ENHANCEMENTS IN FINGERPRINT AUTHENTICATION

A MASTER'S THESIS

in

Information Technology

Atilim University

by

MOHAMMED ABDULRAHEEM TAQI ALSUBAIHAWI

JUNE 2017

ENHANCEMENTS IN FINGERPRINT AUTHENTICATION

A THESIS SUBMITTED TO

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCE

OF

ATILIM UNIVERSITY

BY

MOHAMMED ABDULRAHEEM TAQI ALSUBAIHAWI

IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE

DEGREE OF MASTER OF SCIENCES

IN

INFORMATION TECHNOLOGY

JUNE 2017

Approval of the Graduate School of Natural and Applied Sciences, Atılım University.

_____

Prof. Dr. Ali KARA

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

_____

Assoc.Prof. Dr. Korhan Levent ERTÜRK

Head of Department

This is to certify that we have read the thesis " Enhancements in Fingerprint Authentication" submitted by "Mohammed Alsubaihawi" and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Asst.Prof. Atila BOSTAN

Supervisor

Examining Committee Members

Assoc.Prof. Dr. Erol ÖZÇELİK _____

Asst.Prof. Dr. Atila BOSTAN _____

Asst.Prof. Dr. Gökhan ŞENGÜL _____

Date: June 30, 2017

I declare and guarantee that all data, knowledge and information in this document has been obtained, processed and presented in accordance with academic rules and ethical conduct. Based on these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Mohammed Abdulraheem Taqi Alsubaihawi:

Signature:

ABSTRACT

ENHANCEMENTS IN FINGERPRINT AUTHENTICATION

Mohammed Abdulraheem Taqi Alsubaihawi
M.Sc., Information Technology
Asst. Prof. Dr. Atila BOSTAN
JUNE 2017, 105 pages

Fingerprint identification and verification tasks are among the most challenging tasks in image processing and machine learning domains. Fingerprint processing presents a key issue in the biometric technologies and information security. According to the fraction of the people population based on the complete detection of the biometric fingerprint feature such as ridge structure, incomplete (portion) fingerprint image identification and verification task is very difficult to be accomplished. The main challenge in this problem is that the partial loss of the ridge structure in the incomplete fingerprint image.

In this thesis, we studied the effectiveness of global feature approach in fingerprint identification and verification task that can deal with the partial image loss or incomplete fingerprint image. Global feature vector extraction is the main global approach that we contribute in this thesis. In this case, we implemented global geometrics based feature extraction for fingerprint identification and verification task. A set of global features (seven-moment values) were extracted from the partial fingerprint (incomplete fingerprint image). The study shows that global feature vector can more efficiently deal with incomplete fingerprint recognition problem when compared with the classical approach to the fingerprint identification and verification problem which is based on extracting minutia features from the fingerprint rides as well as the pores in different feature extraction levels.

The studied system has been tested using a database that was randomly generated out of some random incomplete fingerprint images. Randomly generated incomplete fingerprint images were sorted into 10 groups according to the size of the missing part in each image. Then we randomly selected random images from each group to compose a new challenge dataset to be tested in two different approaches which are global, and Local feature extraction approaches.

The experimental results show that global approach has about 87% while the local approach has 17% of identification and verification effectiveness. This means global approach improves the performance of the fingerprint identification and verification system on partial (incomplete) fingerprint images by 70% more than the classical approach.

Keywords: Fingerprint identification and verification, Minutia features, ridge features, Local feature approach, Global feature approach, Invariance Moment function, Region Of Interest (ROI)

ÖZ

PARMAK İZİ DOĞRULAMADA GELİŞME

Mohammed Abdulraheem Taqi Alsubaihawi
Bilişim Teknolojileri Yüksek Lisans
Doç. Dr. Atila BOSTAN
Haziran 2017, 105 sayfa

Parmak izi tanımlama ve doğrulama görevleri, işleme ve makine öğrenimi alanlarındaki en zorlu görevler arasındadır. Parmak izi işlemesi, biyometrik teknolojisi ve bilgi güvenliğinde kilit noktayı teşkil etmektedir. Çizgi yapısı gibi biyometrik parmak izi özniteliğinin bütün tanımlamasına dayalı halk nüfusu oranına göre, eksik (kısım) parmak izi görüntü tanımlaması ve doğrulamasının yapılması çok zordur. Bu sorundaki asıl zorluk eksik parmak izi görüntüsündeki çizgi yapısının kısmi kaybıdır.

Bu tezde, kısmi görüntü kaybı ve ya eksik parmak izi görüntüsüyle çalışabilen parmak izi tanımlama ve doğrulama görevine küresel öznitelik yaklaşımının etkinliğini inceleyeceğiz. Küresel öznitelik vektör çıkarımı, bu tezde incelediğimiz ana küreselleşme yaklaşımıdır. Bu durumda, parmak izi tanımlama ve doğrulama görevi için, küresel geometri temelli öznitelik çıkarımı uyguladık. Birtakım küresel öznitelikler (yedi moment değeri), kısmi parmak izinden (eksik parmak izi) çıkarılmıştır. Bu çalışma, farklı öznitelik çıkarımı seviyelerinde parmak izi dalgaları ve gözeneklerinden küçük detaylı öznitelik çıkarma işleminden oluşan parmak izi tanımlama ve doğrulama problemine yönelik geleneksel yaklaşımla karşılaştırıldığında, küresel öznitelik vektörünün eksik parmak izi tanımlama problemiyle daha etkin bir şekilde çalışacağını göstermektedir.

Üzerinde çalışılan sistem, birtakım rastgele seçilmiş eksik parmak izi görüntülerinden oluşturulmuş bir veri tabanı kullanılarak test edilmiştir. Rastgele oluşturulan eksik parmak izi görüntüleri, her görüntüdeki eksik parçanın büyüklüğüne 10 gruba ayrılmıştır. Sonrasında, her gruptan rastgele seçilen üç görüntüden yeni bir veri seti oluşturulmuş ve küresel ve yerel öznitelik çıkarımı olmak üzere iki farklı yaklaşımla test edilmiştir.

Deneysel sonuçlar, küresel yaklaşımın %87 oranında tanımlama ve doğrulama etkinliği varken yerel yaklaşımın %17 oranında etkinliği olduğunu göstermiştir. Bu sonuç, küresel yaklaşımın, parmak izi tanımlama ve doğrulama

sisteminin kısmi (eksik) parmak izi görüntüleri üzerindeki performansını, geleneksel yaklaşımdan %70 oranında daha fazla geliştirdiğini göstermektedir.

Anahtar Kelimeler: Parmak izi tanımlama ve doğrulama, Küçük detaylı öznitelikler, çizgi öznitelikleri, Yerel öznitelik yaklaşımı, Küresel öznitelik yaklaşımı, Sabit Moment işlevi, İlgi Bölgesi

To My Parents

ACKNOWLEDGMENTS

I would like to express my deep gratitude to Asst.Prof. Atila BOSTAN, my research supervisor, for his patient guidance, enthusiastic encouragement and useful critiques of this research work.
I would also like to extend my thanks to the technician of the laboratory of the Information System Engineering Department for his help in offering me the resources in running the program.
I would also like to express my very great thank to my Wife for her continuous support and patience during this period, my Children Mustafa ALSUBAIHAW and Ali ALSUBAIHAW , my Sisters and Brothers for their support, help and humor.

Last but not least, I wish to thank my parents Ameerah IBRAHEEM and Abdulraheem ALSUBAIHAWI for their support, encouragement.

TABLE OF CONTENTS

LIST OF TABLES

TABLE

LIST OF FIGURES

FIGURES

LIST OF ABBREVIATIONS

ATM - Asynchronous Teller Machine

DNA - Deoxyribo Nucleic Acid

ROI - Region of Interest

AFRS - Automatic Fingerprint Recognition Systems

ICP - Iteration Close Point

RANSAC - RANdom Sample Consensus

SIFT - Scale Invariant Features Transform

BPNN - Back Propagation Neural Network Method

SVM - Support Vector Machine

SR - Stochastic Resonance

FRR - False Reject Rate

FAR - False Acceptance Rate

ZS algorithm - Zhang-Suen algorithm

CN - Crossing Number

IMF - Invariant Moments Function

CHAPTER 1

INTRODUCTION

1.1 Introduction

Person authentication schemes to either identity or verify the identity of the individual using a variety of system requires reliable person information. This information in such as these cases are very important to the individual who are participating and requesting such service from the system that are required these identification information [1].

The purpose of the scheme is to make sure that is the rendered service such as person identification and verification task are accessed by a legitimate user which is not anyone else can use the user information for access [1]. Such good examples of the systems which include secure access to the building, computer system, cellular phones, personal laptop, bank account, and Asynchronous Teller Machine (ATMs). However, in the absence of robust and reliable authentication system which required and include (identification and verification) procedure that is vulnerable to the wiles of an impostor [1].

Basically, different identification information based security requirements such as identification card (Token-Based Security) and password (knowledge-based security) have been suggested and used to restrict access to systems. Therefore, the security task can be easily latched in the system when the provided information such as a password is divulged to unauthorized used or the identification card that has been stolen [2]. In this case, may be simple passwords that will be simply to guess by the person who is the imposter and also difficult password may be hard to recall by

the person who is a legitimate user. For this critical situation and difficult condition, the biometric information has address this kind of problem for the plague traditional verification and identification task [2].

Among all the biometric information that are shown in Figure 1.1 which are proposed and used in such different systems, fingerprint information's have shown that they have one of the highest levels of the reliability that is basically used by forensic experts to detect and discover the criminal investigation. Basically, fingerprint refers to the flow and organize such of ridge pattern in the tip of the finger. Those pattern is being organized in a practical and unique pattern for each person [2].

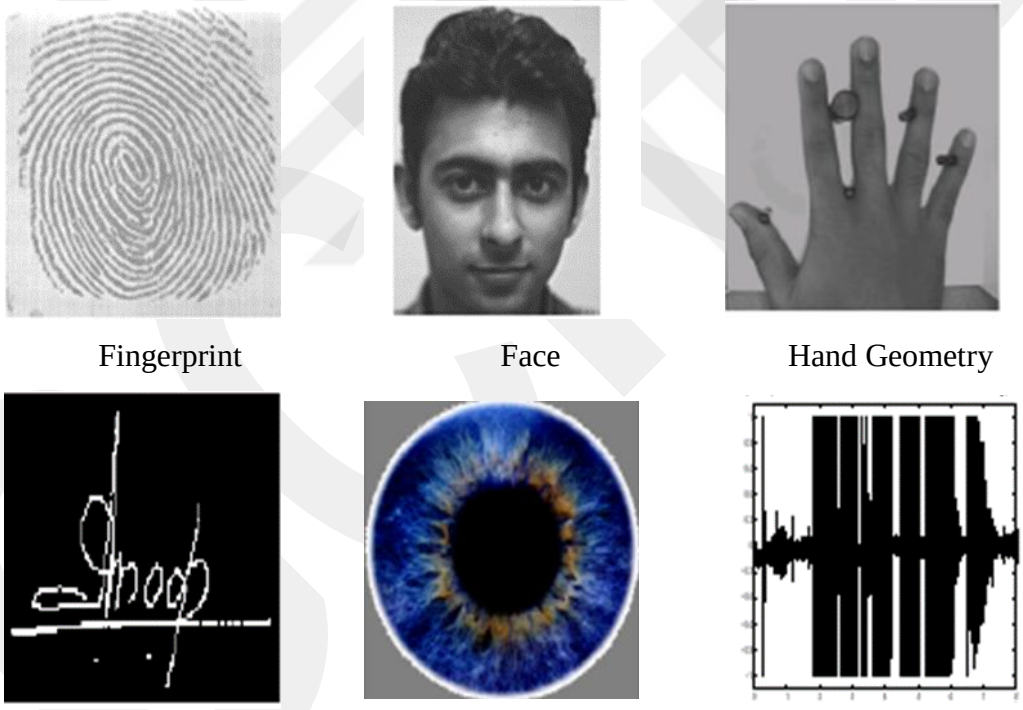


Figure 1.1: Some example of biometric traits information that used for authenticating (identification/verification) for an individual [2]

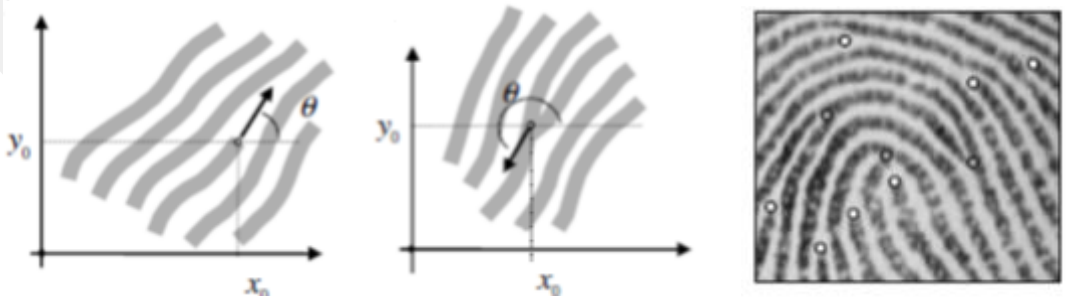
The ridge flow exhibits anomalies in local regions of the fingerprint is represented as the position and orientation. In this case, those positions and orientations are used to represent and identify (match) the fingerprints. Although, scientifically established of the fingerprints are believed to be unique across the

individuals and across fingers of the same individual [2]. Even the identical twins that having similar Deoxyribo Nucleic Acid (DNA), are believed that having different fingerprints. Traditionally, fingerprint patterns that have been extracted by creating an inked impression of the fingertip on paper [1].

The electronic era device that has ushered in the range of the compact sensor which is basically used to provide digital images of the fingerprint pattern. This type of acquisition sensor can be easily incorporating into such existing computer peripherals such as a mouse or a keyboard. There are making this mode of identification very useable and attractive. This kind is led to push up and increased the participant to use the automatic fingerprint identification and verification system based on authentication approach [2].

1.2 Fingerprint Concept

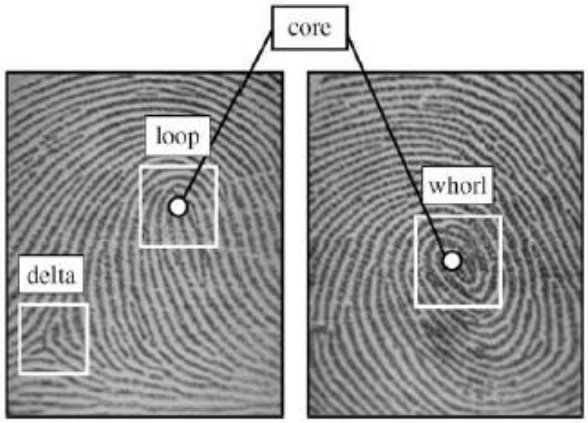
Fingerprints are the most important part in biometric for human identification. They are unique and stable from birth to death. So, fingerprints have been used for the forensic application and personal identification. Fingerprint has some unique points on the ridge which is known as minutiae point. A minutia can be in one of two main types which are termination point and bifurcation point [3]. As shown in Figure 1.2.



(a) (b) (c)

Figure 1.2: Fingerprint minutia features (a) a termination minutia feature (b) bifurcation minutia feature (c) termination feature [3]

Fingerprint pattern contains such one or more regions. These regions are constructed form such lines that create special shapes which may be classified into three main classes as it shown in Figure 1.3 [4].



(a) (b)

Figure 1.3: Fingerprint landmark core point and region detection (a) Delta and Loop features, (b) Whorl feature [4].

Loop, Delta, and whorl are the main shapes that are regions are classified to. Many fingerprint identification and verification algorithms depend on matching approach as a final stage of the fingerprint processing as well as to some pre-processing techniques that based on the landmark point detection or to the center point of the fingerprint which is called the core point. The region and core point detection in the fingerprint is called the Region of Interest (ROI) inside the fingerprint image as it shown above in Figure 1.3 [4].

Ridges and furrows in the fingerprint area present good similarity indication such as parallel are mind average [5]. Technically, fingerprints are not distinguished by the ridges and furrows that are detected and extracted in particular case inside the fingerprint, but it by the minutia feature. Minutia features are some abnormal and traditional cases of the feature points in the fingerprint which is originally used the ridges as it shown in Figure 1.3 [6]. Those features are traditionally the standard features which most of the fingerprint identification and verification systems depend

on in the matching stage. Typically, the individual young man has an average on 20.7 ridges per centimeter while the individual female has on 23.4 ridges per centimeter [6].

1.3 Automatic Fingerprint System

Personal identification and verification systems most widely used biometric characteristic such as fingerprint information for personal verification. This is due to the well-known fingerprint permanence, distinctiveness, ease of acquisition, universality, stability over time and high matching accuracy rates [7]. The fingerprint attributes can be divided into three levels, as shown in Figure 1.4 [6]:

The first level of features is the Level-1 feature attributes such as the overall fingerprint ridge patterns. The second level of the features is Level-2 attributes such as the local ridges attributes which represented by the minutiae, have been extensively studied and they are employed in most existing Automatic Fingerprint Recognition Systems (AFRS). Level-3 feature attributes which are the third level of the feature represented by the ridges dimensional attributes. This type of feature is ignored in many AFRS, even though they are also very distinctive and have been used for a long time in the forensic community [8]. Level-3 features refer to Ridge dimensional attributes such as ridge contours and pores, which are fine details on ridges [9].

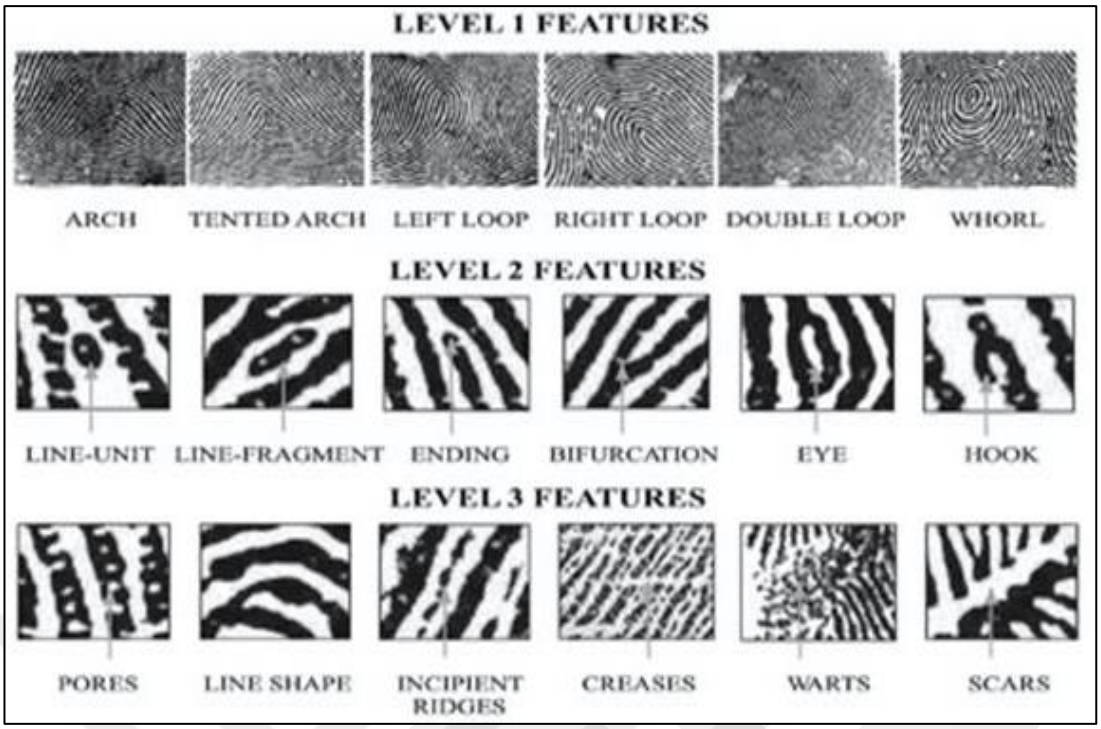


Figure 1.4: Fingerprint attribute at level1 (i.e., overall fingerprint ridge patterns), level2 (i.e., local ridges attributes), and level3 (i.e., ridges dimensional attributes) [6]

1.4 Problem Statements

Accurate and reliable fingerprint identification and recognition task is a big challenge task of data recognition since it depends on the quality of the fingerprint information which is in regularly on the scanned fingerprint image quality. In other words, fingerprint recognition systems are very sensitive to the image noise and the degradation level since it depends on the recognition performance in term of the feature extraction and the matching stage [10].

