint Hash code or Password does not matches user is considered as an unauthorized user. If OTP, not matches then user is blocked from further steps in authentication process

## 7.6 LIMITATIONS OF THE RESEARCH STUDY

Some of the limitations of this research work are listed below.

- Fingerprint Hash code alone does not give full security.
- When Mobile service Provider Network fails, user cannot get authenticated.
- This system does not suit for general applications like attendance maintenance system, entry control system, which does not make use of client server architecture.

- Dynamic fingerprints captured through fingerprint sensor cannot be used every time for authentication process due to translation and rotation invariant Hash code.
- A good network, Database and Mobile service provider network are essential for smooth working of the new Multifactor Authentication Model based on Fingerprint Hash code, OTP and Password.

## 7.7 FUTURE RESEARCH DIRECTIONS

The future research directions are listed below;

- The Fingerprint Hash code is used as Index or Identity-key and Hash code can be combined with other biometrics like Iris or retina in order to avoid password in Multifactor authentication model.
- Along with Fingerprint Hash code, some live behaviors of the user can be combined with lip movement or behavioral biometrics like gait style or behavior so that user can authorize or verified without remembering anything.
- All the six Methods of fingerprint Hash code can be compared based on Time complexity.
- Multifactor Authentication model using Fingerprint Hash code, Password and OTP can be implemented using smartphones model in Mobile phone platform and can be effectively and truly tested.

## 7.8 A BRIEF DISCUSSION ON MULTIFACTOR AUTHENTICATION MODEL USING FINGERPRINT HASH CODE AND IRIS RECOGNITION

This part makes a real attempt to elaborate the future scope of the Multifactor Authentication Model. One of the Major difficulties in Multifactor Authentication model using Fingerprint Hash code, Password and OTP (Model discussed in this research study) is, it makes password mandatory and the user should remember password which is mixed with a number, special characters, letters with upper cases and lower cases. This future work model proposes instead of password iris of the user, which is also one of the strongest Physiological biometrics recognition systems. The iris is absolutely fashioned by way of the eighth month of adults and remains stable throughout the lifespan. Statistically extra accurate than even DNA matching since the opportunity of irises being same is 1 in $10^{78}$. Iris is specific and pleasant biometrics that is mainly used for the established order of instant personal identification or verification systems as compared with different biometric technology, together with a face,

speech and fingerprint image and iris verification can without any problems be considered as the most dependable form of physiological biometric technology.

In recent years, the usage of iris for human identification has substantially grown due to the tremendous advantages with traditional or usual or normal authentication techniques based on private identity numbers (PINs) or passwords. In fact, given that iris is intrinsically and uniquely related to a character, they can't be forgotten, without difficulty stolen or reproduced. But, the use of iris may additionally have some drawbacks related to viable safety breaches. On the grounds that iris traits are limited and immutable, if an attacker has got access to the database where they are saved, the system security may be irreparably compromised. To deal with this hassle, an iris structure with template protection becomes very much essential. In these systems, irreversible cryptographic adjustments, inclusive of hash functions, are used to produce secured hash functions earlier than storing them. Lamentably, slight differences in the acquired iris statistics because of acquisition noise, bring about a huge distinction inside the cryptographic functions output.

So here also if we could able to develop an iris recognition system with error correction code or symmetric hash function it will become a highly secured authentication system. In fingerprint recognition system even if we the error correction code or symmetric key based hash function which is not useful in maximum extent because of Fingerprint image an easily mimic-able and compromised very A password using some latest technologies. On the other hand iris recognition not so because we don’t leave iris as like we leave fingerprint anywhere at door, car, and walls or in the crime scene.

## 7.9 CHAPTER SUMMARY

In this concluding chapter, we have discussed summary related to Fingerprint Hash code generation using all six Methods and summary of Multifactor Authentication Model based on Fingerprint Hash code, OTPutilizeand Password. This chapter also listed out Finding of the research with general discussions and conclusion. The limitations of the research work are also listed out. Finallyemphasizedthe chapter mentions about Future research directions.

**********

## REFERENCES


Abdullah-Al-Wadud, M. (2012). A modified histogram equalization for contrast enhancement preserving the small parts in images. *International Journal of Computer Science and Network Security (IJCSNS)*, 12(2), 1.

Adams, R., & Bischof, L. (1994). Seeded region growing. IEEE Transactions on pattern analysis and machine intelligence, 16(6), 641-647.

Adler, A. (2004). Images can be regenerated from quantized biometric match score data. *Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No.04CH37513*, *1*, 469–472. DOI: https://doi.org/10.1109/CCECE.2004.1345057.

Ahmed, M., & Ward, R. (2002). A rotation invariant rule-based thinning algorithm for character recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *24*(12), 1672-1678.

Ailisto, H. J., Lindholm, M., Mantyjarvi, J., Vildjiounaite, E., & Makela, S.-M. (2005). Identifying people from gait pattern with accelerometers. *Proceedings of SPIE - The International Society for Optical Engineering*, *5779*(May 2016), 7–14. DOI: https://doi.org/10.1117/12.603331.

Aithal P. S, Shailashree V. T., Suresh Kumar P. M., (2015). A New ABCD Technique to Analyze Business Models & Concepts. *International Journal of Management, IT and Engineering*, 5 (4), 409 – 423.

Aithal, P. S. (2016). Study on ABCD Analysis Technique for Business Models, Business strategies, Operating Concepts & Business Systems, *International Journal in Management and Social Science*, 4(1), 98-115. DOI: http://doi.org/10.5281/zenodo.161137.

Aithal, P. S. and Pai T, Vaikunta (2016). Concept of Ideal Software and Its Realization Scenarios. *International Journal of Scientific Research and Modern Education (IJSRME)*, 1(1), 826-837.

Aithal, P. S., Shailashree, V. T. & Suresh Kumar, P. M., (2016d). Analysis of ABC Model of Annual Research Productivity using ABCD Framework. *International Journal of Current Research and Modern Education (IJCRME)*, 1(1), 846-858. DOI: http://doi.org/10.5281/zenodo.62022.

Aithal, P. S., Shailashree, V. T., & Kumar, P. M. (2015). A New ABCD Technique to Analyze Business Models & Concepts.

Aithal, P. S., Shailashree, V. T., & Suresh Kumar P. M., (2016a). ABCD analysis of Stage Model in Higher Education. *International Journal of Management, IT and Engineering (IJMIE)*, 6(1), 11-24. DOI: http://doi.org/10.5 281/zenodo.154233.

Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2016b). Application of ABCD Analysis Framework on Private University System in India. *International Journal of Management Sciences and Business Research (IJMSBR)*, 5(4), 159-170. DOI: http://doi.org/10.5281/zenodo.161111.

Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2016c). The Study of New National Institutional Ranking System using ABCD Framework, *International Journal of Current Research and Modern Education (IJCRME)*, 1(1), 389–402. DOI: http://doi.org/10.5281/zenodo.161077.

Aithal, S., & Aithal, P. S. (2016). ABCD analysis of Dye doped Polymers for Photonic Applications, IRA-International Journal of Applied Sciences, 4 (3), 358-378. DOI: http://dx.doi.org/10. 21013/j as.v4.n3.p1.

Akram, M. U., Tariq, A., Khan, S. A., & Nasir, S. (2008). Fingerprint image: pre-and post-processing. *International Journal of Biometrics*, *1*(1), 63-80.

Ali, J. M. H., & Hassanien, A. E. (2003). An iris recognition system to enhance e-security environment based on wavelet theory. *AMO-Advanced Modeling and Optimization*, *5*(2), 93–104.

Alibeigi, E., Rizi, M. T., & Behnamfar, P. (2009). Pipelined minutiae extraction from fingerprint images. In *Canadian Conference on Electrical and Computer Engineering* (pp. 239–242). DOI: https://doi.org/10.1109/CCECE.2009.5090128.

Alonso-Fernandez, F., Fierrez-Aguilar, J. and Ortega-Garcia, J. (2005) An enhanced Gabor filter based segmentation algorithm for fingerprint recognition systems, *Proc. IEEE Intl. Symposium on Image and Signal Processing and Analysis, ISPA, Spec. Sess On. Signal Image Processing for Biometrics, IEEE Press, Zagreb (Croatia), September 2005*, 239–244. DOI: https://doi.org/10.1109/ISPA.2005.195416.

Amengual, J. C., Juan, A., Pérez, J. C., Prat, F., Sáez, S., & Vilar, J. M. (1997). Real-time minutiae extraction in fingerprint images.

Amy, L. (1948). Recherches sur L'identification des Traces Papillaries. *Annales de Medecine Legale*, *28*(2), 96-101.

Arakala, A., Jeffers, J., & Horadam, K. J. (2007, August). Fuzzy extractors for minutiae-based fingerprint authentication. In *International Conference on Biometrics* (pp. 760-769). Springer, Berlin, Heidelberg.

Arcelli, C., & Di Baja, G. S. (1985). A width-independent fast thinning algorithm. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, (4), 463-474.

Asker M. Bazen and Sabih H. Gerez. 2001. Segmentation of Fingerprint Images, Workshop on Circuits, Systems and Signal Processing, Veldhoven. The Netherlands.

Balthazard, V. (1911). De l'identification par les empreintes digitales. *Comptes Rendus, des Academies des Sciences*, *152*, 1862.

Bansal, R., Sehgal, P., & Bedi, P. (2010). Effective morphological extraction of true fingerprint minutiae based on the hit or miss transform. *International Journal of Biometrics and Bioinformatics (IJBB)*, *4*(2), 71.

Bansal, R., Sehgal, P., & Bedi, P. (2011). Minutiae extraction from fingerprint images-a review. *arXiv preprint arXiv:1201.1422*.

Barreto, P., Marques, A.C. and Thome, A.C. (2005) A neural network fingerprint segmentation method, 5th International Conference on Hybrid Intelligent Systems P.6.

Bazen, A. M., & Gerez, S. H. (2000, November). Directional field computation for fingerprints based on the principal component analysis of local gradients. In *Proceedings of ProRISC2000, 11th Annual Workshop on Circuits, Systems and Signal Processing* (pp. 215-222). Veldhoven, the Netherlands.

Bazen, A.M. and Gerez, S.H. (2000) Directional field computation for fingerprints based on the principal component analysis of local gradients, Proceedings of ProRISC2000, 11th Annual Workshop on Circuits, Systems and Signal Processing, Veldhoven, The Netherlands.

Beleznai, C., Ramoser, H., Wachmann, B., Birchbauer, J., Bischof, H., & Kropatsch, W. (2001, October). Memory efficient fingerprint verification. In *International Conference on Image Processing* (pp. 463–466).

Bernard, M., Fromont, E., Habrard, A., & Sebban, M. (2012, June). Handwritten digit recognition using edit distance-based KNN. In *Teaching Machine Learning Workshop*.

Brin, D. (1999). *The transparent society: Will technology force us to choose between privacy and freedom?*. Perseus (for Hbg).

Brown, M. E., & Rogers, S. J. (1996). *U.S. Patent No. 5,557,686*. Washington, DC: U.S. Patent and Trademark Office.