Generally, fingerprint recognition systems such as fingerprint identification and verification approach rely on the quality of the fingerprint images in many cases such as the preferable to an elimination of the low -quality fingerprint image as well as to replace them with the acceptable high-quality fingerprint images. This process is required to achieve better performance accuracy rather than attempting steps to enhance the input image in the pre-processing stage during the identification and verification task [11].

There are several factors which can determine the quality of the fingerprint image such as [12]:

1. Acquisition device condition such as dirtiness, sensor, and time-consuming for fingerprint images.
2. Individual artifacts such as the skin environment, age, skin disease, and pressure condition.

Many of these factors lead to partial loss some of the fingerprint images attributes. Fingerprint images quality is usually depending on the clarity of feature points such as ridges and valleys which consequently depend on the extraction stage of the fingerprint feature points which will use later for the matching stage [12].

Most of the existing Automatic Fingerprint Recognition System (AFRS) use the local feature extraction approach for fingerprint authentication system. This approach depends on the local feature points which are determined by minutia features such as the terminations and bifurcations of fingerprint ridges. However, this approach for the fingerprint identification and verification task has many issues that related with the minutia features such as [13].

1. The amount of noise and distortion during the acquisition stage of the fingerprint image which causes error in minutia extraction by missing minutia feature points where the performance of the recognition (identification and verification approach) relies on [14].

2. Rotation, different orientation, and the displacement of the fingerprint image that placed on the sensor during the scanning or image acquisition step. this issue can lead to different images for the basically the same fingerprint image by having just a part that only overlaps area which is resulting in only a small number of the corresponding minutia feature points [15].

3. Poor or low-quality fingerprint images be very difficult to rely on those to obtain the minutia features. Therefore, it is very necessary to exploit such a

novel model for attributed extraction like local ridge features as well as developed a new methodology which is more suitable for partial fingerprint recognition (identification and verification task) [16].

1.5 Fingerprint Identification and Verification

This thesis focuses on the incomplete image problem in fingerprint verification and identification task of the fingerprint image.

1.5.1 Fingerprint Verification Task

Verification of the fingerprint image task is the comparison of the tested (claimant) fingerprint against an enrollee one. In this task, the main intention of the verification task is to match the claimant fingerprint image. This should be done by finding the better matches for the claimant or the tested fingerprint image to the enrolled fingerprint images that have been stored in the database [17].

To prepare for verification task, the tested person is initially enrolling his or her fingerprint image into the verification system. Then, a representation of that fingerprint feature is stored in some compressed format along with the person's name or another identity [17].

1.5.2 Fingerprint Identification Task

Identification task is the also one of the most important tasks for the fingerprint identification and verification (fingerprint recognition). In this task, both verification and identification are used to identify the users [17].

In the identification stage, an individual person is recognized by comparing his/her fingerprint image with the entire fingering images that have been extracted and stored in the database. This step as the fingerprint identification is required for finding the best template matching [18]. In this case, the system conducts the identification stage as the one-to-many comparison to establish the identity of the

individual user that is trying to enroll in the system. The individual user that is trying to be identified does not have to claim that any identification such as (Who am I?). In contrast, in the verification system, the individual user that to be identified must claim his/her identity such as (Am I whom I claim to be?). Then, this template compared to the individual's biometric features (characteristic) [18]. More precisely, the identification task conducts one-to-one comparisons to establish the identity of the individual used in contrast with the verification task [19].

In general, before the fingerprint identification and verification system is able to verify/identify the specific biometrics of the individual user, the system requires some initial data to compare with the database. In this case, a profile or template containing the biometric features or properties such as specific features to store in the system. This step is called the used enrolling, identification, and the verification which is described and illustrated in Figure 1.5 [20].

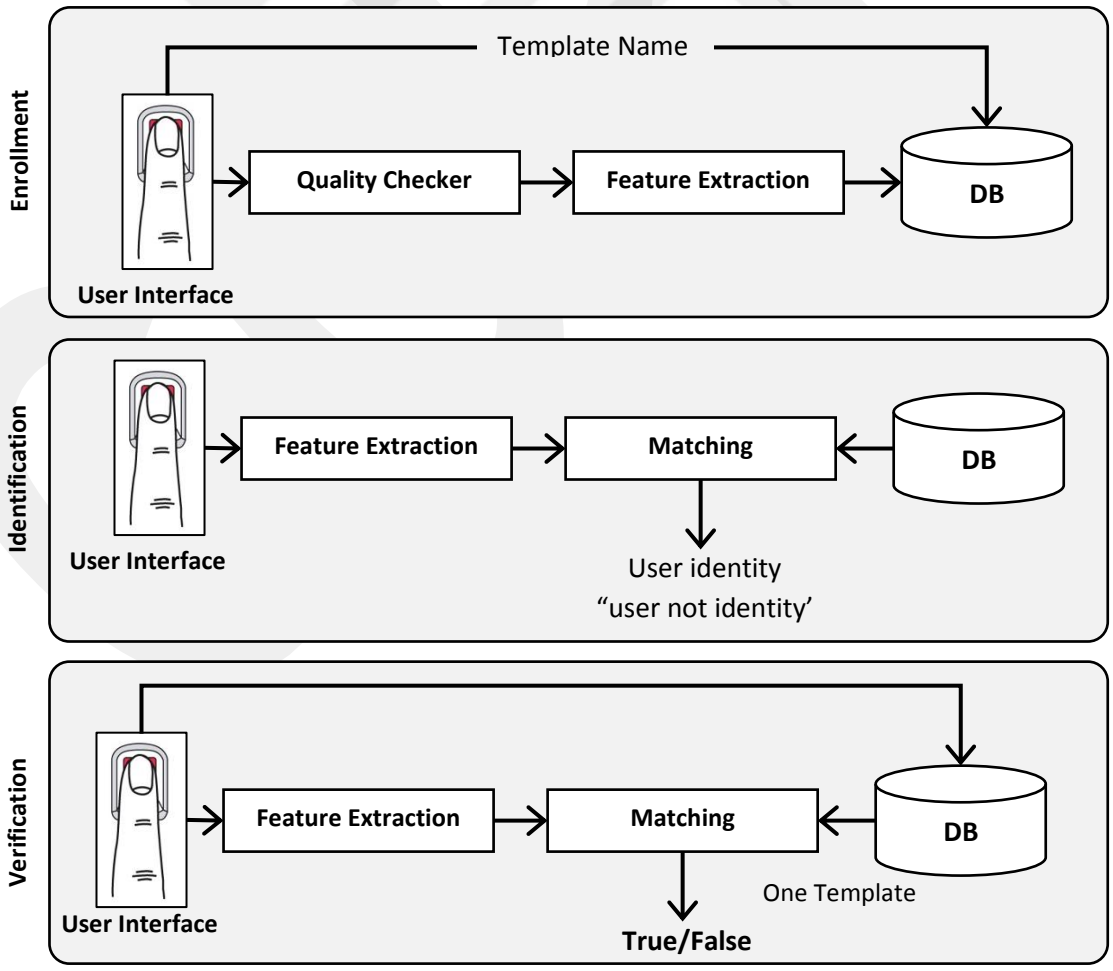


Figure 1.5: Enrollment, Identification and Verification system

1.6 Research Objectives

The main objective of this research work is to develop a fingerprint identification and verification algorithm which is functional on incomplete fingerprint images as well. The success rate accuracy of the propped algorithm should be significantly better than that of local minutia approach. The system performance will be investigated to determine the system performance behavior, and its dependency on the partial fingerprint features loss will be investigated.

1.7 Aim of Thesis:

Because of the uniqueness and invariability of fingerprints, fingerprints identification and verification system (fingerprint recognition) have been used in several applications such as access control to such particular systems like the bank account, or banking system. In additional to the security verification of purchasers and firearm as well as to the driver's license application verification system which is usually associated with the police work.

Fingerprint identification and verification approach in some cases is very challenge task such as in noisy finger, rotation, incomplete image, and bad quality fingerprint image. Since the most popular approach that relies on the minutia feature extraction for fingerprint identification and verification approach which is a (Local Approach) is not robust enough to deal with such those problems, in this thesis we propose such a different approach which is a Globalize approach to solving the incomplete fingerprint identification and verification approach that the local approach has felt on that.

1.8 Contribution of Research

The main contribution of this thesis is to develop and enhancement the unnormal fingerprint identification and verification approach by proposing a Global feature extraction approach by extract the global feature vector instead or rely on the Local approach that depends on the minutia feature extraction. The main part of our

contribution is that we used incomplete fingerprint image samples instead of the regular fingerprint image sample by generate such random incomplete fingerprint image and compare between our contribution approach and the standard approach.

Finally, our approaches that we have used for this thesis and our contribution are:

1. Implement the Local approach for fingerprint authentication which is based on the Minutia feature extraction as a main approach for fingerprint identification and verification task.
2. Implement our proposed approach the Global approach for fingerprint authentication which is based on another methodology for feature extraction to avoid the main limitations of the local approach. In this approach, we proposed another technique of adaptive way for solving the rotation, noisy, and the fingerprint orientation which is based on the invariance moment methodology for global feature extraction.
3. Generate such random samples of the incomplete fingerprint images that are used mainly as the main challenge of the fingerprint images dataset which is proposed for fingerprint authentication that it used in this thesis.
4. Compare between the Local and Global approach for the incomplete fingerprint identification and verification task.
5. Draw a conclusion after we calculate the final conclusion and the behavior of each approach separately and discuss them in detail.

1.9 Thesis Organization

This thesis shows the design of fingerprint authentication system by obtaining the global fingerprint features and apply the matching alignment algorithm (invariance moment function) on incomplete fingerprint images. The system consists of three main stages: image pre-processing stage, feature extraction stage, and finally the matching stage. The thesis consists of five chapters:

Chapter 1: This chapter gives a brief introduction to the biometric fingerprint systems, and describes the Biometrics types and the definition. It also gives their application areas.

Chapter 2: Lists the related works and the recently literature survey of the biometric fingerprint authentication system.

Chapter 3: System design and implementation of the proposed system: it illustrates the proposed system (automatic fingerprint identification system based on the global approach).

Chapter 4: Describes the implementation results and discussion of the local and global approach for fingerprint authentication system.

Chapter 5: Contains the conclusion and gives some suggestion for future works.

CHAPTER 2

LITERATURE SURVEY

2.1. Introduction

Recently, accurate and efficient human recognition and identification have become crucial and critical for forensic applications. Due to the large diversity of crime scenes, identify criminals from the available crime pieces of evidence is increasely needed. Recently, there were many challenges in many different types of crimes detection and crime scenes which vary from physical crime to computer crimes [21].

Biometrics information is a good and robust technology that provides such accurate and robust and a high level secure personal detection and investigation system. Person identification and verification for civilian applications are the most significant forensic application. The intensive impact of the biometric information is that is rapid development in the computer science which gives a good opportunity to develop it to be more reliable systems by applying such computational intelligence, and computing approaches. This development of the systems that deals with the biometric system have reflected in the biometric system modularity such as in biometric capturing process, feature detection and extraction, robustness features modulation and accurate template matching [21].

Biometric data such as biometric fingerprint recognition (identification and verification task) has different approaches with different performance results. Recently, biometric fingerprint identification and verification based on the local detection of the minutia features have been proposed in this rate [21].

2.2. Literature Survey

Nowadays, most of the countries in the world are interested in the fingerprint authentication because of the increase of criminal issues in any domain life. Hence, the fingerprint is individuality to anyone personally, therefore the central search is doing many researchers on fingerprint and develop it and saved massively on the computer in order to identify, verifying, matching and displaying output. All of them tried to find a way for fingerprint identification that is more accurate and less sophisticated. Several kinds of research have gone to develop the newest and best algorithms fingerprint recognition since the emergence of this concept at the first time. In this chapter, we show and review some literature in which associated with this work.

Kryszczuk et al. [22] This works investigated the effect of different level of the fingerprint features. It depends on to detect and extract the pores features which are used later in the matching fragmentary for the fingerprint. This approach concludes that the pores feature become more useful than other feature in such a fragment size as well as the decreasing number of minutia features. In some situation such as fingerprint image resolution, the degree of the skin condition will increase which in this case and this approach will be not favorable and not give reliable performance results. This approach, the state-of-the-art of the minutiae feature extraction based on local feature fragment position (pores) has been proposed for the matching method. This approach has achieved performance results by 30% performance results improving in fingerprint recognition accuracy just by depending on the pores features. Although, by combing minutia feature with pores this combination approach has improved the fingerprint recognition accuracy with respect to that just using the minutia features. This approach as satisfied about 29.82% and 37.46% performance results improving.

Jea and Govindaraju [23] This work presents an approach for local fingerprint feature detection and extraction by using local secondary features. This kind of feature is derived from the relative minutia feature information that already have been extracted from the same area of the fingerprint image. The experimental results show that the fragmentary fingerprint approach for small region of fingerprint

will be very possible to be no sufficient minute information can be extracted. Therefore, in this case by using neural network in this approach the experimental results show that for generating similarity scores have been improved by obtaining about 1.21% and 0.68% on a minimum total of the total error for the fingerprint recognition in different databases.

Jain et al. [24] This work presents a utilize local approach for Level 3 feature detection and extraction by include pores and ridges features. In this work, fingerprint image with 100 dpi resolution has been used in this approach for the fingerprint images matching. This approach proposed a wavelet transform and Gabor filter to extract the Level 3 features level and locally matched using the Iteration Close Point (ICP) based matching algorithm. The experimental results of this work show that by using median size fingerprint images dataset depending on the Level 3 features carry out significant discriminatory relative information which reduces the EER value by relatively 20%.

Jain et al. [25] This work proposes an approach by using advanced fingerprint sensing. The sensing technology that used in this approach by equipped with dual fingerprint image resolution (500 ppi and 1000 ppi) scanning capability. However, increasing the fingerprint image scan resolution does not necessarily provide any improving in the performance results of the fingerprint image matching. Unless an expected features set is locally utilized in this approach. The experimental results of this approach show that the dynamic study to determine how much performance improving gain and achieved by using Level 3 features in the Automatic Fingerprint Identification System (AFIS). In this case, this approach has achieved about 12% to 15% error rate (EER) for the fingerprint image identification based pore matching approach.

Qijun et al. [26] This approach presents a real pores model for real pores that are not always isotropic. In this approach, an adaptive anisotropic per model has been proposed for accurately and robustly pores feature extraction. According to the fingerprint ridge features direction and period, the parameters are adjusted adaptively. The proposed system for this approach depends on that the fingerprint is partitioned into blocks and local model is determined for each block. Then, within

the local pore model, a matched filter is used to extract the pores features within each particular block. The experimental results show that by using a high-resolution fingerprint image (12000 dpi) dataset, the proposed system can locally locate the pores feature. In other words, the performance results of this approach demonstrate that the proposed pore extraction model accurately and robustly locate the pores features by depending on the minutia features points as well. This approach improves the performance results by reduceing the minim error for only minutia feature based fingerprint recognition by 34%.

Qijun Zhao et al. [27] This work proposes a novel approach for fingerprint matching based pores features. This approach first determines the correspondence between pores features based on the poser local feature points (positions). Then, it uses the RANSAC which is (RANdom Sample Consensus) as an algorithm to refine the pore correspondence which is obtained in the first step. This approach presents a similarity score computing results by final calculate based on the pore matching based results. The proposed method (pore matching) is successfully avoids the pore features dependency that causes my matching on minutia matching results. The experimental results of this approach show that the fingerprint recognition performance accuracy can be greatly improved by using the method which proposed in this paper approach. Recognition accuracy in term of the EER and the FMR1000 with respect of using the minutia features is improved by about 29.83% and 37.46%.

Abhyankar et al. [28] This work presents a study of using a fingerprint pore along the ridge features based fingerprint matching. Wavelet transform has been also proposed to extract those features base on using an enhancement technique which is mainly implemented to detect the Level3 features. The approach also present a Delaunay triangulation based alignment and matching of the fingerprints. The pores features are checked for the liveness by perspiration the activity in the time series which is captured during the process. The performance results show that the developed fingerprint matching approach that has proposed in this work has achieved lower error rate by 2.97% of EER after tested on high-resolution fingerprint image (686 ppi) for 144 live samples and spoof fingerprint classes.

Nedia et al. [29] This work focuses on such different fingerprint problem of reducing the fingerprint features that has been entered to the neural network. In this work. An algorithm was introducing to work a prepared codebook to code the normalized input fingerprint samples of the back-propagation approach. The main advantage of doing the preparing step is that is simplicity of its step is that its high-speed processing step. The experimental results of this approach show that the recognition rate of the fingerprint images have achieved about 94% with error rate (EER) by 2.1% when it has tested on the FCV2002 fingerprint images dataset.

Chandra et al. [30] in this paper uses (Scale Invariant feature transform) SIFT algorithm. Firstly, fingerprints of good quality are acquired by using optical scanner. Image normalization is done using Gaussian blurring and sliding window contrast adjustment. Pores are extracted and estimated. Using these estimated pores, matching is done from template database to stored database using SIFT algorithm. Scale Invariant Features Transform (SIFT) is an algorithm in computer vision to detect and describe local features in images. The features are invariant to image scaling and rotation. They are well local in both the spatial and frequency domains the proposed level-3 feature extraction algorithm yields a verification accuracy of 94%.

Mela et al. [31] in this work, develops a geometrically based method for fingerprint recognition and verification tasks; a set of partial local features extracted from fingerprint ridges, minutia, and pores attributes are used. The proposed system passes through two main phases: training phase and test phase. In the training phase, the system is trained using a set of low quality fingerprint images to select the best discriminating local features this can lead to best recognition rates. During the test phase, the system performance is examined to know the attained recognition rate is (100%) and verification with error rate of approximately (1.2%) at threshold value equal to (39.5). Using features based on local ridges attributes only can lead to near optimal recognition rate of (99.37%).

Divyaloshini V. et al. [32] in this paper presents a unique verification system which is called fingerprint biometric authentication using Back Propagation Neural Network Method The results of authentication has been compared with previously, implemented algorithm SVM. The mechanism has been tried with different sets of

rotation and matching, score at the end has been computed to 93% on an average with BPNN whereas the accuracy for SVM lies in the range from 70 to 80 %.

Ross et al. [33] This work presents a suggestion model of using both minutia and texture feature information to represent the fingerprint images in a matching stage. In this approach, the ridge features map along with the minutia set of some images have proposed and used for the matching purpose. The genuine accept rate of the hybrid matching approach that has been proposed in this work observes to be 10% higher than that of a minutia-based feature matcher at low false acceptance rate. The fingerprint verification of this approach has achieved lower time consuming by 1,.4 seconds on the hybrid marcher took.

Kryszczuk et al. [34] This work presents an investigation model to affect the pores in matching fingerprint fragmentary. This work concludes that the pores become more useful features in the fragment size wherein the same way it decreases the number of the minutia features. Although, there is some limitation of this approach that is related to the fingerprint image resolution. When the image resolution decrees or the skin condition become not favorable, in this case, the proposed method will not give any reliable results.

Jeo et al. [35] This work discusses the matching task of the partial fingerprint image. This proposal presents an approach to match partial fingerprint images by using singular rides structure which is based on the alignment techniques. Although, this work indicate that such techniques failed especially when have applied on the partial fingerprint images which do not include such structure such as core and delta. This approach presented a multi-path fingerprint matching approach by locally utilized the secondary features which are derived using the relative information of the minutia features.

Nandakumar and Jain [36] This work presents a model of using both minutia features and ridges information. In this approach, the query fingerprint image is aligned to the template matching by using only the ridges associated with the minutia features itself.

Jea and Govindaraju [37] This work presents an approach of utilizing the secondary features form that is derived from the relative minutia feature information. This kind of feature in this approach appears when the fragment fingerprint image with small fingerprint image regions are given. In this case, it would be very possible that no such sufficient minutia feature that is available.

Marana and Jain [38] This approach presents a new methodology for fingerprint matching that based on the ridge features. In this approach, a ridge based feature extraction has combined with the minutia based feature extraction technique for fingerprint image matching. The experimental results of this approach show that this methodology is able to detect the false or the non-match are minutia base features by computing the matching score. Although, combination methodology shows that this approach led to the reduction of the false matching rate by approximately achieved 1.7% error rate (EER).

Zakaria [39] This work present propose an embedded software design for the biometric fingerprint image authentication system. This approach involves interface design and software development system which focus on enhancing the fingerprint image. The main focus of this approach is enhanced the feature extraction approach, fingerprint image, as well as enhanced the matching template that is previously stored in the matching database. In this approach, an embedded software that is designed in this proposal to verify the minutia templates extraction as well as fingerprint matching.

Islam et al. [40] This work presents a model to improve the fingerprint authentication system by using low price webcam. This approach presents advance preprocessing approach for the low-quality webcam by using gamma manipulation and gamma correction technique. In this approach, this technique is mainly used to adjust lightness and intensities of the fingerprint image by using gamma manipulation and gamma correction technique. The experimental results show that the proposed approach has achieved about 97.4% performance accuracy when it has been tested using Fingerprint Verification Competition (FCV2004) database.

Yang et al. [41] This work presents an efficient algorithm for low-quality fingerprint image enhancement. It has been mainly proposed when the rides pattern is very noisy and have been corrupted. This approach proposes an enhancement ridge extraction methods with a combination of local normalization and local ridge compensation filter, which uses the local ridge orientation. The proposed approach has achieved about 3.96% in error rate (EER) when it has been tested FVC2004 DB2.

Ram [42] This work presents a novel model for fingerprint ridge orientation detection and modeling. This approach addressed the smoothing orientation data while preserving details in high curvature are which is especially around singular point. The ephemeral results show that this approach has achieveed EER was 1.81% and 0.18% when it has been tested using FVC2004 DB3 images and on FVC2006 DB2 fingerprint images.

Ryu et al. [43] This work presents a new methodology by designed an approach for fingerprint image feature extraction enhancement. The new extraction technique based low-quality fingerprint image by adding such noise to the original image signal. The Stochastic Resonance (SR) was proposed and applied to 20 fingerprint images using the FVC2004 DB2 database where originally have been rejected by the state-of-the-art fingerprint verification algorithm. The experimental results show that this approach has been improved the feature extraction using SR by decreasing the EER of the fingerprint verification from 6.55% to 5.03%.

Xie et al. [44] This work presents a model to estimate the quality and the validity of the fingerprint image capturing in advance for the fingerprint identification system. In this approach, the estimation algorithm has been designed to address the problem of the quality assessment as a classification problem.

Elmir et al. [45] This work presents such model to develop a full automatic identification system that based on using Support Vector Machine (SVM). Also, develop the recognition algorithm which is specifically associated with their system by including the original image processing techniques such as minutia feature extraction, singular point local, and Gabor filter. The experimental results show that

the proposed system has achieved 73.6% performance accuracy when has been tested in FVC2004 databases, and 94.7% when it has been tested in FVC2004 DB3.

Indra et al. [46] This work presents a new fingerprint recognition model that use ridge based coordinate system to extract the feature points such as ridge length, ridge count ridge type, and curvature direction which applied and extracted from the low-quality fingerprint images. The proposed approach found that the ridge count feature is more reliable and robustness to such condition such as to the curvature direction and ridge length which will in this approach increase the discriminating power of the ridge count feature.

Ouzounoglou et al. [47] This work proposed a fingerprint matching approach that based on the non-necessity of detection and constructing minutiae points in the input fingerprint image. The proposed system shows that the matching algorithm has achieved 0.058506 of error rate (EER) when it has been evaluated using the DB3 database of FVC2004 DB3.

Short et al. [48] This work presents a model to address the problem of the feature extraction on the low-quality fingerprint image. This approach proposes a filtration approach for fingerprint image enhancement based on tracking the ride's line by estimating the ridge flow direction of a ridge points. The experimental results show that the proposed approach led to reducing the False Reject Rate (FRR) by 11.1% as well as to False Acceptance Rate (FAR) of 1% for a group of low-quality images.

CHAPTER 3

THE PROPOSED FINGERPRINT ATHENTICATION MODELS

3.1 Introduction

This chapter is dedicated to present the design considerations, implementation requirements and the steps taken throughout the establishment of the fingerprint proposed models. Two models have been studied in this thesis. These models for fingerprint authentication and verification are local approach which is the first one, and global approach as the second one. The implementation steps are illustrated in detail using diagrams and/or pseudo code.

In general, the proposed model has the essential stages to perform all relevant recognition and verification tasks. The general structure of the typical fingerprint authentication and verification system has two main models as it is shown in Figure 3.1. The first one is the enrollment model and the second one is the authentication and verification model. Each main model has many sub models or stages. Each model from the main model has main sub-stages or (sub-models), the four important modules for each main model are:

1. **Sensor Module**: In this model, the biometric fingerprint image is scanned or captured for the individual user who is a participant in the fingerprint identification and verification system.

2. **Feature Extraction Module:** The main purpose of this model is to acquires the data which is processed to extract the features from the fingerprint image that has been scanned and captured from the Sensor Model. For example, the

feature points, as well as feature orientation, be detected and extracted from the fingerprint image using this model.

3. **Matching Module**: The third model of the fingerprint indentation and verification system is the Matching Model where the feature values are compared against all the template feature that are extracted from the users and store in the system database. The matching model using matching score by generating a matching score based on the template matching, for example, the number of the minutia feature that matched between the query fingerprint image and the template one.

4. **Decision-making Module**: The last model of the fingerprint identification and verification model is the Decision-making Model which in this model the user is claimed that is in either way accepted or rejected depending on the matching score.

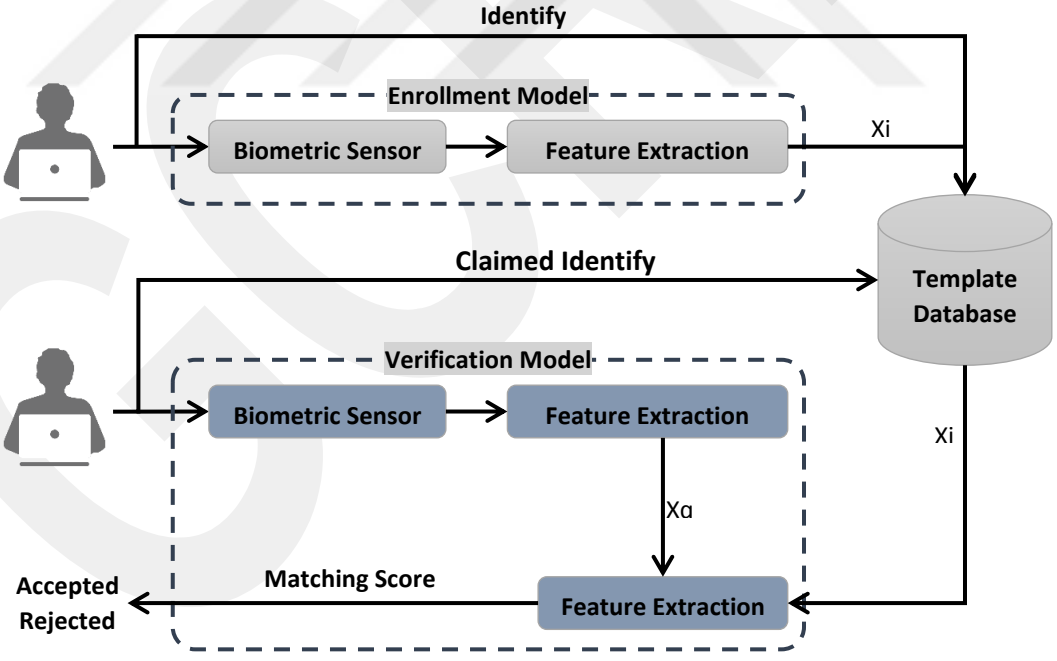


Figure 3.1: The enrollment model and the verification model a biometric system

3.2 Proposed System Layout

In our proposed system, we develop and test a fingerprint identification and verification algorithm which is functional designed on the incomplete fingerprint image scans by utilizing the global features in fingerprint by proposing a global feature vector extraction approach. In our approach.

In order to prove our approach is more efficient than the standard one (Local Approach) based minutia feature extraction approach for fingerprint identification and verification the proposed approach used identification and verification algorithm is functional on incomplete fingerprint images we have run the Local feature methods as well to be able to compare the results which show that our Global feature approach has score better than the Local feature approach as it will show in details in chapter 4. .

Rotation, noisy, and incomplete fingerprint image are the most important cases that have been failed on the first approach, and we assume that our approach has been successes on them. The general approach structure of the proposed system is shown in Figure 3.2.

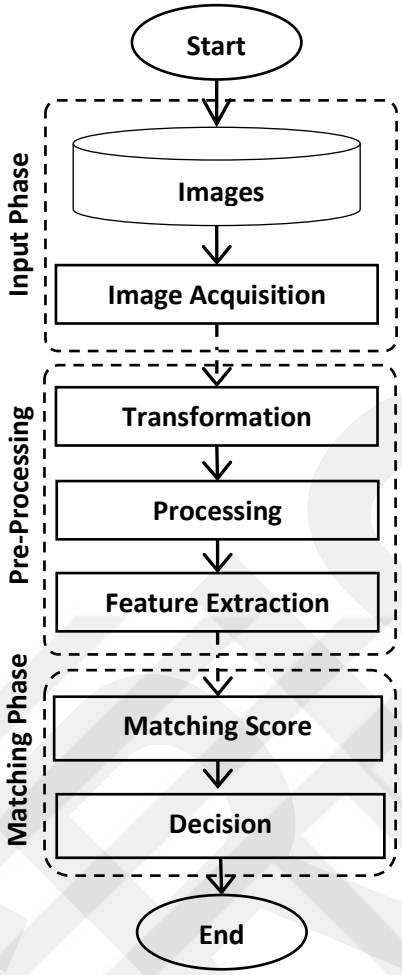


Figure 3.2: The Framework of fingerprint authentication and verification general approach

Input phase: This phase consists of uploading images from datasets into the authentication and verification system in this phase we have to do two general steps:

- ***Database image selection*:** In this step, the dataset has been selected based on different datasets version that we want to use in our system such as FCV2002, FCV2004, and FVC2006.

- ***Image acquisition***: In this step, the fingerprint image that it has to be tested is loaded from hard disk (where the dataset is located and saved) to the memory of the authentication system.

Pre-processing phase: In this phase, there are many steps should be implemented in term of enhanced the fingerprint images such as:

- ***Transformation*:** In this step, depending on the approach that we are going to used which is mainly depends on the fingerprint image type (color, gray), there is some transformation steps should be implemented to prepare the fingerprint image to the next stage which is the feature vector extraction.

- ***Processing*:** in this step, some pre-processing step has been done, like convert the fingerprint image from domain to another domain, specifically depends on the type of feature extraction approach. For example, minutia features for fingerprint required some specific step and preprocessing tools to extract those feature as will have explained briefly in the local approach.

- ***Feature Extraction:*** in this step, depends on the type of the authentication and verification approach the appropriate features will be extracted.

Matching Phase: in this phase, the feature vector for the tested fingerprint will be in two cases. The first one if the fingerprint image in the test part which is already in the authentication and verification system, the feature vector will be matched and tested with the whole feature vectors in the authentication system and the matching score will be computed.

Depending on the matching score the final decision will be made in the fingerprint will be authorized or not. The second case if the fingerprint feature vector is not in the authentication system it will automatically store the database on the system.

3.3 Local Approach

Local feature extraction depends on the minutia feature extraction which is a local feature extraction approach. This model has the essential stages to perform all relevant recognition and verification tasks. The general structure of the local approach for fingerprint authentication and verification system is shown in Figure (3.3).

The implementation of the fingerprint biometric template system (fingerprint identification and verification system) is based on developed some stages to be consisting of four major stages such as preprocessing, feature extraction, post-processing, and matching (or enrollment). These five stages are executed sequentially. The performance stage of feature extraction and matching stage which mainly depends on the quality of the input fingerprint image. There are several reasons may degrade the quality of the fingerprint image. Therefore, the main stage of the local feature extraction approach for fingerprint authentication can be summarized in:

Pre-processing Stage: The preprocessing stage in the fingerprint identification and verification system is considered as a necessary step in the established model. For fingerprint cognition (identification and verification) tasks, the preprocessing stage should cover two main tasks such as:

- ***Image Binarization:*** The first task is image transformation; the applied fingerprint in the binarization algorithms is applied mainly on the gray-scale level image which is based on automatic determination of optimum threshold value such as the local thresholds. However, it should cause efficient separation of objects ROI from their background.

- ***Thinning:*** The second task is thinning the edges appeared in the produced binary image. The thinning process should preserve the connectivity of the ridge structures while forming a skeleton version of the binary image. The thinning process should preserve the connectivity of the ridge structures while forming a skeleton version of the binary image. The skeleton image is normally used to extract the existing minutia in the image.

Feature Extraction Stage: In this stage of the fingerprint identification and verification system which is the feature extraction stage, a simple image scan aims to detect the minutia pixels. according to different types of distortions which may appear locally in the fingerprint image such as under-inking, overlinking, scars, or

excessively worn prints, as well as due to thinning process, many false minutia may be nominated among the candidate minutia detected in the thinned image.

Post-processing Stage: A post-processing phase of minutia purification represents an important part of the local feature extraction model for fingerprint authentication and verification approach. Also, this phase includes:

- ***Remove False Minutia:*** This step is important because holes will reduce the accuracy of the thinning algorithm thus creating false minutia point(s).

- ***Detect the Region of Interest:*** The ROI contains the desired fingerprint impression which is extracted to avoid detection of false features outside the fingerprint pattern.

Matching Stage: The fourth stage, the matching scores are determined for each set of extracted features from the feature vectors. At the matching stage, the calculated distance either matched with the previously extracted vectors listed in fingerprints database for recognition or verification purpose, using match module or stored in fingerprint database, during the enrollment phase.

The main diagram of the local feature extraction approach for fingerprint authentication and verification system is illustrated in Figure 3.3. This figure shows the main stages of the local approach which has many stages

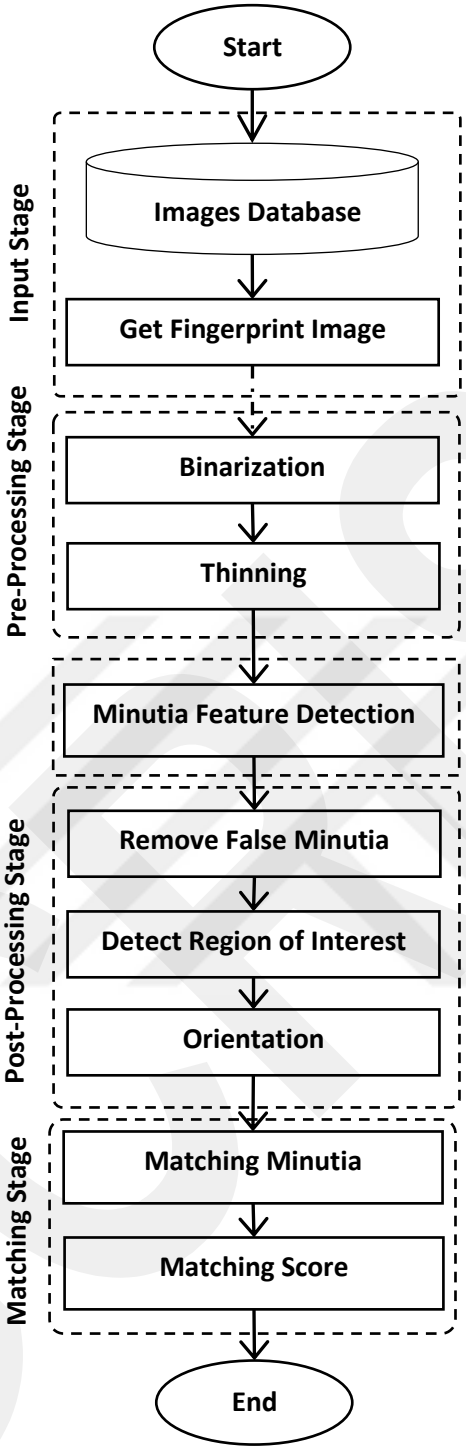


Figure 3.3: The local feature extraction model architecture

3.4.1 Read Fingerprint Image

In this stage, the fingerprints images are fed to the system as a PNG image files; the color resolution of the image is taken either 24 bit/pixels. The image data (i.e. RGB components) is loaded and then used to compute the Gray array from the loaded Red, Green, and Blue data.

3.4.2 Pre-processing Stage

The first stage in any authentication and verification system is the pre-processing phase. This phase includes many steps as explained in Figure (3.3). The main focusing of this stage is to transform the image and skeletonized the image. Fingerprint image preprocessing stage is crucial for both enrollment and cognition tasks.

A. Convert to Gray-scale image

The first one is to convert the image color representation to gray image representation. The Gray value is computed from Red, Green, and Blue arrays by converting them to YIQ which is (Luminance (Y), color chrominance (I and Q)) models, then the gray value is set equal to the intensity, Y, component [49].

B. Image Binarization

The selected threshold used to convert gray image to black and white is chosen manually, and it is choosing Gray image represents the red, green and the blue color components of the pixels in an image take the same value between 0-255. Hence the model fixed value by trailed and error threshold values 128 will be chosen using the gray value component, threshold. A simple output is a jpeg image which consists of only two gray levels (black and white), then the output is a binary image in which black generally represents the foreground pixels or the pixels of interest and white represents the background pixels [50]. Blow a process of thresholding has represented in algorithm as shown in algorithm (3.1).

Global (Automatic) threshold

The fingerprints in the database are all gray-scale images. A global threshold is determined. The value of the threshold value depends on brightness of the image. Then each pixel is smaller than the threshold will be set to zero, otherwise, it is kept unchanged. Algorithm (3.1) presents the implemented steps for global thresholding task [51] [52] [53].

Algorithm (3.1) Global Thresholding

Inputs:

Gray: image array of gray pixels values
Hgt : Image Hight
Wid : Image width

Output:

Glo : the array of enhanced gray image

1. **Initialize** minimum (Min) and Max values
2. Min ←Gray (0, 0); Max← Gray (0, 0);
3. **Compare** each pixel with Min and Max
4. **For** all pixels in the image // x as row number, y as column number
5. **If** Gray_value (x, y) < Min Then
6. Min← Gray (x, y)
7. **End If**
8. **If** Gray_value (x, y) > Max Then
9. Max← Gray (x, y)
10. **End If**
11. **End For** // x & y
12. Thr ← (Min + Max) / 2 // Calculate threshold
13. **For** all pixel in the image // I as row number, J as column number
14. **If** Gray_value (x, y) ≥ Thr Then
15. Glo (x, y) ← Gray (x, y)
16. **Else**
17. Glo(x, y) ← 0
18. **End If**
19. **End For**
20. **END**

The result of the binarization algorithm that applied on the fingerprint image is shown in Figure 3.4

Original Fingerprint Image Global Binarization Result

Figure 3.4: Global (automatic) image threshold

Local (Manual) threshold

The conversion step from the gray-scale fingerprint image to black and white fingerprint image is performed by applying thresholding upon the fingerprint gray image. The selection of threshold value is either done manually by the user, or it is assessed manually. In our developed system, the proper value of threshold is selected manually. Also, the local thresholding method is adopted which is based on some category such as the local characteristics of fingerprint image. The threshold assessment process is started with calculating the average intensity value. Then, all the pixels belong to a small block lay within the central area of the large block are binarized by comparing its value with the determined threshold value to decide whether each pixel belong to ridge or background [54].

Algorithm (3.2) presents the taken steps for making local thresholding.