C. Domeniconi, S. Tari, and P. Liang. (1998). Direct Gray Scale Ridge Reconstruction in Fingerprint Images. International Conference on Acoustics, Speech, and Signal Processing, 5, 2941-2944.

Canny, J. (1986). A computational approach to edge detection. IEEE Transactions on pattern analysis and machine intelligence, (6), 679-698.

Cao, G., Zhao, Y., Ni, R., Yu, L., & Tian, H. (2010). Forensic detection of median filtering in digital images. In *2010 IEEE International Conference on Multimedia and Expo, ICME 2010* (pp. 89–94). DOI: https://doi.org/10.1109/ICME.2010.5583869.

Cappelli, R., Maio, D., Lumini, A., & Maltoni, D. (2007). Fingerprint image reconstruction from standard templates. *IEEE transactions on pattern analysis and machine intelligence*, *29*(9).

Cavoukian, A., & Stoianov, A. (2007). *Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy*. Information and Privacy Commissioner, Ontario.

Chakraborty, A., Staib, L. H., & Duncan, J. S. (1996). Deformable boundary finding in medical images by integrating gradient and region information. IEEE Transactions on Medical Imaging, 15(6), 859-870.

Chen, S. Der, & Ramli, A. R. (2003). Contrast enhancement using recursive mean-separate histogram equalization for scalable brightness preservation. *IEEE Transactions on Consumer Electronics*, 49(4), 1301–1309. DOI: https://doi.org/10.1109/TCE.2003.1261233.

Chen, X., Tian, J., Cheng, J., & Yang, X. (2004). Segmentation of fingerprint images using linear classifier. *EURASIP Journal on Advances in Signal Processing*, *2004*(4), 978695.

Chi-Chia, S., Shanq-Jang, R., Mon-Chau, S., & Tun-Wen, P. (2005). Dynamic contrast enhancement based on histogram specification. *Consumer Electronics, IEEE Transactions on*, 51(4), 1300–1305. DOI: https://doi.org/10.1109/TCE.2005.1561859.

Chikkerur, S., Govindaraju, V., & Cartwright, A. N. (2005, August). Fingerprint image enhancement using STFT analysis. In *International Conference on Pattern Recognition and Image Analysis* (pp. 20-29). Springer, Berlin, Heidelberg.

Choi, H., Boaventura, M., Boaventura, I. A. G., & Jain, A. K. (2012). Automatic segmentation of latent fingerprints. 2012 IEEE Fifth International Conference on Biometrics: Theory, Applications, and Systems (BTAS), 303–310. DOI: https://doi.org/10.1109/BTAS.2012.6374593.

Coetzee, L., & Botha, E. C. (1993). Fingerprint recognition in low quality images. *Pattern recognition*, *26*(10), 1441-1460.

Collins, F.S., et al. (2004). Finishing the euchromatic sequence of the human genome. Nature, 431(7011), 931-45.

Connie, T., Teoh, A., Goh, M., & Ngo, D. (2005). PalmHashing: a novel approach for cancelable biometrics. *Information processing letters*, 93(1), 1-5.

Cummins, H., & Midlo, C. (1961). Fingerprints palms and soles-an introduction to dermatoglyphics. New York: The Blakistan Co.

Cummins, H., Midlo, C., & Fingerprints, P. (1961). Soles: An Introduction to Dermatoglyphics. *New York*.

Cuntoor, N., Kale, A., & Chellappa, R. (2003). Combining multiple evidences for gait recognition. In *2003 IEEE International Conference on Acoustics, Speech, and Signal Processing, 2003. Proceedings. (ICASSP '03).* (Vol. 3, p. III-33-6). DOI: https://doi.org/10.1109/ICASSP.2003.1199100.

Daugman, J. (2006). Probing the uniqueness and randomness of iriscodes: Results from 200 billion iris pair comparisons. *Proceedings of the IEEE*, *94*(11), 1927–1934. DOI: https://doi.org/10.1109/JPROC.2006.884092.

David, M., Jain, M. and Prabhakar, S. (2005) Handbook of Fingerprint Recognition, Springer Verlag, New York.

Davida, G. I., Frankel, Y., Matt, B., & Peralta, R. (1999). On the relation of error correction and cryptography to an online biometric based identification scheme. In *Workshop on coding and cryptography*.

De La Torre, Á., Peinado, A. M., Segura, J. C., Pérez-Córdoba, J. L., Benítez, M. C., & Rubio, A. J. (2005). Histogram equalization of speech representation for robust speech recognition. *IEEE Transactions on Speech and Audio Processing*, 13(3), 355–366. DOI: https://doi.org/10.1109/TSA.2005.845805.

Dharchaudhuri, M. (2010) Indexing of large biometric database, Bachelor in Technology thesis, Department of Computer Science and Engineering, National Institute of Technology, Rourkela, Pp. 18,19

Di Zenzo, S., Cinque, L., & Levialdi, S. (1996). Run-based algorithms for binary image analysis and processing. *IEEE Transactions on pattern analysis and machine intelligence*, *18*(1), 83-89. DOI: http://doi.org/10.5281/zenodo.810343.

Dowling, J. (2007) Retina, Scholarpedia, Vol.2, No.12, P.3487.

E. R. Henry (1900), Classification and Uses of Fingerprints, London: Routledge, 54-58.

Espinosa-Duro, V. (2002). Mathematical Morphology approaches for fingerprint Thinning. In *Security Technology, 2002. Proceedings. 36th Annual 2002 International Carnahan Conference on* (pp. 43-45). IEEE.

Farina, A., Kovacs-Vajna, Z. M., & Leone, A. (1999). Fingerprint minutiae extraction from skeletonized binary images. *Pattern recognition*, *32*(5), 877-889.

Faundez-Zanuy, M. (2007). On-line signature recognition based on VQ-DTW. *Pattern Recognition*, *40*(3), 981–992.DOI: https://doi.org/10.1016/j.patcog.2006.06.007.

Feng, J., & Jain, A. K. (2009, June). FM model based fingerprint reconstruction from minutiae template. In *International Conference on Biometrics* (pp. 544-553). Springer, Berlin, Heidelberg.

Fields, C., Falls, H. C., Warren, C. P., & Zimberoff, M. (1960). The ear of the newborn as an identification constant. *Obstetrics & Gynecology*, *16*(1), 98-hyhen.

Fronthaler, H., Kollreider, K., & Bigun, J. (2005, October). Local feature extraction in fingerprints by complex filtering. In *IWBRS* (pp. 77-84).

Gafurov, D., & Snekkenes, E. (2009). Gait recognition using wearable motion recording sensors. *EURASIP Journal on Advances in Signal Processing*, *2009*, 7.

Galton, F. (1892). *Finger prints*. Macmillan and Company.

Galton, F. (1965). Fingerprints (reprint). *Da Capo Press*, 63, 4-7.

Galy, N., Charlot, B., & Courtois, B. (2007). A full fingerprint verification system for a single-line sweep sensor. *IEEE Sensors Journal*, *7*(7), 1054-1065.

Gamassi, M., Piuri, V., & Scotti, F. (2005, September). Fingerprint local analysis for high-performance minutiae extraction. In *Image Processing, 2005. ICIP 2005. IEEE International Conference on* (Vol. 3, pp. III-265). IEEE.

Gao, X., Chen, X., Cao, J., Deng, Z., Liu, C., & Feng, J. (2010, September). A novel method of fingerprint minutiae extraction based on Gabor phase. In *Image Processing (ICIP), 2010 17th IEEE International Conference on* (pp. 3077-3080). IEEE.

Garcia, J. D. (1986). *U.S. Patent No. 4,621,334*. Washington, DC: U.S. Patent and Trademark Office.

Gnanasivam, P., & Muttan, S. (2010). An efficient algorithm for fingerprint preprocessing and feature extraction. *Procedia Computer Science*, *2*, 133-142.

Goldstein, A. J., Harmon, L. D., & Lesk, A. B. (1971). Identification of human faces. *Proceedings of the IEEE*, *59*(5), 748-760.

Gonzalez, R. C., & Woods, R. E. (1992). Digital image processing.

Gonzalez, R. C., Woods, R. W. (2002). *Digital Image Processing*. *Education*. DOI: https://doi.org/10.1049/ep.1978.0474.

Gonzalez, R. C., Woods, R. W. (2002). *Digital Image Processing*. *Education*. DOI: https://doi.org/10.1049/ep.1978.0474.

Govindaraju, V., Shi, Z., & Schneider, J. (2003, March). Feature Extraction Using a Chaincoded Contour Representation of Fingerprint Images. In *AVBPA* (pp. 268-275).

Greenberg, S., Aladjem, M., Kogan, D., & Dimitrov, I. (2000). Fingerprint image enhancement using filtering techniques. In *Pattern Recognition, 2000. Proceedings. 15th International Conference on* (Vol. 3, pp. 322-325). IEEE.

Gupta, S. R. (1968). Statistical survey of ridge characteristics. *Int. Criminal Police Review*, *218*(130).

Halici, U., Jain, L.C. and Erol, A. (1999) Introduction to fingerprint recognition, The Crc International Series On Computational Intelligence, Intelligent biometric techniques in fingerprint and face recognition, CRC Press Inc., Pp.1-34.

Hao, F, Anderson, R & Daugman, J 2006, _Combining Crypto with Biometrics Effectively', IEEE Transactions on Computers, vol. 55, pp. 1081-1088.

Harris, C., & Stephens, M. (1988, August). A combined corner and edge detector. In *Alvey vision conference* (Vol. 15, No. 50, pp. 10-5244).

Hastings, E. (1992). A survey of thinning methodologies. *Pattern analysis and Machine Intelligence, IEEE Transactions*, *4*(9), 869-885.

He, Y., Tian, J., Luo, X., & Zhang, T. (2003). Image enhancement and minutiae matching in fingerprint verification. *Pattern recognition letters*, *24*(9), 1349-1360.

Heath, M. D., Sarkar, S., Sanocki, T., & Bowyer, K. W. (1997). A robust visual method for assessing the relative performance of edge-detection algorithms. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *19*(12), 1338-1359.

Holst, J. C., & Draper, D. A. (1999). *U.S. Patent No. 5,999,039*. Washington, DC: U.S. Patent and Trademark Office.

Hong, L., Jain, A.K., Pankanti, S. & Bolle, R. (1996). Fingerprint Enhancement. Proceedings of the First IEEE WACV, Sarasota, FL, pp. 202–207.

Hong, L., Wan, Y., & Jain, A. (1998). Fingerprint image enhancement: Algorithm and performance evaluation. *IEEE transactions on pattern analysis and machine intelligence*, *20*(8), 777-789.

http://www.bccresearch.com/report/biometrics-technologies-markets-ift042e.html. Last Access Date: 06-08-2017.

https:// www.barcode.ro/tutorials/biometrics/fingerprint.html. Last Access Date: 14-08-2017.

https://hackaday.com/2015/11/10/your-unhashable-fingerprints-secure-nothing/, Last Accesses Date: 05-12-2017.

https://security.stackexchange.com/questions/42384/is-there-any-way-to-cryptographically-hash-a-human-thumbprint, Last Accesses Date: 05-12-2017.