Algorithm (3.2) Local Thresholding (Manual)

Inputs:

Gray: Gray Image

Output:

Binarized Image

1. **Initialize** minimum (Min) and Max values
2. **Set** thr= 128 or any number // threshold value
3. **For** all pixel in the image // I as row number, J as column number
4. **If** (pixel < thr)
5. **Set** pixel=1 // white pixel
6. **Else**
7. **Set** pixel=0 // black pixel
8. **End If**
9. **End For**
10. **END**

The result of the local fingerprint image thresholding (Manual) by selecting different threshold values are shown in Figure 3.5.

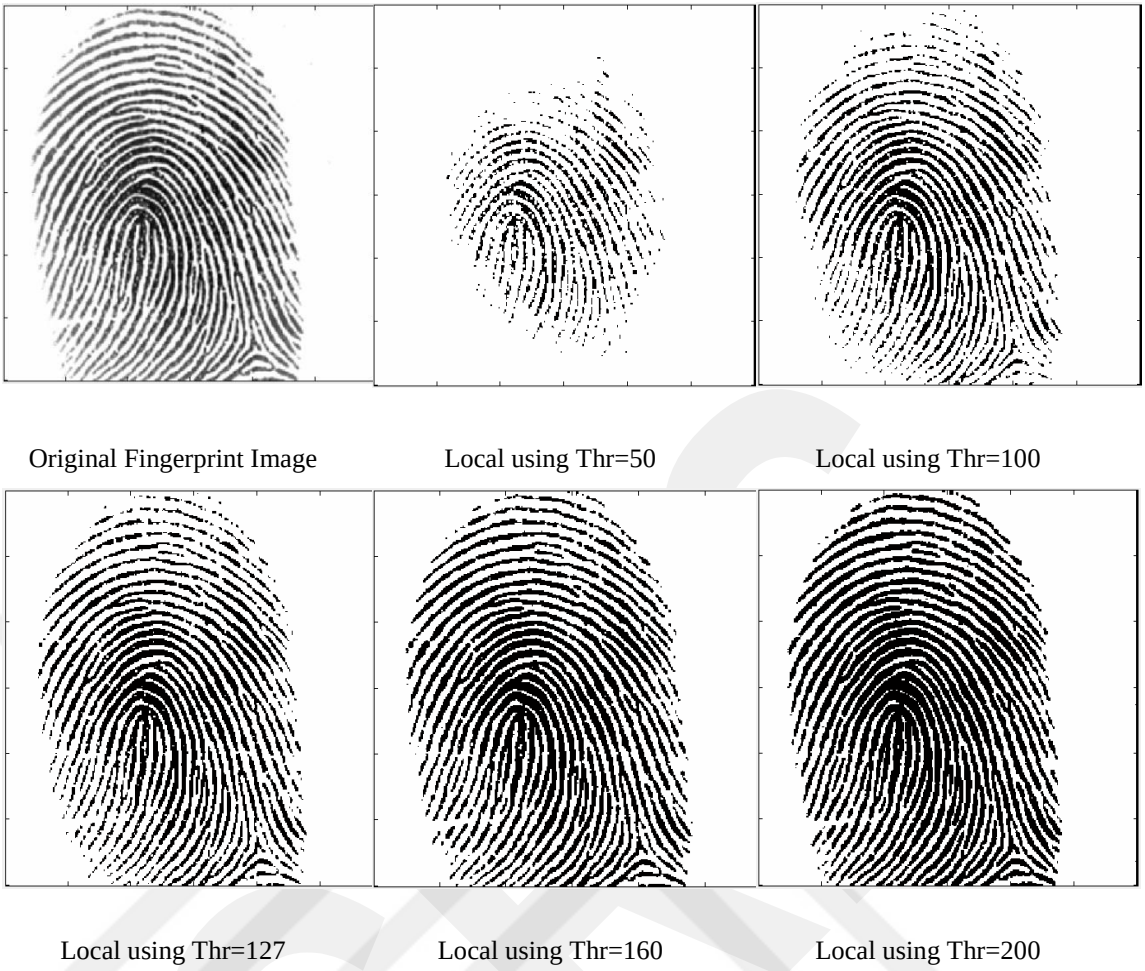


Figure 3.5: Local (manual) Image threshold

C. Thinning (Skeletonizing)

The Zhang-Suen algorithm (ZS algorithm) is a the Fast-Parallel based Algorithm for Thinning Digital Patterns. In this algorithm, a 3x3 window (mask) is moved down throughout the image and calculations are carried out on each ridge pixel, which has the value "1" and black color, in this case to decide whether it needs to stay in the image or not. Figure 3.6 which presents a description of the window and the classification that given to the pixels that surround the center pixel. Usually, the method consists of successive passes of two basic sub-iterations, until the image reaches a stable state. The iteration from one pixel to another used in this algorithm is clockwise [52].

P_9 (x-1,y-1)	P_2 (x-1,y)	P_3 (x-1,y+1)
P_8 (x,y-1)	P_1(x,y)	P_4 (x,y-+1)
P_7 (x+1,y-1)	P_6(x+1,y-1)	P_5 (x+1,y+1)

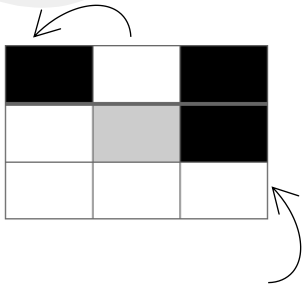
Figure 3.6: 3x3 Structuring Element

Regarding the 8-neighborhood notation in Figure 3.6:

Odd sub-iteration flags a point P1 for deletion or pixel ignoring if all the following conditions have been satisfied:

a. Count with connectivity 1.
   A(P1) = 1
b. Have several nonzero black neighbors, B(P1), between 2 and 6 (included).
   $2 \leq B(P1) \leq 6$
c. Have at least one of the following pixels in zero white:
   $[x-1, y], [x, y+1], [x+1, y]\ P2 \times P4 \times P6 = 0$
d. Have at least one of the following pixels in zero white $[x-1, y], [x+1, y], [x, y-1]$
   $P4 \times P6 \times P8 = 0$

Where A(P1) is total occurrences of 0-1 patterns (current pixel value 0 and next pixel value 1) in the ordered sequence P2, P3, P4, P5, P6, P7, P8, and P9, the "×" expresses logic "AND" operation, and the B(P1) function returns the number of nonzero black pixels in the structuring element as it shown in Figure 3.7 [53].



$A(P1) = 2, B(P1) = 3$

Figure 3.7: A(P1) and B(P1) Example

The proposed model used a compact representation called skeleton. In order to achieve faster processing and smaller memory fingerprint. A skeleton must

preserve the structure of the shape but all redundant pixels should be removed. In this module, the outer edge point of the fingerprint image is deleted iteratively until the skeleton points remain as a binary fingerprint image [54]. Algorithm 3.3 shows a thinning process [55].

Algorithm (3.3) Thinning

Inputs:

The binarized image

Output:

Thinning image

```
a [8]= kernel 3x3
For image height and width do
    ar= image data (0 and 1)
    p1 = a [0] * a[2] * a[6]
    p2 = a [0] * a[4] * a[6]
    b = number of 1's in current window (mask)
    If ar=1 and b>=2 and b<=6 and p1=0 and p2=0
        y =1
    Else
        y =0
    End If
End For
Set y to new image
End
```

The output of thinning module results for the local fingerprint feature extraction is illustrated by the example shown in Figure 3.8.

Original Fingerprint Image Global Binarization Result Thinning Result

Figure 3.8: Skeletonizing (Thinning) process result

We can notice that different binary fingerprint image gives different thinning (skeleton) image output. For example, if we used the local binarization (manual) process that effects on the output of the thinning results, as it is shown in Figure 3.9.

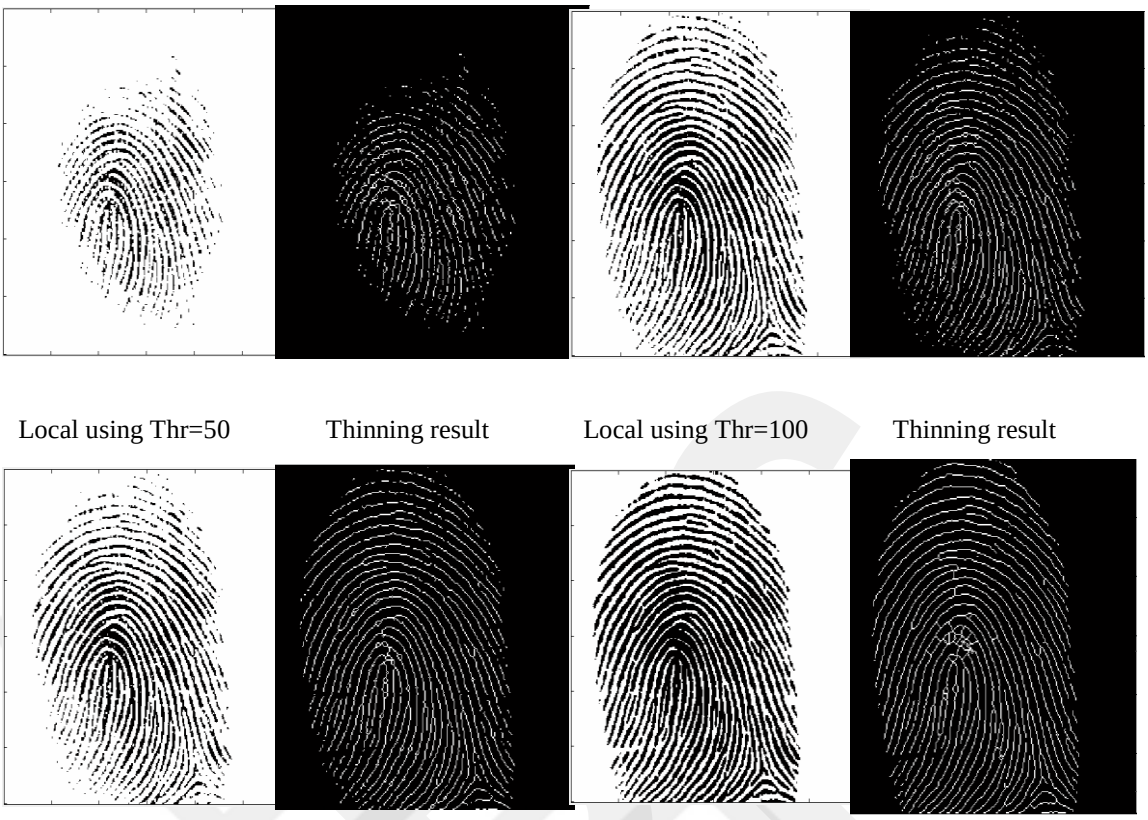


Figure 3.9: Different thinning results

D. Minutia Extraction

The extraction of minutiae points is a critical step in fingerprint authentication and verification systems. Ridge ending points and ridge bifurcation points are extracted from the thinned image after going through the minutiae extraction module in the local feature extraction approach. The extraction process starts by defining 3×3 structure element which is used to scan each pixel in the image.

The concept of Crossing Number (CN) is widely used for extracting the minutiae. This method extracts the minutia points from the skeleton image by examining the local neighborhood of each ridge pixel using a 3×3 window. CN is defined by Rutovitz as half the sum of the differences between the pairs of adjacent pixel. Rutovitz's definition [56] of CN for a pixel P_1 is

P_9	P_2	P_3
P_8	P_1	P_4
P_7	P_6	P_5

$$CN = \frac{1}{2}\sum_{i=2}^{9}|P_i - P_{i+1}| \quad (3.1)$$

Where Pi is the binary pixel value in the neighborhood of P1 with Pi = (0 or 1) and P10 = P2. Minutiae detection in a fingerprint skeleton is implemented by scanning thinned fingerprint and counting the CN [57]. Thus, the minutiae points can be extracted, as depicted in Table 3.1 and Figure 3.10.

For a pixel P1, the eight pixels are scanned in a clockwise direction. The pixel can be classified after obtaining its pixel value. A CN value of zero refers to an isolated point, value of one to a ridge ending, two to a continuing ridge point, three to a bifurcation point and a CN of four means a crossing point. The coordinates and type of minutiae of each minutiae point is recorded for each minutia [58].

Table 3.1: Crossing Number (CN)

CN	Property
0	Isolated point
1	Ending point
2	Connective point
3	Bifurcation point
4	Crossing point

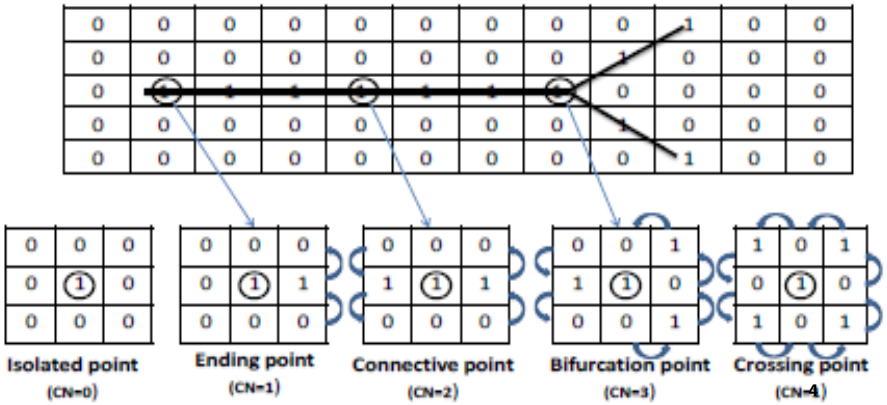


Figure 3.10: Illustration of CN properties ("1": black pixels in the skeleton image)

The CN for each pixel, which is the center of this structure, is calculated using equation (3.1). If the cross number for the pixel is 1, the pixel is considered as an end point and the position of the pixel and its neighbor are stored in "end points" list, and if the cross number for the pixel is 3, the pixel is nominated as "bifurcation point" the position of the pixel and its three neighbors are stored in bifurcation points list. The way to calculate CN is shown in Figure 3.10. This process is shown in the Algorithm 3.4 [58].

Algorithm 3.4: Minutia extraction

Inputs:

Lin() : continuous ridge thinning Image
Hgt : the height of thinning Image
Wid : the width of thinning Image

Output:

End(),Bi() // arrays of the position of end and bifurcation point

1. **Define** 3×3 structuring element p[9], 3×3 structure element for ridge position p1[9]
2. **Initialize** the counters
3. end_counter ← 0;
4. bi_counter ← 0;
5. **Scan** image with 3×3 structure element
6. **Calculating** CN for each pixel
7. $CN = \frac{1}{2}\sum_{i=2}^{9}|P_i - P_{i+1}|$
8. **Check** the value of the CN
9. **If** CN=1 Then
10. End(end_counter).x_position ←x;
11. End(end_counter).y_position ←y;
12. End(end_counter).x0_position ←x0;
13. End(end_counter).y0_position ←y0;

```
14.     end_counter ← end_counter+1;
15. Else if CN=3 Then
16.     Bi(bi_counter).x_position ←x;
17.     Bi(bi_counter).y_position ←y;
18.     Bi(bi_counter).x0_position ←x0;
19.     Bi(bi_counter).y0_position ←y0;
20.     Bi(bi_counter).x1_position ←x1;
21.     Bi(bi_counter).y1_position ←y1;
22.     Bi(bi_counter).x2_position ←x2;
23.     Bi(bi_counter).y2_position ←y2;
24.     bi_counter ← bi_counter+1;
25. End If
26. Return Bi(),End(), bi_counter, end_counter;
```

The results of the minutia feature extraction for different fingerprint images in the local fingerprint authentication approach are shown in Figure 3.11.

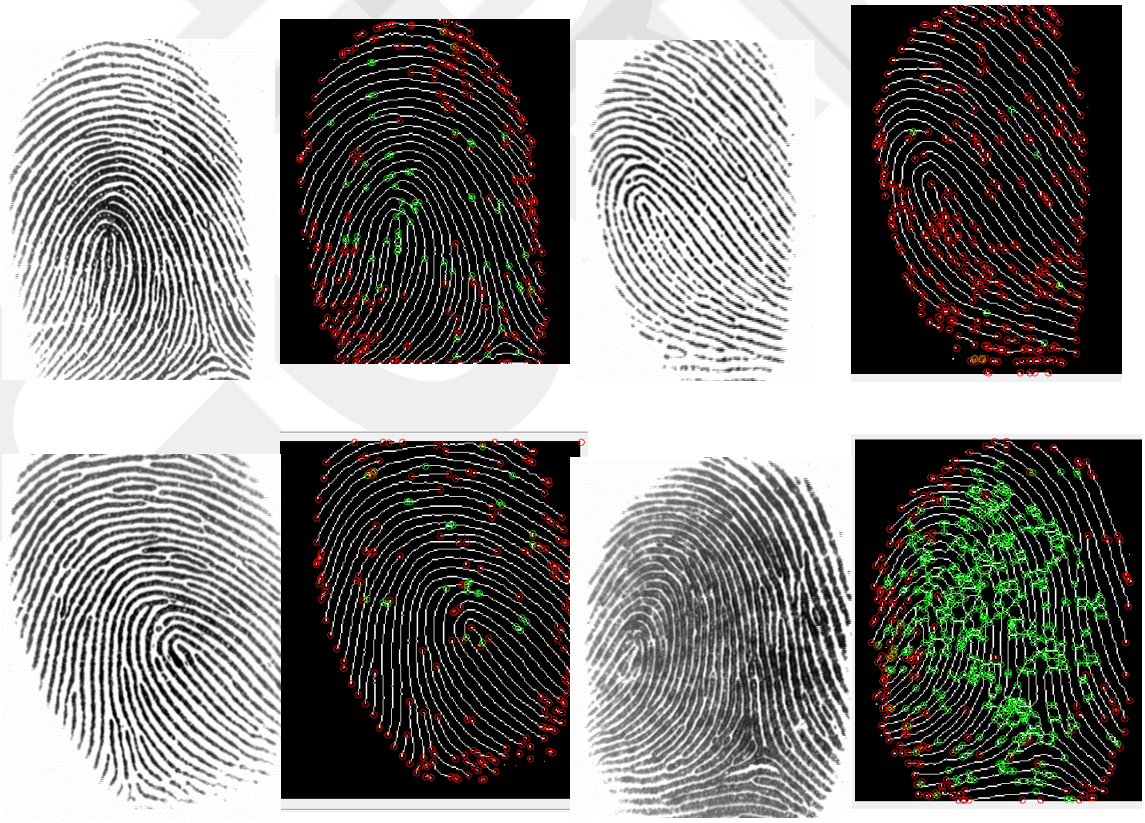


Figure 3.11: Minutia feature extraction results for the local approach

E. Remove False Minutia

The minutia extraction step incurs many errors as there will be many ridge-ends in border regions and spurious bifurcations and ridge-endings inside the fingerprint. Most of them are clearly recognizable to the trained eye, but in the case of an automatic system, a series of rules have to be used to delete the so-called "false-minutiae" [59].

The set of rules employed in false minutiae detection are able to efficiently find false minutiae that form one of the following structures: broken ridges, bridge, short ridges, hole, spur, and ladders [60]. Explanations of some false minutia structures are given in the following [61]:

- **Broken ridges:** Because of scars and insufficient finger pressure on the input device, a ridge may break into two ridges creating two endpoints. Obviously, these two endpoints are false minutiae and should be eliminated. These two endpoints are identified as a broken ridge structure.
- **Bridge structure:** Due to excessive finger pressure or noise in the image, two separate ridges are sometimes connected by a short ridge to make a bridge structure.
- **Short Ridge Structure**: All short ridges should be considered as false minutiae because they are usually artifacts introduced by image preprocessing procedure such as ridge segmentation and thinning.
- **Hole Structure:** Hole structures occur due to pores and dirt's on fingerprints. Vary wide ridges may generate hole structures.
- **Spur Structure:** Vary wide valley may generate spurs.
- **Spike Structure:** The spike structure generates two false minutiae and may occur when thinning a non-smooth ridge.
- **Ladder Structure:** Ladder structures usually occur between close ridges.

The most common types of false minutia structures which may be encountered into a thinned fingerprint image are shown in Figure 3.12. Each such structure generates two or more false minutiae [62].

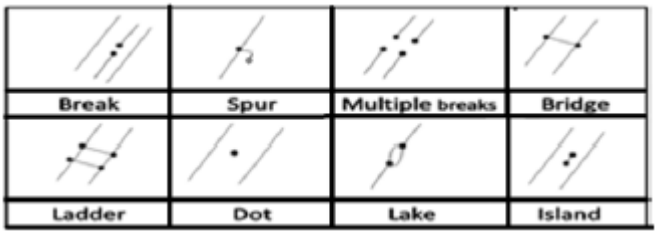


Figure 3.12: The most common false-minutia structure [62]

The minutiae points extracted in minutiae extraction module may contain false minutiae points due to noisy image or artifacts created by the thinning process. Some of the structures shown in Figure (3.13) with blue central point which have three neighbors may have three bifurcation points in the same structure, (i.e., the central is bifurcation point and two of its neighbors are also bifurcation points). If this case occurred, then we should consider the central point in the structures as the bifurcation point and its neighbors must be deleted from the bifurcation points list [62].

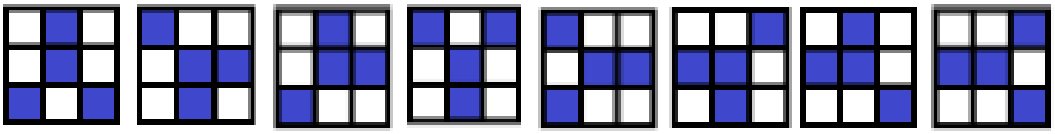


Figure 3.13: Structure elements for bifurcation points [61]

After the minutiae are extracted, it is necessary to employ post processing stage in order to validate that they are real minutia points. The two steps of postprocessing stage for minutia manipulation are:

1. Minutia invalidation with false minutia structures
2. Minutia validation. It can be seen.

The implemented steps for noise elimination module are illustrated in Algorithm 3.4. The process starts by defining a list of 3×3 structures which will be used to test each black pixel in the image. Then these 3×3 structures are passed over the image pixels to scan each black pixel in the image.

Figure 3.14 presents the adopted 3×3 structures in this work. If the central element of the structure has blue color then it will not be considered as noise point and must not be deleted; while those central pixels with the other colors (i.e., red, green, brown) are considered as noise points and must be deleted.

The central pixel of each structure, shown in Figure 3.14, represents the black pixel in the examined image that needs to be tested. All surrounding pixels within the area of the structure are tested and checked if they are black. If the surrounding black pixels in the (3×3) neighborhood met one of structures, then the central pixel should be deleted if its color in the found structure is not blue. After the entire pixels in the image are tested, the process is repeated. The repeated process includes handling black pixels which have two black neighbors and those have three black neighbors. The repetition is used to remove the remaining noise point which may not delete (or they created) in first iteration.

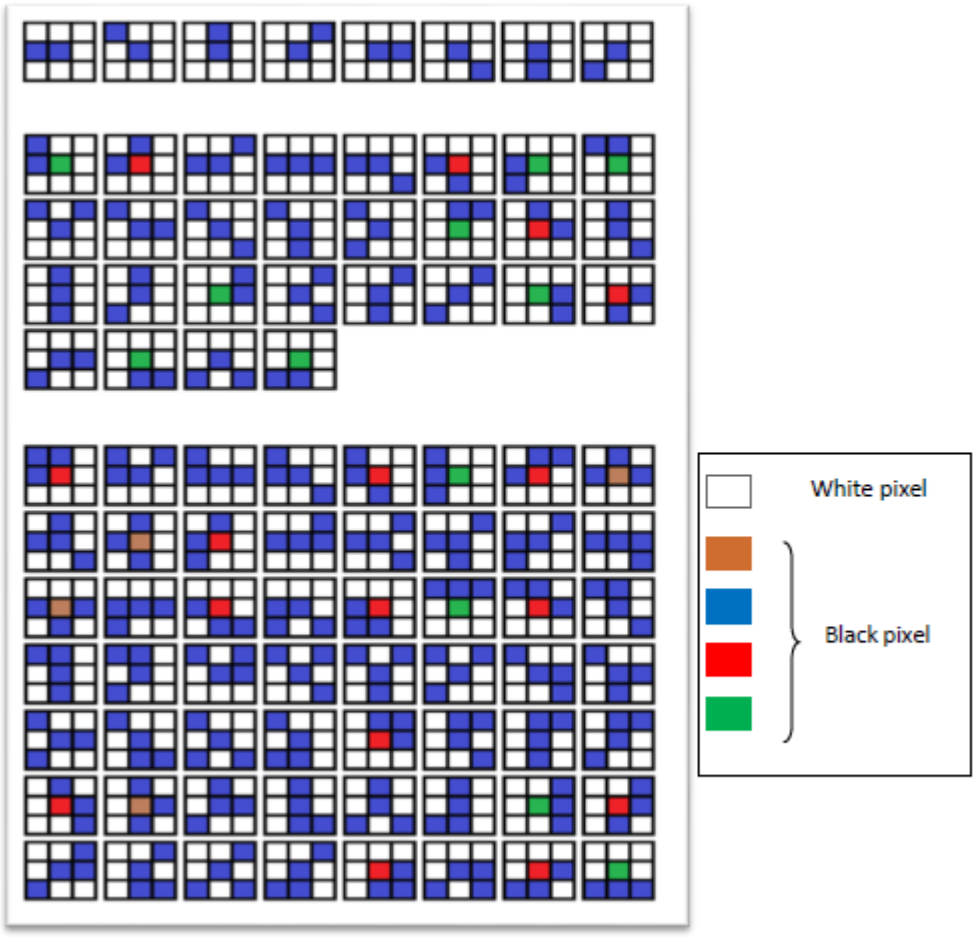


Figure 3.14: Structuring elements used in noise elimination process [62]

In third group, the cases with red and green center pixels lead to ridge points that have three neighbors belong to the ridge. This will confuse the minutia extraction algorithm by deciding that these ridgeline points are ridge bifurcations. The cases with brown centered pixels produce double ridge bifurcation points lying next to each other while, in fact, there is only one bifurcation point there. Algorithm 3.4 presents the implemented steps for noise removal task.

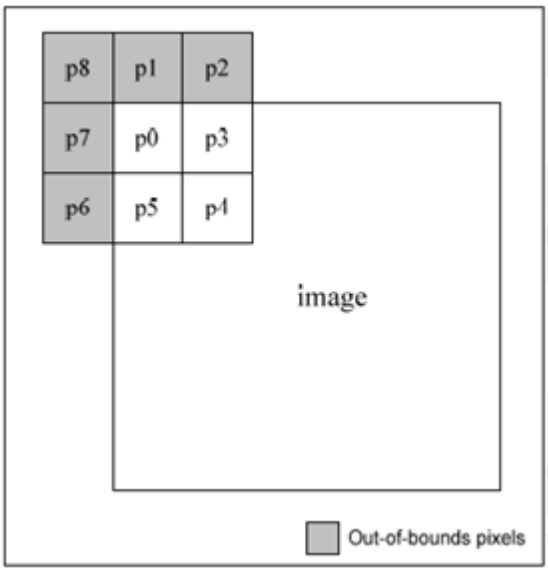


Figure 3.15: Example of out-of-bounds structuring elements [62]

Figure 3.11, that the spur structure generates false ridge ending, where both the hole and triangle structures generate false bifurcations. The spike structure creates a false bifurcation and a false ridge ending point. The set of rules employed for detection of false-minutiae that form one of the following structures: broken ridges, bridge, short ridges, spur, and ladders.

For minutia validation, this approach incorporates the validation of different types of minutiae into a single algorithm. It tests the validity of each minutiae point by scanning the skeleton image and examining the local neighborhood around the minutiae. The algorithm is then able to cancel out [62].

Algorithm 3.4: Remove False Minutia (Noise Elimination)

Inputs:

Thin() // array of binarized Thinning Image
Hgt // the height of Binary Image
Wid // the width of Binary Image

Output:

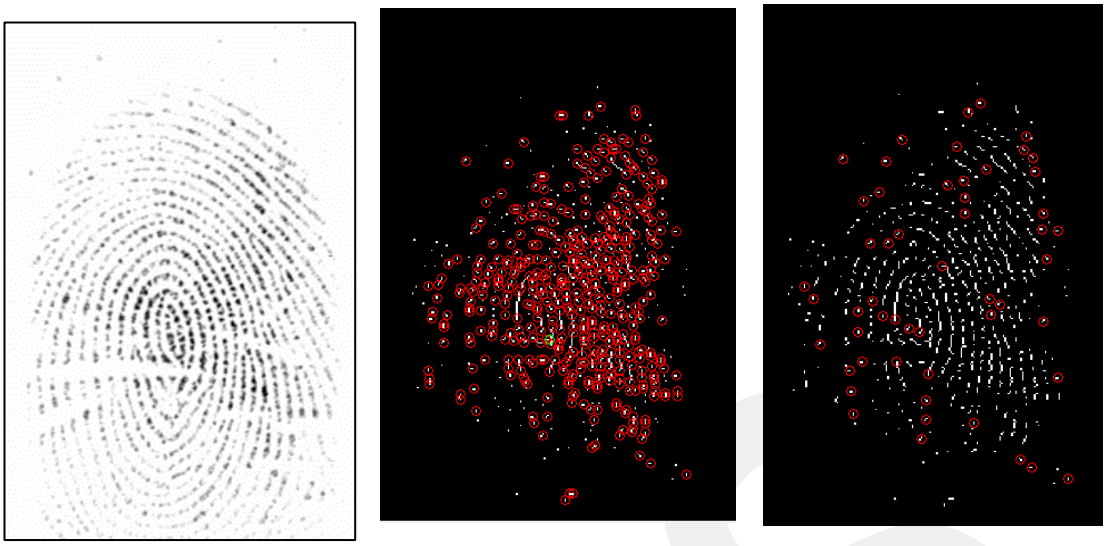
bb() // noise free array

1. **Define** 3×3 structuring element p[9],and expand the boundaries of the image with zero.
2. **Enter** Number of iteration for handling the Points with Two Neighbors
3. j←0;
4. **Repeat**
5. **Scan** each pixel, which has the value 1, with the 3×3 structuring element, p [9].
6. **Count** the number of surrounding neighbors which have values = 1
7. n ← 0;
8. **For** all i = 0 → 7
9. n ← n + p(i);
10. **End For** // i
11. **Meet** the conditions, when the pixel has two neighbors
12. **Check If** n = 2 Then
13. flg ← 0; //initialize flag with 0
14. **For** all i = 0 → 6 step 2 // check L shape
15. **Check If** p(i) = 1 And p(i + 2) = 1
16. Then flg ← 1;
17. **End If**
18. **End For** // i
19. **Check If** flg = 0 Then
20. **For** all i = 0 → 7
21. **Check If** p(i) = 1 And p(i + 1) = 1 Then flg ← 1; End If
22. **End For** // i
23. **End If**
24. **Delete** the pixel exactly like the condition met
25. **Check If** flg = 1
26. Then pixel ← 0;
27. **End If**
28. **End If**
29. **Until** j=itr;
30. **Enter** Number of iteration for handling the points with three neighbors
31. **Set** j←0;

```
32. Repeat
33.     Scan each pixel, which has the value 1, with the 3×3 structuring
        element, p [9].
34.     Repeat Step (6)
35.     Meet the conditions, when the pixel has three neighbors
36.     Check If n = 3 Then
37.         flg ← 0; //initialize flag with 0
38.         For all i = 0 → 6 step 2
39.             Check If p(i) = 1 And p(i + 2) = 1 And p(i + 4) = 1
40.                 Then flg ← 1;
41.             End If
42.         End For // i
43.     Check If flg = 0 Then
44.          For all i = 0 → 7
45.              Check If p(i) = 1 And p(i + 1) = 1 And p(i + 2) = 1
46.                  Then flg ← 1;
47.              End If
48.          End For // i
49.     End If
50.     Check If flg = 0 Then
51.         For all i = 0 → 3
52.          Case I of
53.                  0: Check If p(0) = 1 And p(2) = 1 And (p(7)
                    = 1 Or p(3) = 1)
54.                      Then flg ← 1;
55.                  End If
56.                  1: Check If p(2) = 1 And p(4) = 1 And (p(1)
                    = 1 Or p(5) = 1)
57.                      Then flg ← 1;
58.                  End If
59.                  2: Check If p(4) = 1 And p(6) = 1 And (p(3)
                    = 1 Or p(7) = 1)
60.                      Then flg ← 1;
61.                  End If
62.                  3: Check If p(6) = 1 And p(0) = 1 And (p(5) =
                    1 Or p(1) = 1)
63.                      Then flg ← 1;
64.                  End If
65.          End case
66.         End For // i
67.     End If
68.     Delete the pixel exactly like the condition met
69.     Check If flg = 1 Then
70.         pixel ← 0;
```

71. **End If**
72. **Until** j= itr;
73. **Repeat** Step 2 and all Step 3
74. **Return** bb();

The results of false minutia removing algorithm for local feature extraction are shown in Figure 3.16.



Origibnal Fingerprint Minuteia Feature Extraction False Minuteia Removing

Figure 3.16: False minutiae feature removing

F. ROI Extraction

The aim of this stage is to allocate the actual region in the fingerprint image by keeping the area within the bounding rectangle of ROI from the original image. The binary image is the input to this stage where the fingerprint ridges have the value "one" while the background has the value "zero". In order to determine the ROI in the image each side of the image boundary is scanned until we reach the row or column that contains ridge pixel(s) [62], as shown in Algorithm 3.5.

Algorithm 3.5: ROI Extraction

Inputs:

Bin() // array of binary image
Hgt // the height of binary image
Wid // the width of binary image

Output:

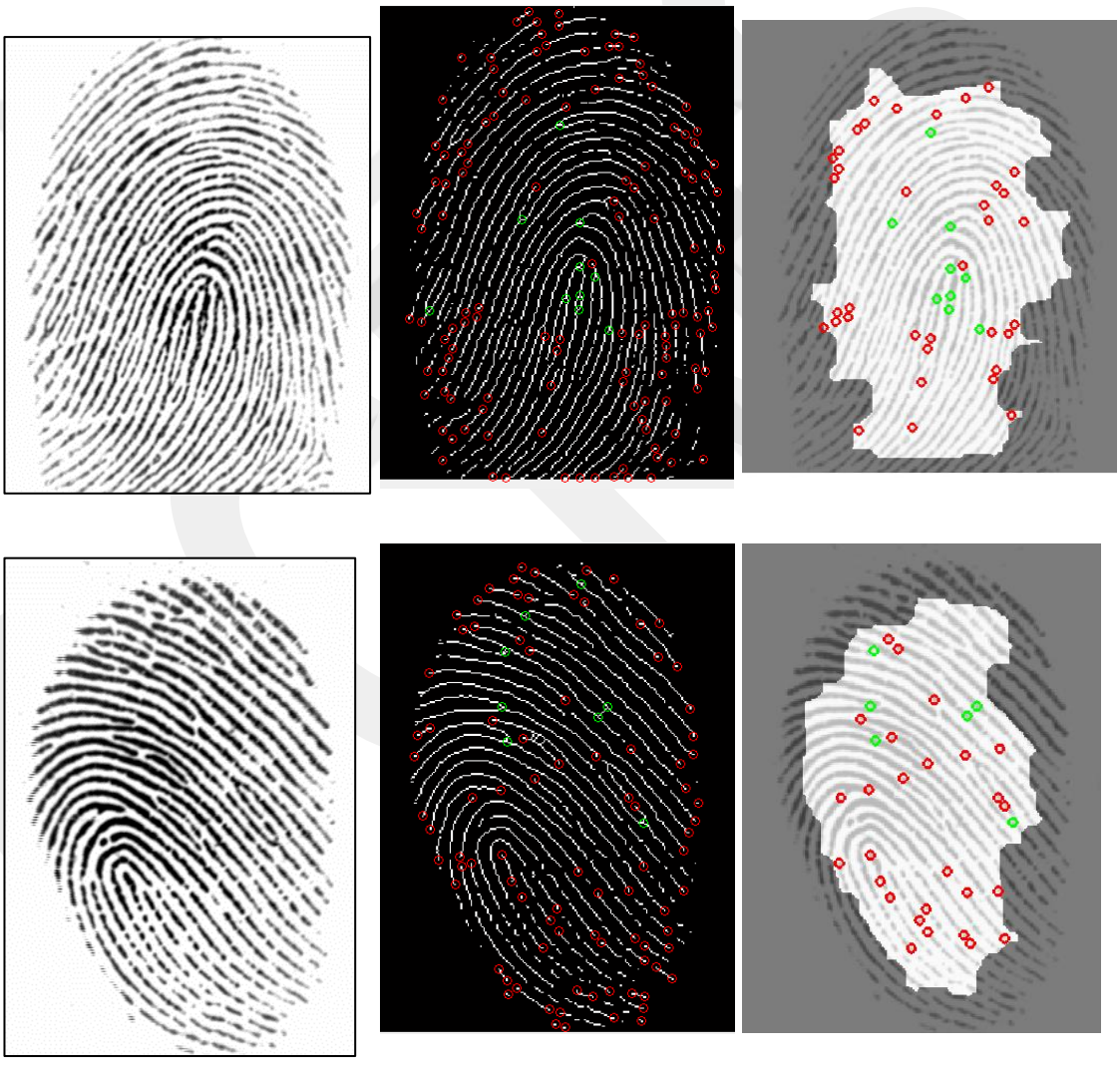
Clip() // ROI image

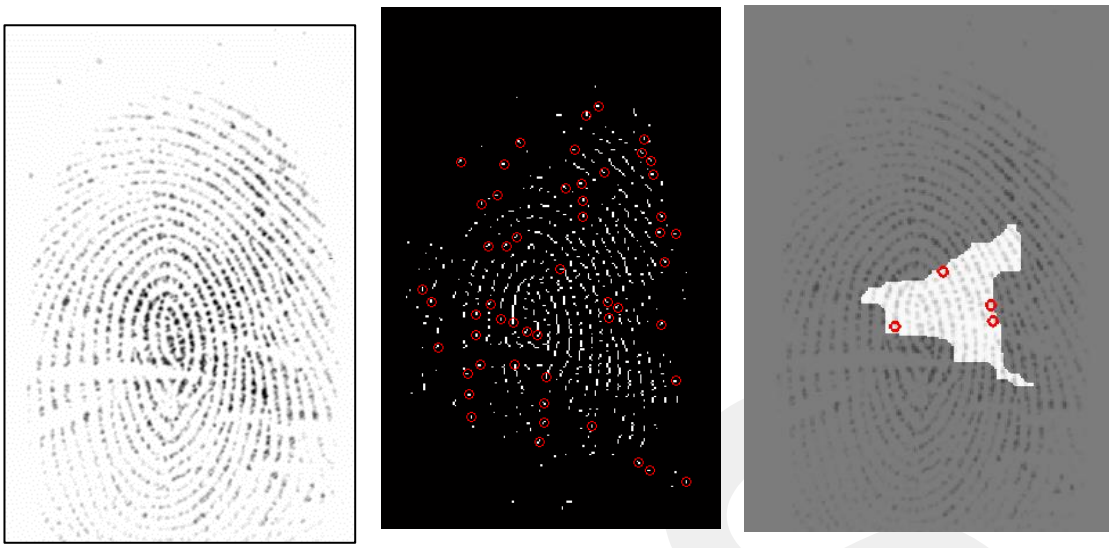
1. **Find** first row in the ROI
2. **For** all x = 0 → Wid-1
3. Set S←0; // initialize summation parameter
4. **For** all y = 0 → Hgt-1
5. S ← S + Bin(x, y);

```
            End For // y
            Check If S <> 0 Then
                X1 ← x;
                Exit For;
            End If
        End For // x
Find last row in the ROI
        For all x = Wid-1 → 0
            S←0; // initialize summation parameter
            For all y = 0 → Hgt-1
                S ← S + Bin(x, y);
            End For // y
            Check If S <> 0 Then
                X2 ← x;
                Exit For;
            End If
            x←x-1;
        End For // x
Find the first column
        For all y = 0 → Hgt-1
            S←0; // initialize summation parameter
            For all x = 0 → Wid-1
                S ← S + Bin(x, y);
            End For // x
            Check If S <> 0 Then
                Y1 ← y;
                Exit For;
            End If
        End For // y
Find last column in the ROI
For all y = Hgt-1→ 0
            S←0; // initialize summation parameter
            For all x = 0 → Wid-1
                S ← S + Bin(x, y);
            End For // x
            Check If S <> 0 Then
                Y2 ← y;
                Exit For;
            End If
            y←y-1;
End For // y
Cut the region
w ← X2 - X1 : Wid ← w;
h ← Y2 - Y1 : Hgt ← h;
```

```
50. For all y {where Y1 ≤ y ≤ Y2}
51.       For all x {where X1 ≤ x ≤ X2}
52.             Clip(x, y) ← Bin(x, y);
53.       End For // x
54. End For // y
55. Return Clip();
```

The results of region of interest detection (ROI) algorithm for local feature extraction are shown in Figure (3.17).