Humbe, V., Gornale, S. S., Manza, R., & Kale, K. V. (2007). Mathematical morphology approach for genuine fingerprint feature extraction. *International Journal of Computer Science and Security*, *1*(2), 45-51.

Iannarelli, A. V. (1989). *Ear identification*. Paramont Publishing Company.

Ibrahim, H., & Kong, N. S. P. (2007). Brightness preserving dynamic histogram equalization for image contrast enhancement. *IEEE Transactions on Consumer Electronics*, 53(4), 1752–1758. DOI: https://doi.org/10.1109/TCE.2007.4429280.

Ibrahim, Haidi. "Histogram equalization with range offset for brightness preserved image enhancement." *International Journal of Image Processing (IJIP)* 5, no. 5 (2011): 599-609.

Im, S. K., Park, H. M., Kim, Y. W., Han, S. C., Kim, S. W., Kang, C. H., & Chung, C. K. (2001). An biometric identification system by extracting hand vein patterns. *Journal-Korean Physical Society*, *38*(3), 268-272.

International Human Genome Sequencing Consortium. (2004). Finishing the euchromatic sequence of the human genome. *Nature*, *431*(7011), 931-945.

Iradian Technologies (2003), Experts in Authentication Technology, http://www.iridiantech.com/technologies (Last retrieval date: 30-08-2012).

Jagatheeswari, P., Kumar, S. S., & Rajaram, M. (2009). Contrast stretching recursively separated histogram equalization for brightness preservation and contrast enhancement. In *ACT 2009 - International Conference on Advances in Computing, Control and Telecommunication Technologies* (pp. 111–115). DOI: https://doi.org/10.1109/ACT.2009.37.

Jain, A. K. (1989). *Fundamentals of Digital Image Processing*. *Portalacmorg* (Vol. 14). DOI: https://doi.org/10.1002/9780470689776.

Jain, A. K., & Dubes, R. C. (1988). Algorithms for clustering data. Prentice-Hall, Inc.

Jain, A. K., Hong, L., Pankanti, S., & Bolle, R. (1997). An identity-authentication system using fingerprints. *Proceedings of the IEEE*, *85*(9), 1365-1388.

Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric template security. *EURASIP Journal on Advances in Signal Processing*, *2008*, 113.

Jain, A. K., Nandakumar, K., & Nagar, A. (2013). Fingerprint template protection: From theory to practice. In *Security and Privacy in Biometrics* (pp. 187-214). Springer London.

Jain, A. K., Prabhakar, S., & Pankanti, S. (2002). On the similarity of identical twin fingerprints. *Pattern Recognition*, *35*(11), 2653-2663.

Jain, A. K., Prabhakar, S., Hong, L., & Pankanti, S. (1999). FingerCode: a filterbank for fingerprint representation and matching. In *Computer Vision and Pattern Recognition, 1999. IEEE Computer Society Conference on*. (Vol. 2, pp. 187-193). IEEE.

Jain, A. K., Prabhakar, S., Hong, L., & Pankanti, S. (2000). Filterbank-based fingerprint matching. *IEEE transactions on Image Processing*, *9*(5), 846-859.

Jain, A. K., Ratha, N. K., & Lakshmanan, S. (1997). Object detection using Gabor filters. *Pattern recognition*, *30*(2), 295-309.

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Commun. ACM*, *43*(2), 90–98. DOI: https://doi.org/http://doi.acm.org/10.1145/328236.328110.

Jain, A.K. and Maltoni, D. (2003) Handbook of fingerprint recognition, Springer-Verlag New York Inc., Secaucus, NJ, USA.

Jiang, X., Yau, W. Y., & Ser, W. (2001). Detecting the fingerprint minutiae by adaptive tracing the gray-level ridge. *Pattern recognition*, *34*(5), 999-1013.

Jin, A. T. B., Ling, D. N. C., & Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition*, *37*(11), 2245-2255.

Juels, A. (2002). M. Sudan 'A fuzzy vault scheme'. In *Proceedings of the 2002 IEEE International Symposium on Information Theory* (Vol. 408).

Juels, A., & Wattenberg, M. (1999, November). A fuzzy commitment scheme. In *Proceedings of the 6th ACM conference on Computer and communications security* (pp. 28-36). ACM.

Krishna Prasad, K., & Aithal, P.S. (2018b). A Study on Pre and Post Processing of Fingerprint Thinned Image to Remove Spurious Minutiae from Minutiae Table**.** International Journal of Current Research and Modern Education, 3(1), 197-212.

Krishna Prasad, K., & Aithal, P. S. (2017a). Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 2(2), 8-19.

Krishna Prasad, K., & Aithal, P. S. (2017b). A Critical Study on Fingerprint Image Sensing and Acquisition Technology. *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, 1(2), 86-92. DOI: http://dx.doi.org/10.5281/zenodo.1130581.

Krishna Prasad, K., & Aithal, P. S. (2017c). A Customized and Flexible Ideal Mobile Banking System Using 5g Technology. *International Journal of Management, Technology, and Social Sciences (IJMTS)*,1(1), 25-37. DOI: http://doi.org/10.5281/zenodo.820457.

Krishna Prasad, K., & Aithal, P. S. (2017d). A Conceptual Study on Image Enhancement techniques for Fingerprint Images. International Journal of Applied Engineering and Management Letters (IJAEML),1(1), 63-72. DOI: http://10.5281/zenodo.831678.

Krishna Prasad, K., & Aithal, P. S. (2017e). Fingerprint Image Segmentation: A Review of State of the Art Techniques. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 2(2), 28-39. DOI: http://dx.doi.org/10.5281/zenodo.848191.

Krishna Prasad, K., & Aithal, P. S. (2017f) A Novel Method to Control Dominating Gray Levels During Image Contrast Adjustment Using Modified Histogram Equalization (September 19, 2017). International Journal of Applied Engineering and Management Letters (IJAEML), 1(2), 27-39. DOI: http://dx.doi.org/10.5281/zenodo.896653.

Krishna Prasad, K., & Aithal, P. S. (2017g).Two Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(2), 51-65.

Krishna Prasad, K., & Aithal, P. S. (2017h). A conceptual Study on Fingerprint Thinning Process based on Edge Prediction. International Journal of Applied Engineering and Management Letters (IJAEML), 1(2), 98-111. DOI: http://dx.doi.org/10.5281/zenodo.1067110.

Krishna Prasad, K., & Aithal, P. S. (2017i). A Study on Fingerprint Hash Code Generation using Euclidean Distance for Identifying a User. International Journal of Management, Technology, and Social Sciences (IJMTS), 2(2), 116-126.

Krishna Prasad, K., & Aithal, P. S. (2018a). A Novel Tuning Based Contrast Adjustment Algorithm for Grayscale Fingerprint Image. Saudi Journal of Engineering and Technology (SJEAT), 3(1), 15-23. DOI: http://10.21276/sjeat.2018.3.1.3.

Krishna Prasad, K., & Aithal, P. S. (2018c). An Alternative Approach to Fingerprint Hash Code Generation based on Modified Filtering Techniques**.** *International Journal of Innovative Research in Management, Engineering And Technology*, 2(12), 1-13. DOI: IJIRMET1602012001.

Krishna Prasad, K., & Aithal, P. S. (2018d). A Study on Fingerprint Hash Code Generation Based on MD5 Algorithm and Freeman Chain Code. *International Journal of Computational Research and Development*. 3(1), 13-22. DOI : http://doi.org/10.5281/zenodo.1144555.

Krishna Prasad, K., & Aithal, P. S. (2018e). A Study on Multifactor Authentication Model Using Fingerprint Hash Code, Password and OTP. *International Journal of Advanced Trends in Engineering and Technology*, 3(1), 1-11. DOI : http://doi.org/10.5281/zenodo.1135255.

Krishna Prasad, K., & Aithal, P. S. (2018f). ABCD Analysis of Fingerprint Hash Code, Password and OTP based Multifactor Authentication Model. Saudi Journal of Business and Management Studies, 3(1), 65-80. DOI: http://10.21276/sjbms.2018.3.1.10.

Krishna Prasad, K., & Aithal, P. S. (2018g). A Comparative Study on Fingerprint Hash Code, OTP, and Password based Multifactor Authentication Model with an Ideal System and Existing Systems. International Journal and Advanced Scientific Research, 3(1), 18-32. DOI : http://doi.org/10.5281/zenodo.1149587.

Ke, Y., & Sukthankar, R. (2004, June). PCA-SIFT: A more distinctive representation for local image descriptors. In *Computer Vision and Pattern Recognition, 2004. CVPR 2004. Proceedings of the 2004 IEEE Computer Society Conference on* (Vol. 2, pp. II-II). IEEE.

Kelkboom, E. J., Gökberk, B., Kevenaar, T. A., Akkermans, A. H., & van der Veen, M. (2007, August). "3D face": biometric template protection for 3D face recognition. In *International Conference on Biometrics* (pp. 566-573). Springer, Berlin, Heidelberg.

Kim, Y. T. (1997). Contrast enhancement using brightness preserving bi-histogram equalization. *IEEE Transactions on Consumer Electronics*, 43(1), 1–8. DOI: https://doi.org/10.1109/30.580378.

Kim, Y.-T. (1997). Quantized bi-histogram equalization. *Acoustics, Speech, and Signal Processing, 1997. ICASSP-97., 1997 IEEE International Conference on*, 4, 2797–2800 vol.4. DOI: https://doi.org/10.1109/ICASSP.1997.595370.

Kingston, C. R. (1964). *Probabilistic analysis of partial fingerprint patterns*. University of California.

Klein, S., Bazen, A., & Veldhuis, R. (2002, November). Fingerprint image segmentation based on hidden Markov models. In *Proceedings of 13th Annual Workshop on Circuits, Systems, and Signal Processing* (pp. 310-318).

Komarinski, P. (2005). *Automated fingerprint identification systems (AFIS)*. Academic Press.

Kus, M., Kacar, U., Kirci, M., & Gunes, E. O. (2013). ARM based ear recognition embedded system. In *IEEE EuroCon 2013* (pp. 2021–2028). DOI: https://doi.org/10.1109/EUROCON.2013.6625258.

Kwok, R. (2009) Fake finger reveals the secrets of touch, Nature, Vol. 29, http://www.nature.com/news/2009/090129/full/news.2009.68.html, Last Access Date: 14-08-2017.

Lam, H. K., Hou, Z., Yau, W. Y., Chen, T. P., & Li, J. (2008, December). A systematic topological method for fingerprint singular point detection. In *Control, Automation, Robotics and Vision, 2008. ICARCV 2008. 10th International Conference on* (pp. 967-972). IEEE.

Lander, E.S., et al. (2001). Initial sequencing and analysis of the human genome. Nature, 409(6822), 860-921. Last Accesses Date: 05-12-2017.

Lee, C., Lee, S., Kim, J., & Kim, S. J. (2006, January). Preprocessing of a fingerprint image captured with a mobile camera. In International Conference on Biometrics, Springer, Berlin, Heidelberg. 348-355.

Lee, P.J. (1973) Life of Latents, Identification News, 23(4), 10-13.

Lee, Y., Lee, K., & Pan, S. (2005, July). Local and global feature extraction for face recognition. In *AVBPA* (pp. 219-228).

Li, S. Z., & Jain, A. K. (2005). *Handbook of Face Recognition*. *Handbook of face recognition*. DOI: https://doi.org/10.1017/CBO9781107415324.004.

Liu, J., Huang, Z., & Chan, K. L. (2000, September). Direct minutiae extraction from gray-level fingerprint image by relationship examination. In *Image Processing, 2000. Proceedings. 2000 International Conference on* (Vol. 2, pp. 427-430). IEEE.

Maddala, S., Bartunek, J. S., & Nilsson, M. (2010, December). Implementation and evaluation of NIST biometric image software for fingerprint recognition. In *Signal and Image Processing (ICSIP), 2010 International Conference on* (pp. 207-211). IEEE.

Mahajan, R., Gupta, T., Mahajan, S. and Bawa, N. (2009) Retina as Authentication Tool for Covert Channel Problem, World Academy of Science, Engineering and Technology, 56,153-158.

Maio, D., & Maltoni, D. (1997). Direct gray-scale minutiae detection in fingerprints. *IEEE transactions on pattern analysis and machine intelligence*, *19*(1), 27-40.

Maio, D., & Maltoni, D. (1998, August). Neural network based minutiae filtering in fingerprints. In *Pattern Recognition, 1998. Proceedings. Fourteenth International Conference on* (Vol. 2, pp. 1654-1658). IEEE.

Malathi, S. (2012). An efficient approach for partial fingerprint recognition based on Pores and SIFT features using fusion methods. Ph.D. Thesis. University of Avinashilingam, Coimbatore, Tamil Nadu, India.

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2003). *Handbook of Fingerprint Recognition*. *Annals of Physics* (Vol. 54). DOI: https://doi.org/10.1109/MEI.2004.1342443.

Maltoni, D., Maio, D., Jain, A., & Prabhakar, S. (2009). *Handbook of fingerprint recognition*. Springer Science & Business Media.

Mäntyjärvi, J., Lindholm, M., Vildjiounaite, E., Mäkelä, S. M., & Ailisto, H. (2005). Identifying users of portable devices from gait pattern with accelerometers. In *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings* (Vol. II).DOI: https://doi.org/10.1109/ICASSP.2005.1415569.

Maria Vlad, M., Anisie, A. and Vlad, M.S. (2012). Automatic identification technologies, *International Journal of Systems Applications, Engineering & Development*, 6(1), 98-105.

Mauceri, A.J. (1965) Feasibility studies of personal identification by Signature verification, Space and Information System Division, North American Aviation Co., Anaheim, USA.

Medien, B., & Burghardt, T. (2002). Report on Identity Verification. *University of Bristol*.

Meghdadi, M., & Jalilzadeh, S. (2005, October). Validity and acceptability of results in fingerprint scanners. In *Proceedings of the 7th WSEAS International Conference on Mathematical Methods and Computational Techniques In Electrical Engineering* (pp. 259-266). World Scientific and Engineering Academy and Society (WSEAS).

Mehtre, B. M., & Chatterjee, B. (1989). Segmentation of fingerprint images—a composite method. Pattern Recognition, 22(4), 381-385.

Mehtre, B. M., Murthy, N. N., Kapoor, S., & Chatterjee, B. (1987). Segmentation of fingerprint images using the directional image. Pattern Recognition, 20(4), 429-435.

Memon, S., Sepasian, M., & Balachandran, W. (2008, December). Review of finger print sensing technologies. In *Multitopic Conference, 2008. INMIC 2008. IEEE International* (pp. 226-231). IEEE.

Mieloch, K., Munk, A., & Mihailescu, P. (2008, September). Hierarchically linked extended features in fingerprints. In *Biometrics Symposium, 2008. BSYM'08* (pp. 47-52). IEEE.

Misra, D. K., Tripathi, S. P., & Singh, A. (2012). Fingerprint image enhancement, thinning and matching. International Journal of Emerging Trends & Tech in Comp Science (IJETTCS), 1(2), 17-21.

Mitnick, K. D., & Simon, W. L. (2003). The Art of Deception: Controlling the Human Element in Security. *BMJ: British Medical Journal*, 368. DOI: https://doi.org/0471237124.

Moayer, B., & Fu, K. S. (1975). A syntactic approach to fingerprint pattern recognition. Pattern Recognition, 7(1–2), 1–23. DOI: https://doi.org/10.1016/0031-3203(75)90011-4.

Moenssens, A. A. (1975). Fingerprint techniques. Chilton.

Moravec, H. P. (1977). Towards automatic visual bbstacle avoidance. In *International Conference on Artificial Intelligence (5th: 1977: Massachusetts Institute of Technology)*.

Moreno, A. B., Sánchez, A., Vélez, J. F., & Díaz, F. J. (2003, September). Face recognition using 3D surface-extracted descriptors. In *Irish Machine Vision and Image Processing Conference* (Vol. 2003).

Naji, A.W., Ramli, A.R., Ali, R., Rahman, S.A., and Ali, M.L. (2002) A segmentation algorithm based on histogram equalizer for fingerprint classification system, Second International Conference on Electrical and Computer Engineering ICECE 2002, Dhaka, Bangladesh, Pp. 390-393.

Nandakumar, K. (2008), Multibiometric Systems: Fusion Strategies and Template Security',( Doctorial Thesis ,Michigan State University, East Lansing, MI, USA).

Nandakumar, K., & Jain, A. K. (2004, December). Local Correlation-based Fingerprint Matching. In *ICVGIP* (pp. 503-508).

Nandakumar, K., Jain, A. K., & Nagar, A. (2008). Biometric template security. *Eurasip Journal on Advances in Signal Processing*, *2008*. DOI: https://doi.org/10.1155/2008/579416.

Nanni, L., & Lumini, A. (2008). Local binary patterns for a hybrid fingerprint matcher. *Pattern recognition*, *41*(11), 3461-3466.

Nauman, M., & Ali, T. (2010). TOKEN: Trustable keystroke-based authentication for web-based applications on smartphones. In *Communications in Computer and Information Science* (Vol. 76 CCIS, pp. 286–297). DOI: https://doi.org/10.1007/978-3-642-13365-728.

Newham, E. (1995). The biometric report. SJB services, 733.

Nikam, S. B., & Agarwal, S. (2008). Local binary pattern and wavelet-based spoof fingerprint detection. *International Journal of Biometrics*, *1*(2), 141-159.

Nilsson, K., & Bigun, J. (2001). Using linear symmetry features as a pre-processing step for fingerprint images. In *Audio-and Video-Based Biometric Person Authentication* (pp. 247-252). Springer Berlin/Heidelberg.

O'Gorman, L., & Nickerson, J. V. (1989). An approach to fingerprint filter design. *Pattern recognition*, *22*(1), 29-38.

Olsen, R. D. (1972). The chemical composition of palmar sweat. *Fingerprint and Identification Magazine*, *53*(10), 3.

Osterburg, J. W., Parthasarathy, T., Raghavan, T. E. S., & Sclove, S. L. (1977). Development of a mathematical formula for the calculation of fingerprint probabilities based on individual characteristics. *Journal of the American statistical association*, *72*(360a), 772-778.

Otsu, N. (1979). A threshold selection method from gray-level histograms. *IEEE transactions on systems, man, and cybernetics*, *9*(1), 62-66.

Pankanti, S., Prabhakar, S., & Jain, A. K. (2002). On the individuality of fingerprints. *IEEE Transactions on pattern analysis and machine intelligence*, *24*(8), 1010-1025.

Parashar, S., Vardhan, A., Patvardhan, C., & Kalra, P. K. (2008). Design and implementation of a robust palm biometrics recognition and verification system. In *Proceedings - 6th Indian*

*Conference on Computer Vision, Graphics and Image Processing, ICVGIP 2008* (pp. 543–550).DOI: https://doi.org/10.1109/ICVGIP.2008.56.

Pathak, P. (2010). Image Compression Algorithms for Fingerprint System. *IJSCI International Journal of Computer Science Issues*, *7*(3), 45-50.

Patil, P. M., Suralkar, S. R., & Sheikh, F. B. (2005, November). Rotation invariant thinning algorithm to detect ridge bifurcations for fingerprint identification. In *Tools with Artificial Intelligence, 2005. ICTAI 05. 17th IEEE International Conference on* (pp. 8-pp). IEEE.

Pei, S. C., Zeng, Y. C., & Chang, C. H. (2004). Virtual restoration of ancient Chinese paintings using color contrast enhancement and Lacuna texture synthesis. *IEEE Transactions on Image Processing*, 13(3), 416–429. DOI: https://doi.org/10.1109/TIP.2003.821347.

Phillips, P. J., Moon, H., Rizvi, S. A., & Rauss, P. J. (2000). The FERET evaluation methodology for face-recognition algorithms. *IEEE Transactions on pattern analysis and machine intelligence*, *22*(10), 1090-1104.

Pizer, S. M. (2003). The Medical Image Display and Analysis Group at the University of North Carolina: Reminiscences and philosophy. *Medical Imaging, IEEE Transactions on*, 22(1), 2–10. DOI: https://doi.org/10.1109/TMI.2003.809707.

Ratha, N. K., Bolle, R. M., Pandit, V. D., & Vaish, V. (2000). Robust fingerprint authentication using local structural similarity. In *Applications of Computer Vision, 2000, Fifth IEEE Workshop on.* (pp. 29-34). IEEE.

Ratha, N. K., Chen, S., & Jain, A. K. (1995). Adaptive flow orientation-based feature extraction in fingerprint images. *Pattern Recognition*, *28*(11), 1657-1672.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001, June). An analysis of minutiae matching strength. In *International Conference on Audio-and Video-Based Biometric Person Authentication* (pp. 223-228). Springer Berlin Heidelberg.

Ratha, NK, Chikkerur, S, Connell, JH & Bolle, RM (2007), Generating cancellable fingerprint templates', IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 561–572.

Roddy, A. R., & Stosz, J. D. (1997). Fingerprint features-statistical analysis and system performance estimates. *Proceedings of the IEEE*, *85*(9), 1390-1421.

Rood, E.P. and Hornak,L.A. (2008) Are you who you say you are ? http://www.worldandicollege.com/public/2003/august/nspub1.asp, Last Visit on September. 2nd, September 2017).

Ross, A. A. A., Nandakumar, K., & Jain, A. A. K. (2006). *Handbook of multibiometrics*. *Interface* (Vol. 6). DOI: https://doi.org/10.1007/0-387-33123-9.

Ross, A., Jain, A., & Reisman, J. (2003). A hybrid fingerprint matcher. *Pattern Recognition*, *36*(7), 1661-1673.

Ross, A., Shah, J., & Jain, A. K. (2007). From template to image: Reconstructing fingerprints from minutiae points. *IEEE transactions on pattern analysis and machine intelligence*, *29*(4), 544-560.