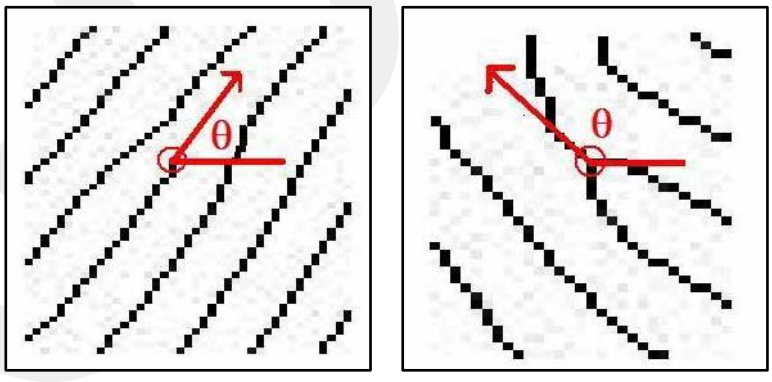


Origibnal Fingerprint Minuteia Feature Extraction False Minuteia Removing

Figure 3.17: ROI detection

G. Features Orientation

A termination angle is the angle between the horizontal and the direction of the ridge, while a bifurcation angle is the angle between the horizontal and the direction of the valley ending between the bifurcation. Figure 3.18 provides a visual description of these definitions [61].



Termination Angle Bifurcation Angle

Figure 3.18: Definition of minutiae angles

To compute the termination angles, the row and column indices for each termination are first recorded. Beginning at each termination, the corresponding ridge is traced backwards by five pixels, and the resulting row and column indices

are stored. Care must be taken to ensure the angle is calculated correctly. Algorithm (3.5) explain the orientation detection of each feature in the local feature extraction approach for fingerprint authentication [60] [61].

Algorithm 3.5: Features Orientation

Inputs:

ROI image

Output:

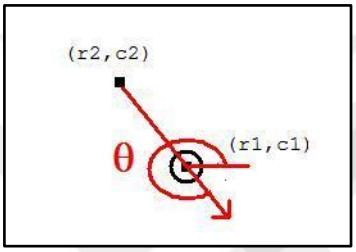
Orientation of each feature

1. **Find** the location of termination
2. **Find** location of the final pixel
3. **Set** r_1: row index of termination
4. **Set** c_1: Colum index of termination
5. **Set** r_2: row index of five-pixel ridge trace
6. Set c_2: column index of five-pixel ridge trace
7. **Check If** (r_1>r_2) and (c_1>c_2) then
8. $\theta = 360^{\circ} - tan^{-1}\left(\frac{r1-r2}{c1-c2}\right)$
9. **End IF**
10. **Check If** (r_2>r_1) and (c_1>c_2) then
11. $\theta = 90^{\circ} - tan^{-1}\left(\frac{r1-r2}{c1-c2}\right)$
12. **End IF**
13. **Check If** (r_1>r_2) and (c_2>c_1) then
14. $\theta = 180^{\circ} + tan^{-1}\left(\frac{r1-r2}{c1-c2}\right)$
15. **End IF**
16. **Check If** (r_2>r_1) and (c_2>c_1) then
17. $\theta = 90^{\circ} + tan^{-1}\left(\frac{r1-r2}{c1-c2}\right)$
18. **End IF**
19. **Check If** (r_1=r_2) and (c_1>c_2) then
20. $\theta = 0^{\circ}$
21. **End IF**
22. **Check If** (r_1=r_2) and (c_2>c_1) then
23. $\theta = 180^{\circ}$
24. **End IF**
25. **Check If** (c_1=c_2) and (r_2>r_1) then
26. $\theta = 90^{\circ}$
27. **End IF**
28. **Check If** (c_1=c_2) and (r_1>r_2) then

29. $\theta = 270^{\circ}$
30. **End IF**

The summarization of the rules that developed by the author in calculating of each angle is illustrated in Figure 3.19.

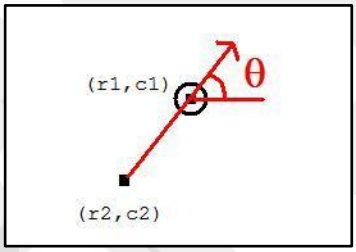
⊙	Location of termination
■	Location of final pixel of five-pixel trace



Check If (r_1>r_2) and (c_1>c_2) then

$$\theta = 360^{\circ} - tan^{-1}\left(\frac{r1 - r2}{c1 - c2}\right)$$

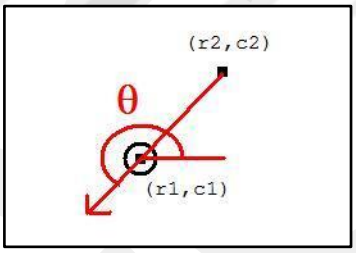
End IF



Check If (r_2>r_1) and (c_1>c_2) then

$$\theta = 90^{\circ} - tan^{-1}\left(\frac{r1 - r2}{c1 - c2}\right)$$

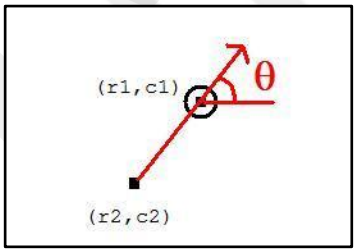
End IF



Check If (r_1>r_2) and (c_2>c_1) then

$$\theta = 180^{\circ} + tan^{-1}\left(\frac{r1 - r2}{c1 - c2}\right)$$

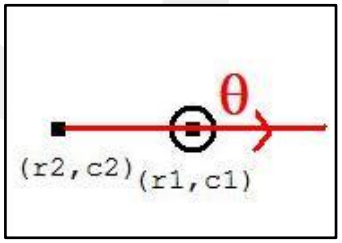
End IF



Check If (r_2>r_1) and (c_2>c_1) then

$$\theta = 90^{\circ} + tan^{-1}\left(\frac{r1 - r2}{c1 - c2}\right)$$

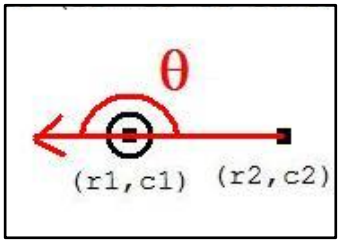
End IF



Check If (r_1=r_2) and (c_1>c_2) then

$$\theta = 0^{\circ}$$

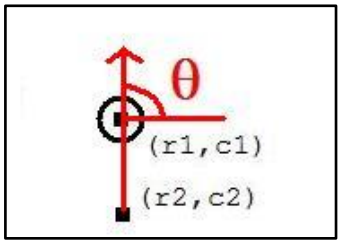
End IF



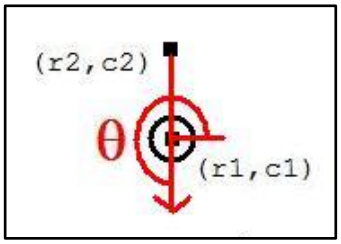
Check If (r_1=r_2) and (c_2>c_1) then

$$\theta = 180^{\circ}$$

End IF

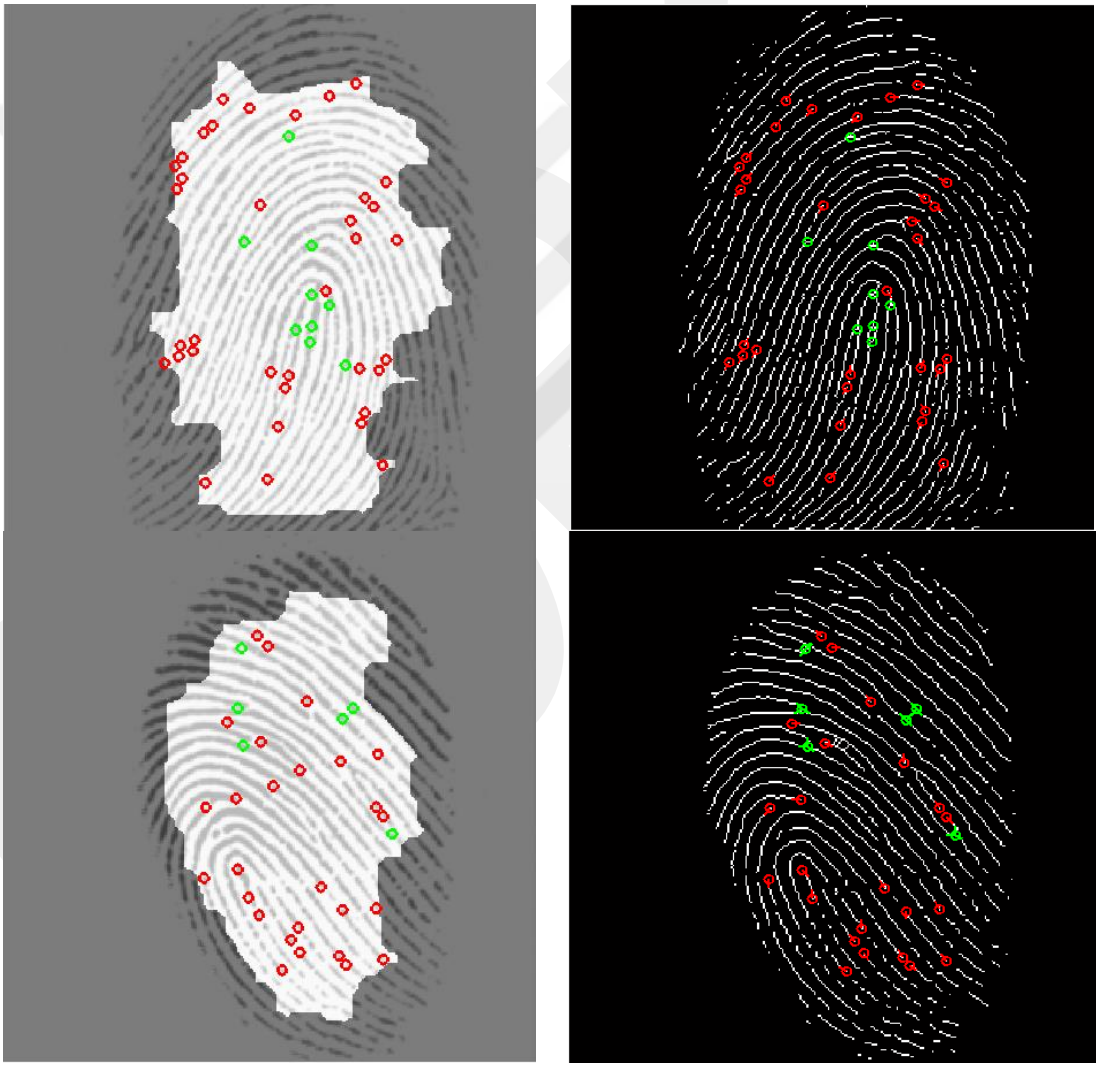


Check If (c_1=c_2) and (r_2>r_1) then
$\theta = 90^{\circ}$
End IF

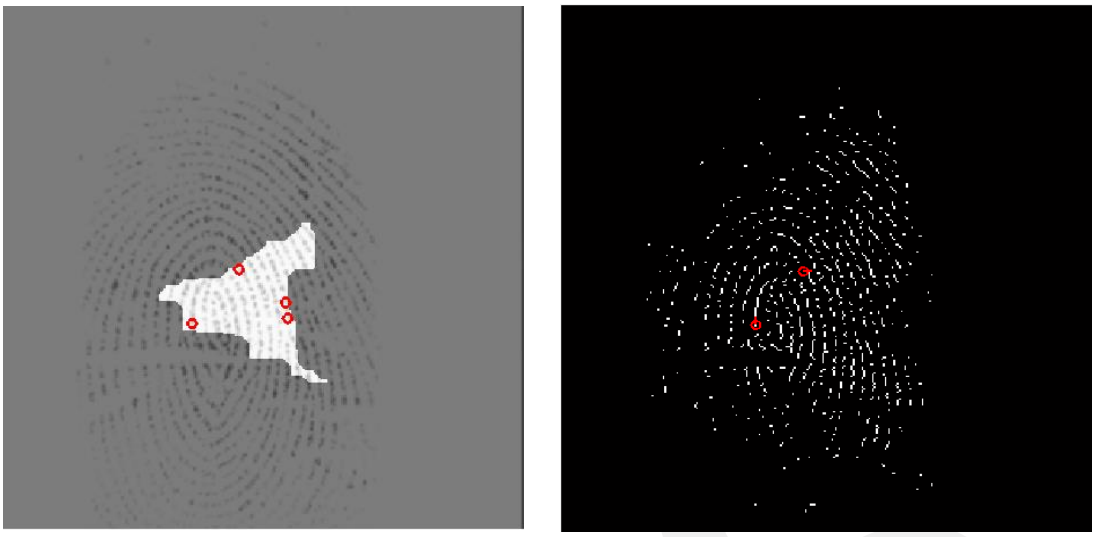


Check If (c_1=c_2) and (r_1>r_2) then
$\theta = 270^{\circ}$
End IF

Figure 3.19: Rules for calculating termination angles



The results of minutia feature orientation detection algorithm for local feature extraction are shown in Figure 3.20.



ROI Orientation Features Detection

Figure 3.20: Feature orientation detection

H. Matching Stage

In this stage, the matching process step involves the comparing between one set of the minutia features to another set. The compares process in this staged depends on the input features set that is previously stored data set with a known identity, referred to as a template. The matching template is also creating during the enrollment process by the user when presents a fingerprint image to the system as a purpose to collect the data. This feature information (data) is then stored as the defining characteristics (features) for that particular user.

Matching stage is the most important part for the local feature extraction approach for fingerprint authentication and verification. In this stage, the two features of the registered and requested features temples (I and R) that are extracted from the query and the references (registered) are compared between each other. In this stage, it returns a binary decision (matching/non-matching) or similarity score ($S(I,R)$) to indicate how the similar two participating fingerprints are in local feature extraction approach [61].

Minutia based fingerprint matching approach involves each for the correspondence between the two lists of the points in Hight-dimensional feature

space which is usually in three dimensional or higher space. Then, a triple $m = \{x, y, \theta\}$ is the most common representation of a minutia, where (x, y) is the location and $\theta$is the orientation of the minutia [60]. Therefore, the templates are represented as [60]:

$$I = \{m_1, m_2, \dots, m_a\}, m_i = \{x_i, y_i, \theta_i\}, \qquad i = 1, \dots, a \tag{3.2}$$

$$R = \{m'_1, m'_2, \dots, m'_a\}, m_i = \{x'_j, y'_j, \theta'_j\}, \qquad i = 1, \dots, b \tag{3.3}$$

Where a and b are the number of the minutia in I and R respectively. A minutia m'_j in R matches of the minutia m_i in I, if they are sufficiently close in terms of the spatial distance and orientation difference. Given two tolerance distance r_0 and θ_0, minutia m_i matches minutia m'_j if and only if [61]

$$\sqrt{(x_i - x'_j)^2 + (y_i - y'_j)^2} \leq r_0 \tag{3.4}$$

and

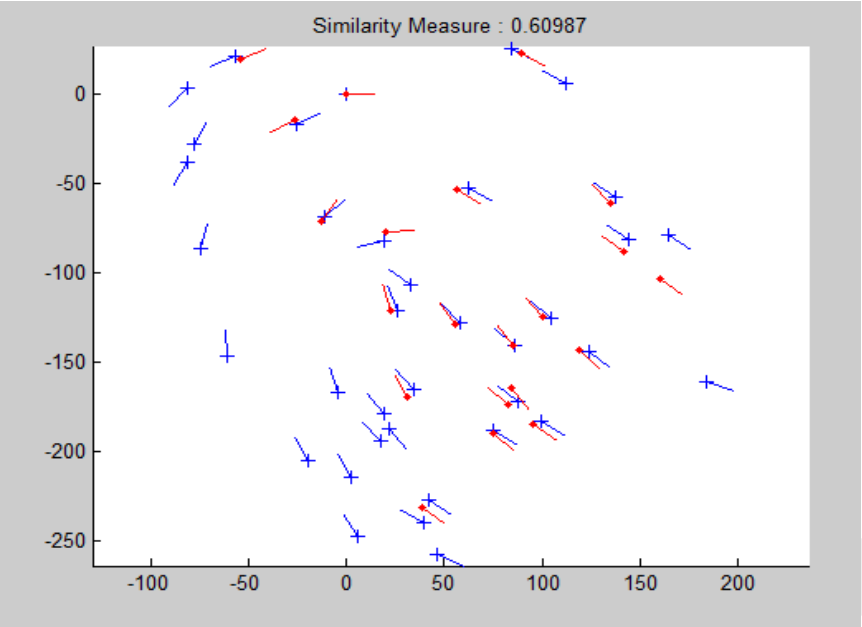
$$min(|\theta_i - \theta'_j|, 360 - |\theta_i - \theta'_j|) < \theta_0 \tag{3.5}$$

The results of minutia feature matching for local feature extraction are shown in Figure

Original Fingerprint image (I)

Requested fingerprint image (R)

3.21.



Matching Score result

Figure 3.21: Minutia matching score

3.5 Global Approach

The global feature extraction approach for fingerprint authentication view of the system consists of two main stages: The input stage and identification stage. The general structure of the global approach for fingerprint authentication and verification system is shown in Figure 3.19.

- **Input stage:** The system will input fingerprint image, person name, personal image and his information. then the system will apply the preprocessing on the input fingerprint image, calculate the seven values of invariant moments for this image and store all that in a database file.

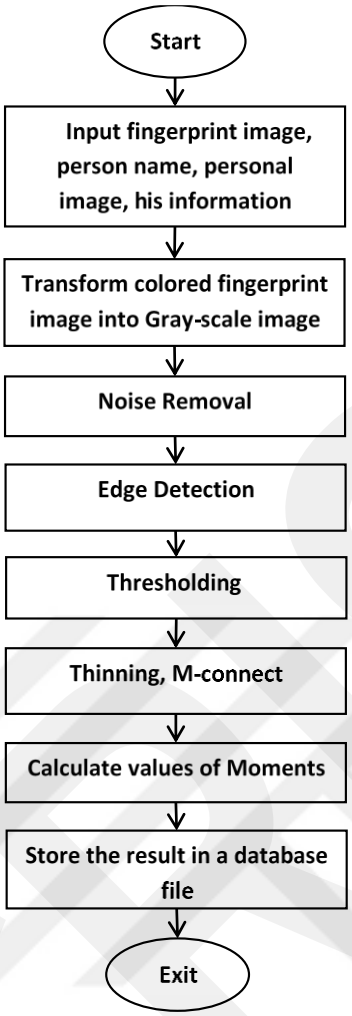


Figure 3.22: The Input stage flowchart

- **Identification stage:** The system will identify the input fingerprint image by calculate the moments values and compare the results with each moment's value stored in the database file and give the result according to a system ratio. The result is either yes or no. if it is yes then the system will display the person image and information. All these processes are shown in Figure 3.23.