Roxburgh, T. J. Y. (1933). Galton's work on the evidential value of finger prints. *Sankhyā: The Indian Journal of Statistics (1933-1960)*, *1*(1), 50-62.

Sagar, V. K., & Alex, K. J. B. (1999). Hybrid fuzzy logic and neural network model for fingerprint minutiae extraction. In *Neural Networks, 1999. IJCNN'99. International Joint Conference on* (Vol. 5, pp. 3255-3259). IEEE.

Sagar, V. K., Ngo, D. B. L., & Foo, K. C. K. (1995, October). Fuzzy feature selection for fingerprint identification. In *Security Technology, 1995. Proceedings. Institute of Electrical and Electronics Engineers 29th Annual 1995 International Carnahan Conference on* (pp. 85-90). IEEE.

Sahoo, S., Choubisa, T., & Mahadeva Prasanna, S. (2012). Multimodal Biometric Person Authentication : A Review. *IETE Technical Review*, *29*(1), 54. DOI: https://doi.org/10.4103/0256-4602.93139.

Saini, A. (2012). Image enhancement techniques for fingerprint images. *International Journal of Emerging Trends and Technology in Computer Science*, *1*(3), 215-17.

Saini, R., & Narinder, R. (2014). Comparison of Various Biometric Methods. *International Journal of Engineering Science & Technology*, *2*(I), 24–30.

Schmeh, K. (2003) Cryptography and Public Key Infrastructure on the Internet, JohnWiley & Sons.

Schmid, C., & Mohr, R. (1997). Local grayvalue invariants for image retrieval. *IEEE transactions on pattern analysis and machine intelligence*, *19*(5), 530-535.

Sengee, N., & Choi, H. K. (2008). Brightness preserving weight clustering histogram equalization. *IEEE Transactions on Consumer Electronics*, 54(3), 1329–1337. DOI: https://doi.org/10.1109/TCE.2008.4637624.

Sepasian, M., Balachandran, W., & Mares, C. (2008, October). Image enhancement for fingerprint minutiae-based algorithms using CLAHE, standard deviation analysis and sliding neighborhood. In *Proceedings of the World congress on Engineering and Computer Science* (pp. 22-24).

Setlak, D. R. (2005). Advances in biometric fingerprint technology are driving rapid adoption in consumer marketplace. *Retrieved December*, *13*.

Sherlock, B. G., Monro, D. M., & Millard, K. (1994). Fingerprint enhancement by directional Fourier filtering. *IEE Proceedings-Vision, Image and Signal Processing*, *141*(2), 87-94.

Shi, Z., & Govindaraju, V. (2006). A chaincode based scheme for fingerprint feature extraction. *Pattern Recognition Letters*, *27*(5), 462-468.

Shin, J. H., Hwang, H. Y., & Chien, S. I. (2006). Detecting fingerprint minutiae by run length encoding scheme. *Pattern recognition*, *39*(6), 1140-1154.

Short, N. J., Hsiao, M. S., Abbott, A. L., & Fox, E. A. (2011). Latent fingerprint segmentation using ridge template correlation. 4th International Conference on Imaging for Crime Detection and Prevention 2011 (ICDP 2011), P28–P28. DOI: https://doi.org/10.1049/ic.2011.0125.

Sirovich, L., & Kirby, M. (1987). Low-dimensional procedure for the characterization of human faces. *Josa a*, *4*(3), 519-524.

Spillane, R. (1975). *Keyboard apparatus for personal identification. IBM Technical Disclosure Bulletin*. Tech. Rep. 17.

Stoney, D. A., & Thornton, J. I. (1986). A critical analysis of quantitative fingerprint individuality models. *Journal of Forensic Science*, *31*(4), 1187-1216.

Subhra, M. and Venkata, D. (2008). Biometric Security Using FingerPrint Recognition, *University of California, San Diego*, 3.

Sujan, V. A., & Mulqueen, M. P. (2002). Fingerprint identification using space invariant transforms. *Pattern Recognition Letters*, *23*(5), 609-619.

Sun, X. and Ai, Z. (1996) Automatic feature extraction and recognition of fingerprint images, Proceeding of ICSP'96, Beijing, Pp.1086-1089.

Thai, D. H., Huckemann, S., & Gottschlich, C. (2016). Filter design and performance evaluation for fingerprint image segmentation. PLoS ONE, 11(5). DOI: https://doi.org/10.1371/journal.pone.0154160.

Tiwari, K., & Gupta, P. (2015). An efficient technique for automatic segmentation of fingerprint ROI from digital slap image. Neurocomputing, 151(P3), 1163–1170. DOI: https://doi.org/10.1016/j.neucom.2014.04.086.

Toledeno, D.T., Pozo, F.R., Trapote, A.H. and Gomez, L.H. (2006) Usability evaluation of multi-modal biometric verification systems, Interacting with Computers, Elsevier Science Inc., New York, USA, 18(5),1101-1122.

Trauring, M. (1963). Automatic comparison of finger-ridge patterns. *Nature*, *197*(4871), 938-940.

Tulyakov, S., Farooq, F., Mansukhani, P., & Govindaraju, V. (2007). Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recognition Letters*, *28*(16), 2427-2436.

Turk, M. A., & Pentland, A. P. (1991, June). Face recognition using eigenfaces. In *Computer Vision and Pattern Recognition, 1991. Proceedings CVPR'91., IEEE Computer Society Conference on* (pp. 586-591). IEEE.

Tuyls, P., Akkermans, A. H., Kevenaar, T. A., Schrijen, G. J., Bazen, A. M., & Veldhuis, R. N. (2005, July). Practical biometric authentication with template protection. In *AVBPA* (Vol. 3546, pp. 436-446).

Uludag, U., & Jain, A. (2006, June). Securing fingerprint template: Fuzzy vault with helper data. In *Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06. Conference on* (pp. 163-163). IEEE.

Uludag, U., & Jain, A. K. (2004, January). Attacks on biometric systems: a case study in fingerprints. In *Proceedings of SPIE* (Vol. 5306, pp. 622-633).

Vacca, J.R. (2007) Biometric technologies and verification systems, Chapter 1, Biometric technologies for personal identification, Elsevier Science and Technology, P.24

Varun Shenoy, & Aithal P. S., (2016). ABCD Analysis of On-line Campus Placement Model, IRA-International Journal of Management & Social Sciences, 5(2), 227-244. DOI: http://dx.doi.org/10.21013/jmss .v5.n2.p3.

Venter, J.C., et al. (2001). The sequence of he human genome. Science, 291(5507), 1304-51.

Vetro, A., & Memon, N. (2007, August). Biometric system security. In *Tutorial presented at Second International Conference on Biometrics, Seoul, South Korea*.

Vuppala, S. K., Grigorescu, S. M., Ristic, D., & Graser, A. (2007, June). Robust color object recognition for a service robotic task in the system FRIEND II. In *Rehabilitation Robotics, 2007. ICORR 2007. IEEE 10th International Conference on* (pp. 704-713). IEEE.

W. F. Leung, S. H. Leung, W. H. Lau, A. Luk, “Fingerprint Recognition using Neural Networks”, in Proc. IEEE Workshop on Neural Networks for Signal Processing, 1991, pp. 226-235.

Wahab, A., Chin, S., & Tan, E. (1998). Novel approach to automated fingerprint recognition. *IEE Proceedings - Vision, Image and Signal Processing*. DOI: https://doi.org/10.1049/ip-vis:19981809.

Weaver, A. C. (2006). Biometric Authentication. *Computer*, *39*(2), 96–97. DOI: https://doi.org/10.1109/MC.2006.47.

Wentworth, B., & Wilder, H. H. (1918). Personal identification. *Boston: RG Badger*.

Wilson, C. L., Candela, G. T., & Watson, C. I. (1994). Neural network fingerprint classification. *Journal of Artificial Neural Networks*, *1*(2), 203-228.

Wongchoosuk, C., Youngrod, T., Phetmung, H., Lutz, M., Puntheeranurak, T., & Kerdcharoen, T. (2011). Identification of people from armpit odor region using networked electronic nose. In *2011 Defense Science Research Conference and Expo, DSR 2011*. DOI: https://doi.org/10.1109/DSR.2011.6026826.

Wongsritong, K., Kittayaruasiriwat, K., Cheevasuvit, F., Dejhan, K., & Somboonkaew, A. (1998, November). Contrast enhancement using multipeak histogram equalization with brightness preserving. In *Circuits and Systems, 1998. IEEE APCCAS 1998. The 1998 IEEE Asia-Pacific Conference on* (pp. 455-458). IEEE.

Woodward, J.D., Orlands, N.M. and Higgins, P.T. (2003) Biometrics, McGraw Hill Osborne, New York.

Wu C., Tulyakov S. and Govindaraju V. (2007). Robust point-based Feature Fingerprint Segmentation Algorithm, ICB (2007), Pp. 1095-1104.

X. You, B. Fang, V. Y. Y. Tang, and J. Huang, “ Multiscale approach for thinning ridges of fingerprint”, in Proc. Second Iberian Conference on Pattern Recognition and Image Analysis, volume LNCS 3523, 2005, pp. 505–512.

Xia, X., & O'Gorman, L. (2003). Innovations in fingerprint capture devices. *Pattern Recognition*, *36*(2), 361-369.

Xiao, Q., & Raafat, H. (1991). Fingerprint image postprocessing: a combined statistical and structural approach. *Pattern Recognition*, *24*(10), 985-992.

Xu, J., Zhang, Z., Xiao, X., Yang, Y., Yu, G., & Winslett, M. (2013). Differentially private histogram publication. *VLDB Journal*, 22(6), 797–822. DOI: https://doi.org/10.1007/s00778-013-0309-y.

Xue, J., & Li, H. (2012, July). Fingerprint image segmentation based on a combined method. In Virtual Environments Human-Computer Interfaces and Measurement Systems (VECIMS), 2012 IEEE International Conference on (pp. 207-208). IEEE.

Yager, N., & Amin, A. (2004). Fingerprint verification based on minutiae features: a review. *Pattern Analysis and Applications*, *7*(1), 94-113.

Yang, J., Liu, L., Jiang, T., & Fan, Y. (2002, August). An improved method for extraction of fingerprint features. In *Proc. the 2nd Int. Conf. Image and Graphics, Anhui, PR China* (pp. 552-558).

Yang, J., Liu, L., Jiang, T., & Fan, Y. (2003). A modified Gabor filter design method for fingerprint image enhancement. *Pattern Recognition Letters*, *24*(12), 1805-1817.

Yıldırım, N., & Varol, A. (2015, May). Android based mobile application development for web login authentication using fingerprint recognition feature. In *Signal Processing and Communications Applications Conference (SIU), 2015 23th* (pp. 2662-2665). IEEE.

You, H. Y., & Wang, S. C. (2003). Morphological Thinning Algorithm With Application to Locating PCB [J]. *Techniques of Automation and Applications*, *10*, 005.

Young, J. R., & Hammon, R. W. (1989). *U.S. Patent No. 4,805,222*. Washington, DC: U.S. Patent and Trademark Office.