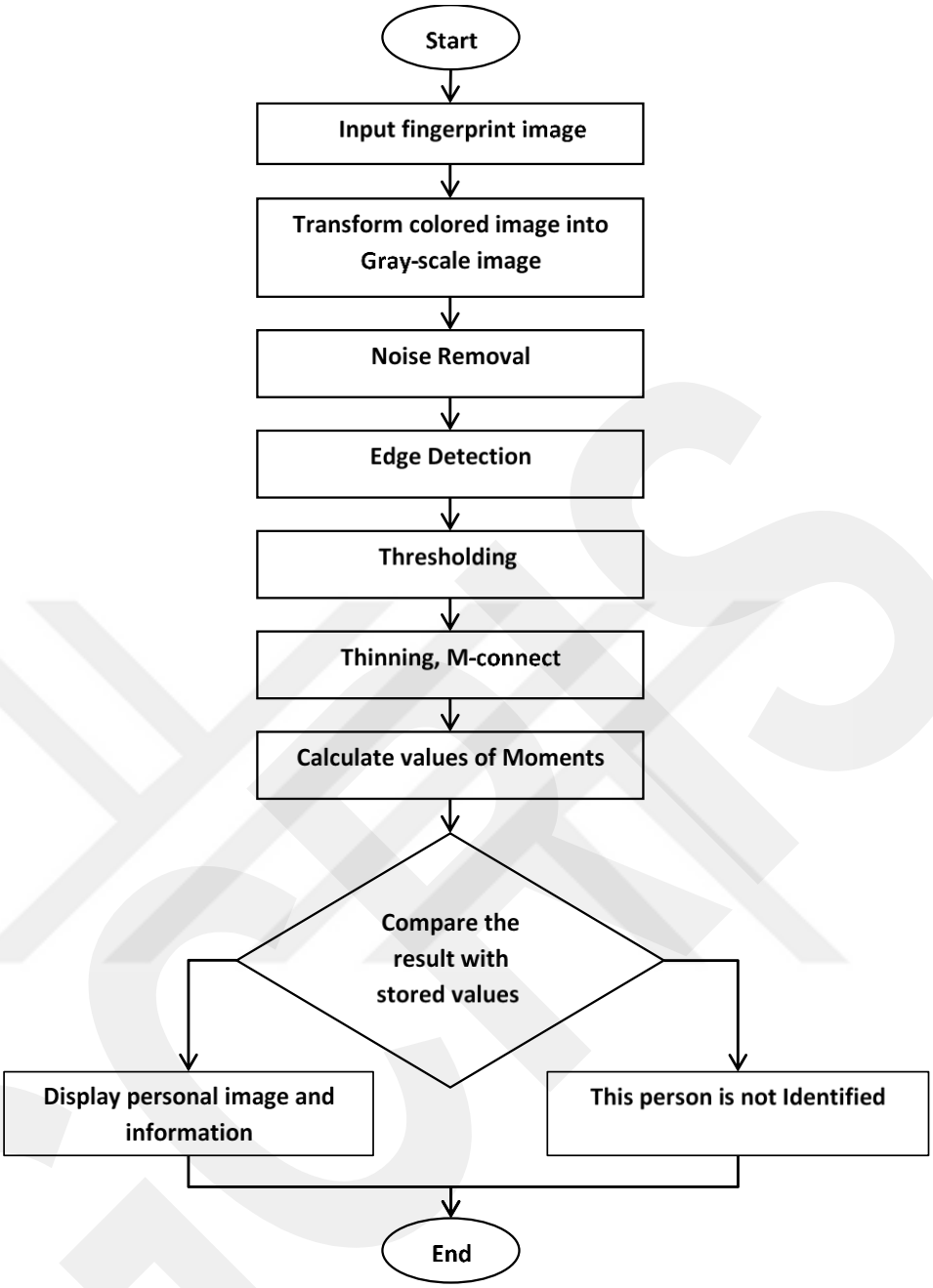


Figure 3.23: The Identification stage flowchart.

3.6.1 Transform colored image to Grayscale

The original and basic way of representing a digital colored image in a computer's memory is obviously a bitmap. A bitmap is constituted of rows of pixels, contraction of the words Picture Element. Each pixel has a particular value which determines its appearing color. This value is qualified by three numbers giving the decomposition of the color in the three primary colors Red, Green and Blue. Any color visible to human eye can be represented this way. The decomposition of a color in the three primary colors is quantified by a number between 0 and 255. For

example, white will be coded as R = 255, G = 255, B = 255; black will be known as (R, G, B) = (0,0,0); and say, bright pink will be (255,0,255). In other words, an image is an enormous two-dimensional array of color values, pixels, each of them coded on 3 bytes, representing the three primary colors. This allows the image to contain a total of 256x256x256 = 16.8 million different colors. This technique is also known as RGB encoding, and is specifically adapted to human vision. With cameras or other measure instruments we are capable of 'seeing' thousands of other 'colors', in which cases the RGB encoding is inappropriate.

Regarding the 3D color space, grayscale is symbolized by the straight generated by the (1,1,1) vector. Indeed, the shades of grays have equal components in red, green and blue, thus their decomposition must be (n, n, n), where n is an integer between 0 and 255. For example: (0,0,0) black, (32,32,32) dark gray, (128,128,128) intermediate gray, (192,192,192) bright gray, (255,255,255) white etc…). Now the idea of the algorithm is to find the importance a color has in the direction of the (1,1,1) vector. We will use scalar projection to achieve this. The projection of a color vector C = (R, G, B) on the vector (1,1,1) is computed by the following algorithm [62]:

Algorithm 3.6: RGB to Grayscale Conversion

Inputs:

Color Image

Output:

Grayscale Image

1. **For** every pixel (i, j) on the source bitmap
2. **Extract** the C = (R, G, B) components of this pixel.
3. **Compute** Grayscale(C) = (R+G+B)/3
4. **Mark** pixel (i, j) on the output bitmap with color (Grayscale(C), Grayscale(C), Grayscale(C)).
5. **End For**

The results of transform colored image from RGB to grayscale step is shown in Figure (3.24).

Original Fingerprint Image (RGB) Grayscale Fingerprint

Figure 3.24: Fingerprint image color transformation

3.6.2 Noise Removal:

Fingerprint image usually contains noise and other defects due to poor quality of the scanning device or similar reasons. Therefore, image enhancement is required. The performance of an invariant moments algorithm relies heavily on the quality of the input fingerprint images, so the typical purpose of image noise removal is to prepare for fingerprint feature by improving the clarity of ridges and furrows and suppress noise. It is however difficult to suppress noise and other spurious information, without corrupting the actual fingerprint pattern. Various image processing techniques have been proposed, and which to use depends on what type of image defects need to be suppressed. Some examples include compensation for non-uniform inking or illumination characteristics of an optical scanner [64].

A further example of image processing, closely related to image enhancement, is the segmentation of fingerprint images. A segmentation algorithm is used to decide which part of the image is the actual fingerprint and what part is the background. Discarding the background will reduce the number of false features detected. To enhance fingerprint image we used mean filtering which is a simple, intuitive and easy to implement method of smoothing images, reducing the amount of intensity variation between one pixel and the next. It is often used to reduce noise in images.

The idea of mean filtering is simply to replace each pixel value in an image with the mean (`average') value of its neighbors, including itself. This has the effect of eliminating pixel values which are unrepresentative of their surroundings. Mean filtering is usually thought of as a convolution filter. Convolution is a simple mathematical operation which is fundamental to many common image processing operators. Convolution provides a way of `multiplying together' two arrays of numbers, generally of different sizes, but of the same dimensionality, to produce a third array of numbers of the same dimensionality. This can be used in image processing to implement operators whose output pixel values are simple linear combinations of certain input pixel values.

The input arrays are normally just a gray-level image. The second array is usually much smaller, and is also two-dimensional, and is known as the kernel [65]. Often a 3×3 square kernel is used, as shown in Figure 3.25.

1/9	1/9	1/9
1/9	1/9	1/9
1/9	1/9	1/9

Figure 3.25: 3×3 kernel often used in mean filtering

The convolution is performed by sliding the kernel over the image, generally starting at the top left corner, so as to move the kernel through all the positions where the kernel fits entirely within the boundaries of the image. Each kernel position corresponds to a single output pixel, the value of which is calculated by multiplying together the kernel value and the underlying image pixel value for each of the cells in the kernel, and then adding all these numbers together. Mean filter is performed by the following algorithm [66]:

Algorithm 3.7: Mean filter

Inputs:

Input Image

Output:

Enhanced Image

1. **If** the image has *M* rows and *N* columns, and the kernel has *3* rows and *3*

columns,

2. then the size of the output image will have *M* rows, and *N* columns.
3. where i runs from 1 to *M* - *m* + 1 and *j* runs from 1 to *N* - *n* + 1.
4. **Removing** n - 1 pixels from the right-hand side and m - 1 pixels from the bottom will fix things.

The result of the image smoothing and noise removing step is shown in Figure 3.26.

Grayscale fingerprint image Noise removed fingerprint image

Figure 3.26: Fingerprint image noise removing

3.6.3 Edge Detection:

Edge detection methods are used as a first step in the line detection process. It is also used to find complex object boundaries by marking potential edge point corresponding to places in some where rapid changes in brightness occur. After these edge points, have been marked they can be merged to form lines and object outlines.

The appearance of edges is caused by changes in color or texture or by the specific lighting conditions present during the image acquisition process. Edge detection operators are based on the idea that edge information in an image is found by locking at the relationship a pixel has with its neighbors. If a pixel's gray-level value is similar to those around it, there is probably not an edge at that point. If a pixel has neighbors with widely varying gray-levels, it may represent an edge point.

So, an edge is defined by the discontinuity in gray-level values. Ideally, an edge separates two distinct objects.

In this work, the sober filter is used as one of the edge detection operators. Sobel operator performs a 2-D spatial gradient measurement on an image. Typically, it is used to find the approximate absolute gradient magnitude at each point in an input grayscale image. The Sobel edge detector uses a pair of 3x3 convolution masks, one estimating the gradient in the x-direction (columns) and the other estimating the gradient in the y-direction (rows). A convolution mask is usually much smaller than the actual image. As a result, the mask is slid over the image, manipulating a square of pixels at a time. The actual Sobel masks are shown below [67]:

-1	0	+1
-2	0	+2
-1	0	+1

Gx

+1	+2	+1
0	0	0
-1	-2	-1

Gy

Figure 3.27: 3×3 Sobel kernel often used in edge detection filtering

The magnitude of the gradient is then calculated using the formula:

$$|G| = \sqrt{Gx^2 + Gy^2} \tag{3.6}$$

An approximate magnitude can be calculated using:

$$|G| = |Gx| + |Gy| \tag{3.7}$$

The mask is slid over an area of the input image, changes that pixel's value and then shifts one pixel to the right and continues to the right until it reaches the end of a row. It then starts at the beginning of the next row.

The result of edge detection process of the fingerprint image is shown in Figure 3.28.

Noise removed fingerprint image Edge detection fingerprint image

Figure 3.28: Fingerprint edge detection using sobel filter

3.6.4 Threshold:

Thresholding is an image processing technique for converting a grayscale or color image to a binary image based upon a threshold value. If a pixel in the image has an intensity value less than the threshold value, the corresponding pixel in the resultant image is set to black. Otherwise, if the pixel intensity value is greater than or equal to the threshold intensity, the resulting pixel is set to white. Thus, creating a binarized image, or an image with only 2 colors, black (0) and white (255). Image thresholding is very useful for keeping the significant part of an image and getting rid of the unimportant part or noise. This holds true under the assumption that a reasonable threshold value is chosen [68]. The threshold value operates by first reading the grayscale value at the first entry and coming up with a pixel intensity between 0 and 255. It increments the total number of pixels and then it will then move on to the next row, column entry until it finishes reading all the raster data. However, while it's reading each entry, if it picks up a pixel intensity value more than once it will increment that particular value [63] [64].

Algorithm 3.8: Thresholding

Inputs:

Enhanced Image

Output:

Threshold Image

```
1. The histogram for image is computed as follows:
2.     Compute its peak limit(P_L)
3.     P_L=Sum of all color values of pixels
4.     Repeat
5.         If pixel>P_L then
6.             Set pixel to foreground
7.         Else
8.             Set pixel to background
9.     Until no more pixels exist
```

The result of thresholding process of the fingerprint image is shown in Figure 3.29.

Edge detection fingerprint image Thresholding result

Figure 3.29: The thresholding results

3.6.5 Thinning

Thinning process allows the lines thickness in an image to be reduced to one pixel wide. In general, the thinning process of the digital image is very time consuming according to the intensive process steps starting from the image is scanned from beginning to end as well as examining the neighborhood of each pixel and checking whether it can be deleted. Typically, 20 - 30 such scans (or passes) are required to thin an image. In this case a pixel is deleted where the value of the tested pixel is changed from 255 to 0. Then, the image is said to be change during this process. Finally, the total number of pixels us deleted in one pass constitutes according to the total number of changes in that pass.

There are several problems with applying thinning technique and they are:

- A lot of information may be lost during the thinning process.
- Thinning process is time consuming due to the iterative nature.
- Thinning technique is unsatisfactory when applied to low quality images.

The skeleton of region may be defined via the Medial Axis Transformation (MAT) approach. The MAT of a region R with border B is as follows: for each point value (p) in R, we find its closest neighbor in B. If p has more than one such neighbor, then it is said to belong to the medial axis (skeleton) of R [65]. It is assumed that the region points have value 255 while background points have value 0. Contour point is any pixel with value 255 and having at least 8-neighbor valued 0. The 8-neighborhood.

The result of thinning process of the fingerprint image is shown in Figure 3.30.

Thresholding result Thinning result

Figure 3.30: The thinning results

3.6.6 Invariance Moments of Two –Dimensional Function:

Recently, Invariant Moments Function (IMF) has been frequently used for the image processing as well as with remote image sensing, shape analysis, recognition and classification. Moment function provides some characteristics or feature space for an object the is uniquely represent. In moment function the invariant shape recognition is performed by classification process in the multidimensional moment invariant feature space. I this case, there is several techniques have been developed by derive the invariant features from moments for object analysis, recognition and representation. These techniques are mainly distinguished by their moment definition (feature values), such as the type of data exploited and the method for deriving invariant values from the image moment values [69].

Traditionally, the moment invariant is computed based on the information that provided by both the shape boundary and its interior region for the same shape. The moment function (moment values) is used to construct the moment invariant which are defined in the continuous signal value but for practical implementation they are computed in the discrete form. For example, by given a function $f(x,y)$, we will assume that the function $f(x,y)$ is a non-negative function with finite values on a bounded image plane. In this case, before we moving on to later steps, that give an illustrative example on moment calculation [70].

A uniqueness theorem that proposed by (Papoulis, 1991) which states that if the function $f(x,y)$ is piecewise continuous and has non-zero values that happen in only a finite part of the x,y plane. In this case, the moments (values) of all shape order is existed and the moment sequence (m_{pq}) is uniquely determined by the function $f(x,y)$. Conversely, this form the (m_{pq}) uniquely determines the function $f(x,y)$ [70].

The central moments of the first order can be expressed as [70]:

$$m_{00} = \sum_{x,y} f(x,y) \tag{3.8}$$

The total mass of the function (which presents the global energy of the whole image in the first order) is given by the moment m_{00}. When the function has been normalized so that it has unit mass it is sometimes called a probability function. The centroid of $f(x,y)$ is the point at which it will balance. The coordinates of the

centroid are found as shown at the right. Note that the function is normalized by dividing by the mass.

$\bar{x} = \frac{m_{10}}{m_{00}}$	(3.9)
$\bar{y} = \frac{m_{10}}{m_{00}}$	(3.10)

For a digital image, the general equation becomes;

$\mu_{pq} = \sum_{x}\sum_{y}(x-\bar{x})^{p}(y-\bar{y})^{q} f(x,y)$	(3.11)

The central moment is obtained by shifting the origin to the centroid of the function. Of order, up to 3 are

$$\mu_{10} = \sum_{x}\sum_{y}(x-\bar{x})^{1}(y-\bar{y})^{0} f(x,y) \quad (3.12)$$

$$\mu_{10} = \mu_{10} - \frac{\mu_{10}}{\mu_{00}}(\mu_{00}) = 0 \quad (3.13)$$

$$\mu_{11} = \mu_{11} - \frac{\mu_{10}\,\mu_{01}}{\mu_{00}} \quad (3.14)$$

To the end equations ($\mu 20, \mu\ 02, \mu\ 12, \mu\ 21, \mu\ 30, \mu\ 03$), where μ is the central moment. The normalized central moment of order $(p+q)$ is obtained by dividing the central moment of the same order by a normalization factor. The factor is a function of p and q. Normalized central moments are:

$$\eta_{pq} = \frac{\mu_{pq}}{\mu_{00}^{\gamma}} \quad (3.15)$$

where

$$\gamma = \frac{p+q}{2} + 1 \ , for\ p,q = 1,2,3,4,\dots,n \quad (3.16)$$

A set of the seven invariant moments (feature values) can be defined by combining the normalized central moments [68] [69] [70].

$$\phi_1 = \eta_{20} + \eta_{02} \quad (3.17)$$

$$\phi_2 = (\eta_{20} + \eta_{02})^2 + 4\,\eta_{11}^2 \quad (3.18)$$

$$\phi_3 = (\eta_{30} + 3\,\eta_{12})^2 + (3\,\eta_{21} - \eta_{03})^2 \quad (3.19)$$

$$\phi_4 = (\eta_{30} + \eta_{12})^2 + (\eta_{21} + \eta_{03})^2 \quad (3.20)$$

$$\phi_5 = (\eta_{30} - 3\,\eta_{12})(\eta_{30} + \eta_{12})[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2 + (3\,\eta_{21} - \eta_{03})(\eta_{21} + \eta_{03})] \quad (3.21)$$

$$\phi_6 = (\eta_{20} - \eta_{02})[(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2] \quad (3.22)$$

$$\begin{aligned}\phi_7 = (3\,\eta_{21} - \eta_{03})(\eta_{30} - \eta_{12})[(\eta_{30} + \eta_{12})^2 \\ - 3(\eta_{21} + \eta_{03})^2] \\ + (3\,\eta_{12} - \eta_{30})(\eta_{21} - \eta_{03})[3(\eta_{30} + \eta_{12})^2 \\ - (\eta_{21} + \eta_{03})^2]\end{aligned} \tag{3.23}$$

3.6.7 Matching

After extracting seven features of fingerprint image from the above section, system must search for identifying person who has these features. To do so, a matching process is applied to compare the entire values with stored values in a database file. Matching process depends on the matching result for each moment value by using these equations:

Algorithm 3.9: Matching

1. **Set** the estimation ration value $\boldsymbol{R_{Estimation}} = 0.05$ which present the error estimation value.
2. **i:** the total number of the fingerprint images in the database.
3. $\boldsymbol{Tested\_Moment_{feature\ vector}}$: the moment feature vector for the tested fingerprint image
4. $\boldsymbol{All\ Moment_{feature\ vectors}}$ [i]: the moment features for the whole fingerprint images in the database.
5. **Compute** range value of the moment vector by $\boldsymbol{Ratio} = Tested\_Moment_{feature\ vector} \times Ratio_{estimation}$
6. **Compute** lower range value $(R1)$ of the extracted features by $\boldsymbol{R_1} = Tested\_Moment_{feature\ vector} - R$
7. **Compute** upper range value $(R2)$ of the extracted features by $\boldsymbol{R_2} = Tested\_Moment_{feature\ vector} - R$
8. **For i**=1: total number of moment feature vector in the database
9. **If** $(All\ Moment_{feature\ vectors}[i] >= R_1$ and $All\ Moment_{feature\ vectors} <= R2_2)$
10. **If** $(All\ Moment_{feature\ vectors}[i] <= Tested\_Moment_{feature\ vector})$ then
11. $\boldsymbol{Matching} = Initial\ Ratio \times (All\ Moment_{feature\ vectors}[i] / Tested\_Moment_{feature\ vector})$
12. **Else**
13. $\boldsymbol{Matching} = Intial\ Ratio \times (Tested\_Moment_{feature\ vector} / All\ Moment_{feature\ vectors}[i])$
14. **Else**
15. $\boldsymbol{Matching} = 0$;

CHAPTER 4

EXPERIMENTAL RESULTS

4.1 Introduction

In this chapter, the results of conducted tests are presented. A set of tests have been conducted in order to evaluate the accuracy of the established fingerprint verification system, as well as to explore the effects of the different involved system parameters on the overall system performance. Also, the results of the analysis stage which was conducted to assess the discrimination capabilities of the extracted fingerprint features are illustrated.