Zhang, J., Lai, R., & Kuo, C. C. J. (2012). Latent fingerprint detection and segmentation with a directional total variation model. In Proceedings - International Conference on Image Processing, ICIP (pp. 1145–1148). DOI: https://doi.org/10.1109/ICIP.2012.6467067.

Zhang, T. Y., & Suen, C. Y. (1984). A fast parallel algorithm for thinning digital patterns. *Communications of the ACM*, *27*(3), 236-239.

Zhang, W., & Wang, Y. (2002). Core-based structure matching algorithm of fingerprint verification. In *Pattern Recognition, 2002. Proceedings. 16th International Conference on* (Vol. 1, pp. 70-74). IEEE.

Zhang, Y., & Xiao, Q. (2006, July). An optimized approach for fingerprint binarization. In *Neural Networks, 2006. IJCNN'06. International Joint Conference on* (pp. 391-395). IEEE.

Zhao, F., & Tang, X. (2007). Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction. *Pattern Recognition*, 40(4), 1270-1281.

Zhu, E., Yin, J., Hu, C. and Zhang, G. (2006) A systematic method for fingerprint ridge orientation estimation and image segmentation, Pattern Recognition, Vol. 39, No.8, Pp. 1452-1472.

Ziaei, A., Yeganeh, H., Faez, K., & Sargolzaei, S. (2008). A novel approach for contrast enhancement in biomedical images based on histogram equalization. In *International Conference on Computer and Communication Engineering 2008* (Vol. 1, pp. 855–858). DOI: https://doi.org/10.1109/BMEI.2008.300.

Zimmerman, J. B., Pizer, S. M., Staab, E. V., Perry, J. R., Mccartney, W., & Brenton, B. C. (1988). An Evaluation of the Effectiveness of Adaptive Histogram Equalization for Contrast Enhancement. *IEEE Transactions on Medical Imaging*, 7(4), 304–312. DOI: https://doi.org/10.1109/42.14513.

Ziou, D. and Tabbone, S. (1998). Edge Detection Techniques - An Overview. *Journal of Pattern Recognition and Image Analysis*, 8, 537-559.

## Annexure 1: Sample Source code of Implementation in MATLAB 2015a

Source code for Fingerprint Hash code Generation using Euclidean Distance using MATLAB 2015a (mainGUI.m)

```
function varargout = mainGUI(varargin)
% MAINGUI MATLAB code for mainGUI.fig
%      MAINGUI, by itself, creates a new MAINGUI or raises the existing
%      singleton*.
%     H = MAINGUI returns the handle to a new MAINGUI or the handle to
%      the existing singleton*.
%%      MAINGUI('CALLBACK',hObject,eventData,handles,...) calls the local
%      function named CALLBACK in MAINGUI.M with the given input arguments.
%%      MAINGUI('Property','Value',...) creates a new MAINGUI or raises the
%      existing singleton*.  Starting from the left, property value pairs are
%      applied to the GUI before mainGUI_OpeningFcn gets called.  An
%      unrecognized property name or invalid value makes property application
%      stop.  All inputs are passed to mainGUI_OpeningFcn via varargin.
%     *See GUI Options on GUIDE's Tools menu.  Choose "GUI allows only one
%      instance to run (singleton)".
% % See also: GUIDE, GUIDATA, GUIHANDLES
 % Edit the above text to modify the response to help mainGUI
 % Last Modified by GUIDE v2.5 06-Jan-2018 00:36:50
 % Begin initialization code - DO NOT EDIT

gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @mainGUI_OpeningFcn, ...
                   'gui_OutputFcn',  @mainGUI_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
if nargin && ischar(varargin{1})
   gui_State.gui_Callback = str2func(varargin{1});
end

if nargout
   [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
   gui_mainfcn(gui_State, varargin{:});
end
% End initialization code - DO NOT EDIT
% --- Executes just before mainGUI is made visible.
function mainGUI_OpeningFcn(hObject, eventdata, handles, varargin)
```

```
% This function has no output args, see OutputFcn.
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% varargin   command line arguments to mainGUI (see VARARGIN)
 % Choose default command line output for mainGUI
handles.output = hObject;
 % Update handles structure
guidata(hObject, handles);
 % UIWAIT makes mainGUI wait for user response (see UIRESUME)
% uiwait(handles.figure1);

 % --- Outputs from this function are returned to the command line.
function varargout = mainGUI_OutputFcn(hObject, eventdata, handles)
% varargout  cell array for returning output args (see VARARGOUT);
% hObject    handle to figure
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Get default command line output from handles structure
varargout{1} = handles.output;

 % --- Executes on button press in pushbutton1.
function pushbutton1_Callback(hObject, eventdata, handles)
% hObject    handle to pushbutton1 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

global in trainfvcb12 binary_image1 label biT2 T2 test
[fi,p]=uigetfile('\Fingerprint_Minutiae_Extraction\*','.*');
in=imread([p fi]);
in=imresize(in,[256 256]);
%in=imrotate(in,3);
%in =imtranslate(in,[2,2]);
%train=trainfvcb12(1:40,:);
%for i=1:40
 %   if i>=1 & i<=8
      % label(i)=1;
  %  elseif i>8 & i<=16
      % label(i)=2;
   % elseif i>16 & i<=24
       %label(i)=3;
   % elseif i>24 & i<=32
```

```
    %    label(i)=4;
    %elseif i>32 & i<=40
     %   label(i)=5;
    %end
%end
axes(handles.axes1)
imshow(in)

% hObject    handle to pushbutton3 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
% --- Executes on button press in pushbutton4.
function pushbutton4_Callback(hObject, eventdata, handles)
% hObject    handle to pushbutton4 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
load trainfvcb12.mat
stepspro1='1) Start wampserver->In Wamp Server select phpMyAdmin-->Click Database Tab and create a new database with name fingerprint1->Create a new table on database fingerprint1->type name as trainhash1 and number of fiel as 2-->Two fields were created-->Field Name and length as id and 10 and 2nd Field Name and length as hash and 100->in 1st field selet type as INT and for 2nd field select type as VARCHAR';
stepspro2='2)APPS-->DATABASE CONNECTIVITY AND REPORTING-->Database Explorer-->Connect to DataSourceDialogue box will appear-->Click cancel in that dialogue box--> Click new and Select JDBC';
stepspro3='3)Create a new JDBC Data Source dialogue box will appear-->In that dialogue box Select MySQL in Vendor-->fill the Data Source Name(any vaiable)->Server Name(loacalhost)->Username(root)->Database(type database name which was in the wamp server)->click Test button and then click save button';
 set(handles.edit1,'string',stepspro1)
  set(handles.edit2,'string',stepspro2)
   set(handles.edit3,'string',stepspro3)
global trainfvcb12

function edit1_Callback(hObject, eventdata, handles)
% hObject    handle to edit1 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: get(hObject,'String') returns contents of edit1 as text
%        str2double(get(hObject,'String')) returns contents of edit1 as a double
 % --- Executes during object creation, after setting all properties.
function edit1_CreateFcn(hObject, eventdata, handles)
```

```
% hObject    handle to edit1 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called
 % Hint: edit controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if                  ispc                &&                  isequal(get(hObject,'BackgroundColor'),
get(0,'defaultUicontrolBackgroundColor'))
   set(hObject,'BackgroundColor','white');
end

function edit2_Callback(hObject, eventdata, handles)
% hObject    handle to edit2 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: get(hObject,'String') returns contents of edit2 as text
%        str2double(get(hObject,'String')) returns contents of edit2 as a double

% --- Executes during object creation, after setting all properties.
function edit2_CreateFcn(hObject, eventdata, handles)
% hObject    handle to edit2 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called

% Hint: edit controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if                  ispc                &&                  isequal(get(hObject,'BackgroundColor'),
get(0,'defaultUicontrolBackgroundColor'))
   set(hObject,'BackgroundColor','white');
end
 function edit3_Callback(hObject, eventdata, handles)
% hObject    handle to edit3 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)

% Hints: get(hObject,'String') returns contents of edit3 as text
%        str2double(get(hObject,'String')) returns contents of edit3 as a double

% --- Executes during object creation, after setting all properties.
function edit3_CreateFcn(hObject, eventdata, handles)
% hObject    handle to edit3 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    empty - handles not created until after all CreateFcns called
```

```
% Hint: edit controls usually have a white background on Windows.
%       See ISPC and COMPUTER.
if ispc && isequal(get(hObject,'BackgroundColor'),
get(0,'defaultUicontrolBackgroundColor'))
   set(hObject,'BackgroundColor','white');
end

% --- Executes on button press in pushbutton5.
function pushbutton5_Callback(hObject, eventdata, handles)
% hObject    handle to pushbutton5 (see GCBO)
% eventdata  reserved - to be defined in a future version of MATLAB
% handles    structure with handles and user data (see GUIDATA)
global in trainfvcb12 binary_image1 label biT2 T2 test
lmax=max(in(:));
nlmax=0;
for i=1:size(in,1)
   for j=1:size(in,2)
      if in(i,j)==lmax
         nlmax=nlmax+1;
      end
   end
end
pdfmax=nlmax./(i.*j);
lmin=min(in(:));
nlmin=0;
for i=1:size(in,1)
   for j=1:size(in,2)
      if in(i,j)==lmin
         nlmin=nlmin+1;
      end
   end
end
pdfmin=nlmin./(i.*j);
alpha=0.2;
for i=1:size(in,1)
   nl=0;
   l=min(in(i,:));
        for j=1:size(in,2)
       if l==in(i,j)
         nl=nl+1;
      end
   end
```

```
   pdfl(i)=nl./(i.*j);
   pdfwl(i)=(pdfmax.*(((pdfl(i)-pdfmin)./(pdfmax-pdfmin)).^alpha));
end
pdfwl(~isfinite(pdfwl))=0;
cdfwl=zeros(1,size(in,1));
for i=1:size(pdfwl,2)
          cdfwl(i)=pdfwl(i)./sum(pdfwl(:));
end
 cdfwl(isnan(cdfwl))=0;
k=1;
for i=1:size(in,1)
    for j=1:size(in,2)
      xz=round((1-cdfwl(k)),6);
    if ~isreal(xz)
    xz=abs(real(xz));
    end
       pow=double((lmax.*((in(i,j)./lmax))));
       power1=pow^xz;
      power1=uint8(power1);
      T1(i,j)=power1;
     end
    k=k+1;
end
biT2=im2bw(T1);
axes(handles.axes4)
imshow(T1)
biT2=(1-biT2);
A=bwdist(biT2);
B=unique(A,'sorted');
disttot=0;
meantot=0;
stddevtot=0;
for i=1:size(B,1)
   disttot=disttot+B(i);
end
meantot=mean2(B);
stddevtot=std(B);
tfsgabfea=[disttot meantot stddevtot];
test=tfsgabfea;
mainGUI3
```

# LIST OF PUBLICATIONS

**Journal Papers (31):**


[1] Krishna Prasad, K. & Aithal, P.S. (2017). A Critical Study on Fingerprint Image Sensing and Acquisition Technology. *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, 1(2), 86-92. DOI: http://dx.doi.org/10.5281/zenodo.1130581.

[2] Krishna Prasad, K. & Aithal, P.S. (2017). A Conceptual Study on Image Enhancement Techniques for Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(1), 63-72. DOI: http://dx.doi.org/10.5281/zenodo.831678.

[3] Krishna Prasad, K. & Aithal, P.S. (2017). Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 2(2), 8-19. DOI: http://dx.doi.org/10.5281/zenodo.835608.

[4] Krishna Prasad, K. & Aithal, P.S. (2017). Fingerprint Image Segmentation: A Review of State of the Art Techniques. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 2(2), 28-39. DOI: http://dx.doi.org/10.5281/zenodo.848191.

[5] Krishna Prasad, K. & Aithal, P.S. (2017). A Novel Method to Contrast Dominating Gray Levels during Image contrast Adjustment using Modified Histogram Equalization. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(2), 27-39. DOI: http://dx.doi.org/10.5281/zenodo.896653.

[6] Krishna Prasad, K. & Aithal, P.S. (2017).Two Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(2), 51-65. DOI: http://dx.doi.org/10.5281/zenodo.1037627.

[7] Krishna Prasad, K. & Aithal, P.S. (2017). A conceptual Study on Fingerprint Thinning Process based on Edge Prediction. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(2), 98-111. DOI: http://dx.doi.org/10.5281/zenodo.1067110.

[8] Krishna Prasad, K. & Aithal, P.S. (2017). A Study on Fingerprint Hash Code Generation using Euclidean Distance for Identifying a User. International Journal of Management, Technology, and Social Sciences (IJMTS), 2(2), 116-126. DOI: http://doi.org/10.5281/zenodo.1133545.

[9] Krishna Prasad, K. & Aithal, P.S. (2018). An Alternative Approach to Fingerprint Hash Code Generation based on Modified Filtering Techniques**.** *International Journal of Innovative Research in Management, Engineering and Technology*, 2(12), 1-13. DOI: **IJIRMET1602012001**.

[10] Krishna Prasad, K. & Aithal, P. S. (2018). A Study on Multifactor Authentication Model Using Fingerprint Hash Code, Password and OTP. *International Journal of Advanced Trends in Engineering and Technology*, 3(1), 1-11. DOI : http://doi.org/10.5281/zenodo.1135255.

[11] Krishna Prasad, K. & Aithal, P. S. (2018). A Study on Fingerprint Hash Code Generation Based on MD5 Algorithm and Freeman Chain Code. *International Journal of Computational Research and Development*. 3(1), 13-22. DOI: http://doi.org/10.5281/zenodo.1144555.

[12] Krishna Prasad, K. & Aithal, P.S. (2018). A Comparative Study on Fingerprint Hash Code, OTP, and Password based Multifactor Authentication Model with an Ideal System and Existing Systems. *International Journal of Applied and Advanced Scientific Research,* 3(1), 18-32. DOI: http://doi.org/10.5281/zenodo.1149587.

[13] Krishna Prasad, K. & Aithal, P. S. (2018). A Novel Tuning Based Contrast Adjustment Algorithm for Grayscale Fingerprint Image. *Saudi Journal of Engineering and Technology (SJEAT),* 3(1), 15-23. DOI: http://10.21276/sjeat.2018.3.1.3.

[14] Krishna Prasad, K. & Aithal, P.S. (2018). ABCD Analysis of Fingerprint Hash Code, Password and OTP based Multifactor Authentication Model. *Saudi Journal of Business and Management Studies,* 3(1), 65-80. DOI: http://10.21276/sjbms.2018.3.1.10.

[15] Krishna Prasad, K. & Aithal, P.S. (2018). A Study on Pre and Post Processing of Fingerprint Thinned Image to Remove Spurious Minutiae from Minutiae Table**.** *International Journal of Current Research and Modern Education*, 3(1), 197-212. DOI: http://doi.org/10.5281/zenodo.1174543.

**Related Area Journals:**

[16] Krishna Prasad, K. and Aithal, P. S. (2017). A Conceptual Study on User Identification and Verification Process Using Face Recognition Techniques. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(1), 6-17. DOI: http://doi.org/10.5281/zenodo.810343.

[17] Krishna Prasad, K. and Aithal, P. S. (2017). A Study on Enhancing Mobile Banking Services using Location based Authentication. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 1(1), 48-60. DOI: http://doi.org/10.5281/zenodo.583230.

**Other Area Journals:**

[18] Krishna Prasad, K. and Aithal, P. S. (2017). A Study on Online Education Model Using Location Based Adaptive Mobile Learning. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(1), 36-44. DOI: http://doi.org/10.5281/zenodo.820457.

[19] Krishna Prasad, K. and Aithal, P. S. (2017). A Customized and Flexible Ideal Mobile Banking System Using 5G Technology. *International Journal of Management, Technology, and Social Sciences (IJMTS),*1(1), 25-37. DOI: http://doi.org/10.5281/zenodo.820457.

[20] Krishna Prasad K. & Dr. Aithal, P.S. (2016). The Growth of 4G Technologies in India-Challenges and Opportunities. *International Journal of Management, IT and Engineering (IJMIE),* 6(1), 543 - 551, (January 2016) ISSN: 2249-0558, I.F. 5. 299. DOI : http://doi.org/10.5281/zenodo.161130.

[21] Krishna Prasad K. & Dr. Aithal, P. S. (2016). Changing Perspectives of Mobile Information Communication Technologies towards Customized and Secured Services Through 5G & 6G. *International Journal of Engineering Research and Modern Education (IJERME),* ISSN (Online): 2455 - 4200 (www.rdmodernresearch.com) 1(2), 2016, 210-224.

[22] Krishna Prasad, K. & Aithal, P. S. (2016). An Online Comparative Study on 4G Technologies Service Providers in India. *International Journal of Advanced Trends in Engineering and Technology (IJATET).* 1(1), 96-101. DOI: http://doi.org/10.5281/zenodo.240269.

[23] K. Krishna Prasad (2016). A Conceptual Study on Changing Perspective of Information Technology Enabled Employment Services Through Freelance Jobs. *International Journal of Engineering Research and Modern Education (IJERME),*1(1), 709-714.

[24] Sridhar Acharya P & Krishna Prasad K. (2016). Modification in the Design of ECU of a Motor Vehicle to Control the Speed Depending on the Density of Vehicle. *International Journal of Scientific Research and Modern Education (IJSRME),* 1(1), 2016, 270-274.

[25] K. Krishna Prasad (2016). An Empirical Study on role of Vedic Mathematics in Improving the Speed of Basic Mathematical Operations. *International Journal of Management, IT and Engineering,* 6(1), 161-171.

[26] K. Krishna Prasad (2016). Blog Based Self Verification And Self Development Curriculum Model-A Novel Approach To Student Centric Learning. *International journal of Scientific Research and Modern Education, 1(1),* 435-441.

[27] M. D. Pradeep & K. Krishna Prasad (2016). Modern Paradigm Shift In Social Work Profession Through Technology - New Dimension in Social Work Education, *International journal of Current Research and Modern Education,* 1(1), 433-443.

[28] K. Krishna Prasad and P.S. Aithal (2015). Mobile System for Customized and Ubiquitous Learning by 4G/5G. *International Journal of Management, IT and Engineering (IJMIE),* 5(7), 63-71.

[29] K. Krishna Prasad and P.S. Aithal (2015), Massive Growth of Banking Technology with The Aid Of 5G Technologies. *International Journal of Management, IT and Engineering (IJMIE),* 5(7), 616-627.

[30] K. Krishna Prasad & S. Sumana (2015). Effect of Social Networking Site on Students' Academic Performance in SIMS, Mangalore: An Investigative Study. GE-International journal of Management Research (GE-IJMR), 3(3), 39–48.

[31] K. Krishna Prasad (2015). An empirical study on apt alumni association in higher education institutions to enhance brand name of the institution. *International Journal of Multidisciplinary Research and Development (IJMRD),* 2(4), 69-74.

**Conference Papers (18)**

[1] K. Krishna Prasad & Dr. P. S. Aithal, An Alternative Approach to Fingerprint Hash Code Generation based on Modified Filtering Techniques. International Conference on Advances in Sciences, Engineering & Management (ICASEM-2018), 21st January 2018, Mangaluru, India. ISBN No.: 9788193221396.

[2] K. Krishna Prasad & Dr. P. S. Aithal, A Study on Euclidean Distance Based Hash Code creation for A Fingerprint Image. National Conference on Innovation and Implications in Information Technology, Management, Social Sciences and Education, 23rd December 2017, SIMS, Mangalore, India. ISBN No.:978-93-5300-723-2.

[3] K. Krishna Prasad & Dr. P. S. Aithal, A Study on Existing Fingerprint Image Segmentation Algorithms. National Conference on Implications of Research in Banking, Management, IT, Education and Social Sciences, 18-19th August 2017**,** SIMS Mangalore, India. ISBN No.: 978-93-5281-474-9.

[4] K. Krishna Prasad & Dr. P. S. Aithal, Fingerprint Image Sensing Technology: A Review of State of the Art Methods. National Conference on Balancing Human Work Life, 30th October 2017**,** SIMS Mangalore, India. ISBN No.: 978-93-5291-481-4.

**Related Area Conference Papers:**

[5] K. Krishna Prasad & Dr. P.S. Aithal, A Literature Survey On Face Recognition Techniques: Applications To User Identification And Verification Process. Current Developments in Computer Science, IT & its Impact on Management, Social Sciences and Education. 26th November 2016, SIMS Mangalore, India. ISBN No.: 978-93-5265-655-4.

**[6]** K. Krishna Prasad & Dr. P. S. Aithal, A Study on Enhancing Mobile Banking Services using location based Authentication**.** National Conference on Reinventing Opportunities in Management, IT, and Social Sciences-MANEGMA, 23-24th April 2017**,** SIMS Mangalore, India. ISBN No.: 978-93-5268-756-5.

[7] K. Krishna Prasad & S. Sumana, "An Improved Multi Phase Security solutions to ATM Banking Systems" in National Conference "E-Learning, E-Business and E-Governance" on 24 January, 2015 at Srinivas Institute of Management Studies, Pandeshwar, Mangalore. ISBN No. 978-81-929306-4-0.

**Other Area Conference Papers:**

**[8]** K. Krishna Prasad & Dr. P. S. Aithal, A Study on Online Education Model using Location Based Adaptive Mobile Learning. National Conference on Emerging Trends in Educational Innovations, 23-24th June 2017**,** SIMS Mangalore, India. ISBN No.: 978-93-5279-403-4.

[9] K. Krishna Prasad, Blog based Self Verification and Self-development Curriculum Model - A Novel Approach to Student Centric Learning, Curriculum Design and Development for Student – Centric Learning, SIMS, Mangalore, India. (March 2016), ISBN No.: 978-81-929306-9-5.

[10] Pradeep M. D., Krishna Prasad K., Modern Paradigm shift in Social Work Profession through Technology- New Dimension in Social Work Education. Curriculum Design and Development for Student – Centric Learning, SIMS, Mangalore, India. (March 2016), ISBN No.: 978-81- 929306-9-5.

[11] K. Krishna Prasad (2016). A Conceptual Study on Changing Perspective of Information Technology enabled Employment Services through Freelance Jobs. The Changing Perspectives of Management, IT and Social Sciences in the Contemporary Environment, SIMS, Mangalore, India. (May, 2016), ISBN No.: 978-93-5265-653-0.

[12] K. Krishna Prasad, P. S. Aithal, An Online Comparative Study On 4G Technologies Service Providers In India, Innovations and Transformations in Banking, Management, IT, Education and Social Sciences, (August, 2016), ISBN No.: 978-93-5265-656-1.

[13] K. Krishna Prasad, P. S. Aithal, A Customized And Flexible Ideal Mobile Banking System Using 5G Technology, Innovations and Transformations in Banking, Management, IT, Education and Social Sciences, (August, 2016), ISBN No.: 978-93-5265-656-1.

[14] K. Krishna Prasad & P.S. Aithal, "Mobile System for Customized and Ubiquitous Learning by 4G/5G" Proceedings of National Conference", "Recent Advances in IT, Management and Social Sciences", Manegma - 2015, Mangalore on 23rd April, 2015, ISBN No. 978-81-929306-6-4.

[15] K. Krishna Prasad & P.S. Aithal "Massive Growth of Banking Technology with the Aid of 5G Technologies" Proceedings of National Conference "Recent Advances in IT, Management and Social Sciences", Manegma - 2015, Mangalore on 23 April, 2015, ISBN No. 978-81-929306-6-4.

[16] P. S. Aithal & K. Krishna Prasad "The Growth of 4G Technologies In India-Challenges and Opportunities" Proceedings of National Conference "Innovative Practices in IT, Management, Education and Social Sciences" October 17th, 2015, ISBN No. 978-81-929306-8-8.

[17] Krishna Prasad, "En Empirical study on Apt Alumni Association in Higher Education Institutions to Enhance Brand name of the Institution" in International conference on Quality Through Innovation on 19th & 20th February, 2015 at Anna University, Chennai.

[18] K. Krishna Prasad "An Empirical Study on role of Vedic Mathematics in Improving the Speed of Basic Mathematical Operations" Proceedings of National Conference "Innovative practices in IT, Management, Education and Social Sciences" October 17, 2015, ISBN No. 978-81-929306-8-8.

**Google scholar Page (**https://scholar.google.com/citations?user=g2I5sKEAAAAJ )

| TITLE | CITED BY | YEAR |
|---|---|---|
| A Conceptual Study on Image Enhancement Techniques for Fingerprint Images<br>K Krishna Prasad, PS Aithal<br>International Journal of Applied Engineering and Management Letters (IJAEML ... | 12 | 2017 |
| Massive Growth Of Banking Technology With The Aid Of 5G Technologies<br>KKPPS Aithal<br>International Journal of Management, IT and Engineering (IJMIE) 5 (7), 616-627 | 12 * | 2015 |
| Fingerprint Image Segmentation: A Review of State of the Art Techniques<br>K Krishna Prasad, PS Aithal | 8 | 2017 |
| Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image<br>K Krishna Prasad, PS Aithal<br>International Journal of Management, Technology, and Social Sciences (IJMTS ... | 8 | 2017 |

| | | |
|---|---|---|
| A Novel Method to Control Dominating Gray Levels During Image Contrast Adjustment Using Modified Histogram Equalization<br>K Krishna Prasad, PS Aithal | 7 | 2017 |
| The Growth of 4G Technologies in India - Challenges and Opportunities<br>PSA K. Krishna Prasad<br>International Journal of Management, IT and Engineering 6 (1), 543-551 | 6 | 2016 |
| Mobile system for Customized and Ubiquitous Learning by 4G/5G<br>PSA K Krishna Prasad<br>nternational Journal of Management, IT and Engineering (IJMIE) 5 (7), 63-71 | 6 | 2015 |
| A Critical Study on Fingerprint Image Sensing and Acquisition Technology<br>K Krishna Prasad, PS Aithal | 4 | 2017 |
| Two Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images<br>K Krishna Prasad, PS Aithal | 4 | 2017 |
| A Customized and Flexible Ideal Mobile Banking System Using 5g Technology<br>PS K. Krishna Prasad., Aithal<br>International Journal of Management, Technology, and Social Sciences 2 (1 ... | 4 * | 2017 |
| A Study on Enhancing Mobile Banking Services Using Location Based Authentication<br>KKPDPS Aithal<br>International Journal of Management, Technology, and Social Sciences (IJMTS ... | 4 * | 2017 |
| A Conceptual Study on Fingerprint Thinning Process based on Edge Prediction<br>K Krishna Prasad, PS Aithal | 3 | 2017 |
| A Conceptual Study on User Identification and Verification Process Using Face Recognition Techniques<br>K Krishna Prasad, PS Aithal | 3 | 2017 |
| An Online Comparative Study on 4G Technologies Service Providers in India<br>PSA K. Krishna Prasad<br>International Journal of Advanced Trends in Engineering and Technology ... | 3 | 2016 |
| Blog Based Self Verification And Self Development Curriculum Model-A Novel Approach To Student Centric Learning<br>K Krishna Prasad<br>Browser Download This Paper | 2 | 2016 |
| Modern Paradigm Shift in Social Work Profession Through Technology - New Dimension in Social Work Education<br>PMDKK Prasad<br>International Journal of Current Research and Modern Education (IJCRME) 1 (1 ... | 2 * | 2016 |
| Changing Perspectives of Mobile Information Communication Technologies towards Customized and Secured Services through 5G & 6G<br>KKPDPS Aithal<br>International Journal of Engineering Research and Modern Education (IJERME ... | 2 * | 2016 |
| A Study on Multifactor Authentication Model Using Fingerprint Hash Code, Password and OTP<br>K Krishna Prasad, PS Aithal | 1 | 2018 |

## CURRICULUM VITAE

Mr. Krishna Prasad K. is belonging to Mangaluru, India born on 25/05/1983. He received his M.Sc (5 years Integrated Course) degree in Information Science from Mangalore University in 2006, M.Phil Degree in Computer Science from Madurai Kamaraj University in 2009 and M.Tech in Information Technology from Karnataka State Open University (KSOU) in 2013 respectively. Presently he is doing his part-time Ph.D. in the field of Biometric Fingerprint Hash code generation methods in Srinivas University, Mangaluru, India. Since June 2006, he is working in Srinivas Institute of Management Studies, Pandeshwar, and designated as Assistant Professor in 2014. He is having 12 years of teaching experience in different Computer Science subjects for BCA and MCA courses.

Currently, he is working as Assistant Professor in College of Computer and Information Sciences, Srinivas University, City campus, Pandeshwar, Mangaluru, India. He has conducted many Guest Lectures in Vedic Mathematics and Shortcuts tricks for competitive examinations in and around Dakshina Kannada District of Karnataka State, India. His research interest includes Fingerprint Hash Code Generation Methods and Multifactor Authentication Model. He was the member of BOE of BCA in Mangalore University for six months in 2013 and for one year in 2017and Paper setter and Evaluator at Mangalore University.

Mr. Krishna Prasad K. has published 31 research papers in refereed international journals with more than 85 Google Scholar citations and Ranked 29 in Elsevier SSRN e-library journal papers of last 12 months updated on 01 March 2018. He has also presented 18 papers in conferences, out of which 2 were International Conferences and remaining were National Conferences.

# NITTE

**(Deemed to be University)**
(Established under Sec. (3) of UGC Act, 1956)
Placed under Category 'A' by MHRD, Govt. of India
Accredited with 'A' grade by NAAC

## Nitte Gulabi Shetty Memorial Institute of Pharmaceutical Sciences

Accredited by NBA – UG Course
Paneer, Deralakatte, Mangalore – 575018
Phone: 0824 - 2203991, 2203992, 2203993 Fax: 0824-2203992
Website: www.nitte.edu.in, E-mail: ngsmips@nitte.edu.in


NITTE DEEMED TO BE UNIVERSITY

## PLAGIARISM CHECKER SERVICE

Access to "**Turnitin/iThenticate**"- Plagiarism Detection Software is provided by the Library for the below Researcher who is submitting his/her thesis to the Srinivas University.

The researcher and supervisor have verified the contents of the thesis against plagiarism and appropriate measures have been taken to ensure originality to research contribution.

| | | | | |
|---|---|---|---|---|
| 1. | Name of the Researcher | Mr.Krishna Prasad K | | |
| 2. | Name of the Guide | Dr. P.Sreeramana Aithal | | |
| 3. | Title of the Thesis | "A STUDY ON MULTIPLE METHODS OF FINGERPRINT HASH CODE GENERATION BASED ON MD5 ALGORITHM USING MODIFIED FILTERING TECHNIQUES AND MINUTIAE DETAILS" | | |
| 4. | Department and Institution | College of Computer and Information Science, Srinivas University, Pandeshwar, Mangalore | | |
| | **Percentage of Similar Content Detected** | | | |
| 5. | Similarity Index | Internet Sources | Publication | Student Papers |
| | **8%** | 7% | 5% | 2% |
| 6. | Date of verification: First scan/After revision: | 10.03.2018 | | |

This 8% of plagiarism includes acknowledged quotes from texts, footnotes, names of the books and repeated words.

Signature

10/3/18

LIBRARIAN

NGSM INSTITUTE OF PHARMACEUTICAL SCIENCES
PANEER, DERALAKATTE-574160
MANGALORE TALUK

# A Study On Multiple Methods Of Fingerprint Hash Code Generation Based On MD5 Algorithm Using Modified Filtering Techniques And Minutiae Details

*by* Krishna Prasad K

**Submission date:** 10-Mar-2018 11:09AM (UTC+0530)
**Submission ID:** 928209593
**File name:** for_originality.docx (3.07M)
**Word count:** 68231
**Character count:** 420053

# A Study On Multiple Methods Of Fingerprint Hash Code Generation Based On MD5 Algorithm Using Modified Filtering Techniques And Minutiae Details

ORIGINALITY REPORT

| 8% | 7% | 5% | 2% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | shodhganga.inflibnet.ac.in<br>Internet Source | 2% |
| 2 | Bansal, Roli. "Minutiae Extraction from Fingerprint Images - a Review", International Journal of Computer Science Issues (IJCSI)/16940784, 20110901<br>Publication | 2% |
| 3 | zenodo.org<br>Internet Source | 1% |
| 4 | www.law.ed.ac.uk<br>Internet Source | 1% |
| 5 | dyuthi.cusat.ac.in<br>Internet Source | 1% |
| 6 | www.onin.com<br>Internet Source | 1% |
| 7 | Madhavi Gudavalli, S. Viswanadha Raju, K. S. M. V. Kumar. "A template protection scheme | 1% |

for multimodal biometric system with fingerprint, palmprint, iris and retinal traits", Proceedings of the CUBE International Information Technology Conference on - CUBE '12, 2012
Publication

| | | |
|---|---|---|
| 8 | www.latent-prints.com<br>Internet Source | 1% |

Exclude quotes
Exclude matches
Exclude bibliography