4.2 Research Methodology

In this part, we will introduce the research methodology that we rely on to use the dataset for the experimental results for the fingerprint identification and verification system. In this task, we use both Local based minutia feature extraction approach and Global based feature extraction for fingerprint identification and verification system. Our research methodology can be summarized in the following steps:

1. We have implement the local based feature extraction approach which is the standard approach for the fingerprint identification and verification task in the market as we have discussed before in chapter three in details. Then we also have implement the Global based feature extraction approach as a proposed approach to solve such a particular issue in the fingerprint identification and verification task which is the incomplete fingerprint images identification and verification task. In case to state that that the Local based feature extraction approach is the more efficient and standard one that has been used in the fingerprint identification and verification market, we have implemented this

approach and compare it with the other more recently related works as it will show and discuss in sec. 4.6.2 in the experimental results.

2. In this part, we have select the partial (incomplete) fingerprint image identification and verification problem as the main challenge issue that we would like to present in this approach which present such a challenge problem that still an open problem till now. This kind of problem is most recently fingerprint problem that has been studied since it presents such a difficult situation in this task. In this case, to study the behavior (performance results) of both Local based feature extraction and the global based feature extraction for the incomplete fingerprint image identification and verification task, we generate random dataset that has many random cases from the incomplete fingerprint images. Since there is no such a standard dataset that has the particular issue that we want to solve such as the standard dataset in FCV2002,2004,2006, we generate those random images in the dataset that it has generated based on my color fingerprint by using the color scanner (Canon PIXMA E404) just in case to make the generated dataset more challenges by choose them as color and incomplete fingerprint images.

3. Our methodology steps for this task (dataset generation) is based on generating the partial fingerprint images (incomplete fingerprint dataset) that have been used in both Local and Global based feature extraction approaches for fingerprint identification and verification task are explained below:

   A. **Random Shape Generation:** In this step, we have designed and implemented a MATLAB code for random shape generating, each shape has four Radom points that are randomly generation depends on the dimension of each image just to make sure that each random shape has to be inside the fingerprint image.

   B. **Incomplete Fingerprint Generation:** In this step, we have measured the dimensionality for each shape inside the fingerprint image and generate the incomplete fingerprint image by cutting and omit the random shape for the fingerprint image and keep the rest. In this case,

the total number of the fingerprint image that we have generating is 1200 incomplete fingerprint image.

C. **Folds Generation:** In this step, we have reorder the generated fingerprint images according to the size of each shape and order them in 10 folds. Each fingerprint image has randomly generated just in case to make blind and random selection for the incomplete fingerprint images. Each fold has a specific number of incomplete fingerprint images according to the quantitative size the missing Radom part.

D. **Random Selection:** In this step, we have blindly and randomly selected three fingerprint images for each fold. Then the final dataset has 30 incomplete fingerprint images that we will use later for the both approaches (Local and Global) for the incomplete fingerprint identification and verification task.

E. **Image Elimination:** In this case, there is some the random shape that is randomly generated is outstanding shape of the fingerprint image dimension. In this case, we have manually selection this image and isolated in the Image Elimination fold which we named as "Image Elimination fold".

4. For our testing methodology, we will do our experimental results depending on two main parts as they will have illustrated and discuss later in the experimental results.

A. **Experimental Results 1:** we first test the local based feature extraction approach on such a standard dataset such as FCV2006 just in term to satisfy that this approach has achieve a better accuracy in this task.

B. **Experimental Results 2:** In this experimental result, we test the local approach based feature extraction on the incomplete fingerprint images dataset that we have generated just in case to study the behavior of the local approach on such a challenged dataset. Moreover, we have test the Global feature extraction approach on same incomplete fingerprint

images dataset just in case to measure the ability of our proposed approach to solve this issue. Finally, we compare the results of the Local and Global feature extraction based approach just to approach that our approach has achieved better accuracy on the incomplete fingerprint image identification and verification.

4.3 Implementation Environment

The developed system has been established and implemented using Visual C++ programming language, MATLAB 2014, Microsoft Excel 2010, and the tests have been implemented under the environment of Windows-10 operating system, laptop computer processor: Intel Core i5-3337U, CPU 1.80 GHz, and (4GB) RAM.

The overview of the hardware environment of our system that has been used for testing our approach local and global approaches for fingerprint authentication and verification system is shown in Figure 4.1.

Figure 4.1: Computer specification that used for our program execution

4.4 Datasets

In this proposed system, we used two different datasets. The first one is the last version of the fingerprint dataset which is gray scale fingerprint images (FVC2006 fingerprint database) "R. Cappelli, M. Ferrara, A. Franco and D. Maltoni, "Fingerprint verification competition 2006", Biometric Technology Today, vol.15, no.7-8, pp.7-9, August 2007". The

second dataset is the colored fingerprint images that we have collected by ours from some participants in our study.

4.4.1 Dataset No.1 (FCV 2006 Gray Scale Fingerprint Dataset)

In our proposed system, the fingerprint images are adopted from database names (FCV2006) loaded from (http://atvs.ii.uam.es/atvs/fvc2006.html) web a BMP 8 bit/pixel (bit depth), the size of each used image is 400×560 pixels with resolution 96 dpi. The dataset has 8 data bases (DB1_A, DB1_B, DB2_A, DB2_B, DB3_A, DB3_B, DB4_A and DB4_B). The number of fingerprint samples in A Groups (1680) and (120) in B Groups, 12 images for each person (i.e. 30 sample were taken) are of different contrast (dark and light) and moves belong to a specific person [71].

Two options were adopted in the proposed system; the first one is to find bifurcation points and their distance while the second stage is to find the matched features for their types. The elapse time has been calculated during matching process to evaluate the proposed system.

Table (4.1) shows the dataset information of the first dataset that has been used in our proposed system depending on the local feature extraction approach by extract minutia features.

Table 4.1: FCV2006 Datasets Information

Dataset Size	**Description**							
	DB1_A	**DB1_B**	**DB2_A**	**DB2_B**	**DB3_A**	**DB3_B**	**DB4_A**	**DB4_B**
7200 images	1680 images	120 images	1680 Images	120 images	1680 Images	120 images	1680 Images	120 images

Figure 4.2 shows some fingerprint image examples from the FCV2006 dataset that we have used as a first dataset in the local approach using minutia feature extraction approach.

Figure 4.2: Sample of fingerprint images from FCV2006 dataset

4.4.2 Dataset No.2 (Colored Fingerprint Dataset)

The second dataset that we have used in our proposed contains colored fingerprint images that are adopted from own database names (colored fingerprint) which has been collected from my fingerprint. In this dataset, we have collected different samples as a part of our colored fingerprint images dataset. Each fingerprint image is higher resolution BMP image 24 bit per pixels, the size of each used image is 304×540 pixels with resolution 1024 dpi. Figure 4.3 shows some example of our color fingerprint image dataset that we have collected (which is just my finger images).

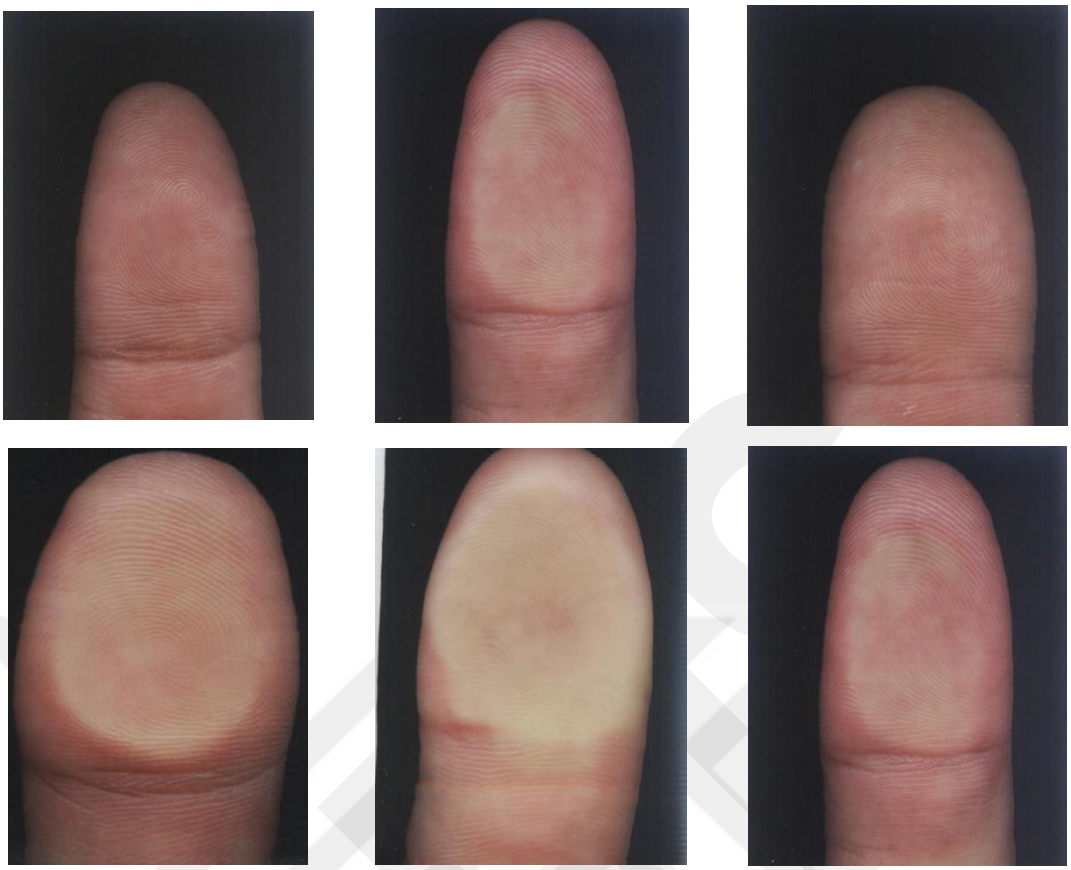


Figure 4.3: Some Fingerprint's Images that have been collected from our colored Dataset

4.5 Evaluation Criteria

The evaluating performance of fingerprint authentication and verification system based on minutia features feature extraction system using the distances between the detected bifurcation points are calculated by Calculate the minimum distance, the Euclidian distance is used between the extracted bifurcation point to the others.

We can define the squared distance between two vectors $x = [\, x1\ x2\,]$ and $y = [\, y1\ y2\,]$ is the sum of squared differences in their coordinates, which denotes that the squared distance between points $(P\ and\ Q)$. To denote the distance between vectors x and y we can use the notation $d_{x,y}$ so that this last result can be written as shown in Equation (4.1) [72]:

$$d^2 = (x_1 + y_1)^2 + (x_2 + y_2)^2 \tag{4.1}$$

which is, the distance itself is the square root as it shown in Equation (4.2) [72]:

$$d_{x,y} = \sqrt{(x_1 + y_1)^2 + (x_2 + y_2)^2} \tag{4.2}$$

What we called the squared length of x, the distance between points P and O, is the distance between the vector $x = [x1\ x2]$ and the zero vector $0 = [0\ 0]$ with coordinates all zero as it given in equation (4.3) [72]:

$$d_{x,y} = \sqrt{x_1^2 + x_2^2} \tag{4.3}$$

4.6 Standard Experimental Results

In this section, we will explain the different experiential results for the fingerprint authentication and verification system depending on the using different datasets and different approaches. The first experimental results rely on the first approach that we have proposed in this thesis which is the Local feature extraction based methodology for fingerprint authorization and verification. This approach is based on using minutia feature extraction and calculate the minimum distance using the first dataset FCV2006 dataset. The second experimental results rely on the second approach which is the Global based feature extraction approach. This Approach relies on the moment function based methodology for feature extraction and matching approach. In this approach, we used the second dataset that we have collected by our self which present the low-quality fingerprint images.

4.6.1 Local Approach Experimental Results

In this approach, we used the local approach which depends on the minutiae general approach to extract the features, then we compute the minimum distance to find the accurate matching results using FCV2006 dataset. We have select 30 random fingerprint image that have been randomly selected form the FCV2006 dataset. The

performance results of our proposed system fingerprint authentication and verification system using local approach is shown in Table 4.2.

In this Table 4.2, we can notice that each column represents the fingerprint image. for each fingerprint image, we have found there is 12 different sample for each fingerprint image and each row represent different results the final matching accuracy the time consuming for each finger that has been tested that has been calculate using a MATLAB function "tic-toc" starting from the final stage of the preprocessing image, feature extraction, false features removing till the final stage of the matching calculation.

Table 4.2: Local Performance result using FCV2006 Dataset

Fingerprint No	**Tested images from FCV 2006**											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1_1-Accuracy	1	0.5063	0.4462	0.4261	0.3512	0.4544	0.4825	0.3791	0.3718	0.378	0.4357	0.4048
1_1-Time	625.3977	1.27E+03	380.3559	704.8512	1.15E+03	1.30E+03	1.56E+03	1.72E+03	1.89E+03	2.10E+03	2.29E+03	2.43E+03
7_1-Accuracy	1	0.5659	0.2948	0.5516	0.5977	0.5337	0.4763	0.5305	0.4577	0.4483	0.3449	0.4387
7_1-Time	198.4294	65.8937	308.7257	372.8286	462.6065	523.4125	588.2893	664.1344	731.0155	794.9503	872.4416	944.1432
8_1-Accuracy	1	0.3485	0.5497	0.4818	0.3532	0.3767	0.4719	0.3304	0.4856	0.4012	0.5149	0.4561
8_1-Time	73.2855	153.909	254.95	305.2913	361.1734	737.5365	785.0334	824.2709	859.1795	898.5833	933.9373	968.8024

9_1-Accuracy	1	0.3213	0.3613	0.3243	0.4958	0.3094	0.3461	0.411	0.3926	0.3271	0.4171	0.3157
9_1-Time	86.1686	142.4503	236.1467	289.756	436.0767	6.82E+04	6.83E+04	6.84E+04	6.85E+04	6.86E+04	6.87E+04	6.88E+04
14_1-Accuracy	1	0.3903	0.4706	0.4438	0.4904	0.3568	0.4351	0.3546	0.3551	0.3631	0.5063	0.3521
14_1-Time	317.1371	1.13E+03	1.51E+03	1.97E+03	2.33E+03	2.45E+03	2.70E+03	2.82E+03	3.03E+03	3.17E+03	3.31E+03	3.44E+03
20_1-Accuracy	1	0.4076	0.7435	0.5583	0.6155	0.489	0.5294	0.5847	0.4701	0.4654	0.5483	0.3814
20_1-Time	149.4655	228.3492	286.7853	368.7981	447.1531	512.5977	564.4125	647.1917	703.7585	783.1898	833.4576	939.4057
25_1-Accuracy	1	0.4549	0.6102	0.4315	0.6753	0.5215	0.4613	0.5042	0.5305	0.4529	0.5775	0.4348
25_1-Time	49.037	134.4133	213.3314	162.3982	523.8742	585.9663	650.3534	698.1655	757.8059	824.3904	881.9028	938.3959
32_1-Accuracy	1	0.6929	0.5909	0.6944	0.6312	0.6232	0.6903	0.5667	0.7314	0.6432	0.6614	0.5333
32_1-Time	44.2883	148.3338	228.4001	285.4622	341.2632	406.4891	477.5215	519.7182	574.2988	630.3202	712.9447	759.2279
35_1-Accuracy	1	0.4057	0.3741	0.366	0.5033	0.3878	0.4773	0.3421	0.4045	0.2916	0.4518	0.3939
35_1-Time	33.424	70.1547	114.9081	161.9323	201.1466	237.0536	284.3576	339.2889	389.5926	439.7275	478.1364	516.5673

41_1-Accuracy	1	0.551	0.6209	0.543	0.6339	0.491	0.593	0.4842	0.5264	0.4458	0.6668	0.5476
41_1-Time	30.513	68.6859	134.1299	176.078	211.5767	259.3974	292.5886	327.1324	363.4725	404.6947	446.4227	487.4477
44_1-Accuracy	1	0.5747	0.589	0.611	0.6181	0.7131	0.7064	0.5965	0.6649	0.5301	0.6079	0.6787
44_1-Time	38.8931	110.0455	190.0159	268.5857	172.4824	100.1777	42.6243	326.5567	370.3333	413.8914	465.3982	505.5111
45_1-Accuracy	1	0.3652	0.49	0.4741	0.3931	0.4364	0.3752	0.423	0.4413	0.4687	0.4531	0.3931
45_1-Time	54.5741	93.0292	147.267	190.1546	229.4932	271.6342	317.6559	354.3585	425.9221	468.5377	505.6243	544.4005
49_1-Accuracy	1	0.2548	0.1768	0.2462	0.252	0.1936	0.2021	0.2309	0.1725	0.2182	0.1944	0.2709
49_1-Time	32.9496	81.1093	151.7813	120.4757	192.6613	223.9693	267.8566	305.9618	345.1336	385.2906	420.3119	454.1459
51_1-Accuracy	1	0.3889	0.3475	0.4813	0.3716	0.6217	0.4514	0.4945	0.4456	0.438	0.438	0.3954
51_1-Time	60.5405	161.8237	344.5887	832.7331	910.8548	973.7084	1.03E+03	1.08E+03	1.13E+03	1.19E+03	1.27E+03	1.31E+03
53_1-Accuracy	1	0.5966	0.6611	0.6753	0.7082	0.7047	0.6254	0.6207	0.6132	0.632	0.5666	0.6207
53_1-Time	45.4473	95.1704	180.1677	227.2931	298.5989	350.9768	405.2602	551.5371	605.5165	644.8008	712.9236	748.9152

58_1-Accuracy	1	0.5098	0.4222	0.6212	0.6264	0.5026	0.576	0.449	0.6002	0.5207	0.5026	0.5704
58_1-Time	79.9803	185.3944	276.2838	347.2331	2.11E+03	2.18E+03	2.25E+03	2.33E+03	2.42E+03	2.49E+03	2.57E+03	2.63E+03
67_1-Accuracy	1	0.6405	0.8721	0.8406	0.8396	0.8285	0.8235	0.6132	0.9223	0.7849	0.8696	0.7866
67_1-Time	49.5492	116.9875	3.32E+03	3.37E+03	3.60E+03	3.69E+03	3.88E+03	5.92E+03	5.96E+03	6.00E+03	6.04E+03	6.07E+03
76_1-Accuracy	1	0.7675	0.8966	0.7548	0.8581	0.8741	0.798	0.651	0.7926	0.8664	0.7905	0.64
76_1-Time	36.4592	84.6616	124.4307	159.6236	195.8121	236.1291	279.9369	313.4003	353.7563	392.6621	431.6071	474.5107
87_1-Accuracy	1	0.3888	0.3081	0.2495	0.453	0.4603	0.4552	0.4874	0.3602	0.4134	0.6186	0.4696
87_1-Time	60.4992	108.0808	162.9314	208.8336	260.5744	297.7514	350.7218	424.7788	470.9243	511.6053	568.1978	615.9272
88_1-Accuracy	1	0.647	0.8193	0.7028	0.8847	0.7438	0.7226	0.6439	0.729	0.6536	0.7581	0.6016
88_1-Time	50.7313	140.5204	182.7461	233.8758	269.6998	352.101	391.0042	430.4929	468.3557	524.9921	564.8924	644.0975
95_1-Accuracy	1	0.9058	0.9098	0.9163	0.9027	0.9027	0.85	0.8948	0.7902	0.9358	0.9383	0.9136
95_1-Time	51.6567	172.4501	244.0228	293.4256	35.0762	83.7191	126.7945	160.2898	225.8639	322.5152	356.3602	391.8813

97_1-Accuracy	1	0.5008	0.5801	0.5384	0.6667	0.6833	0.51	0.6868	0.6736	0.5963	0.6339	0.598
97_1-Time	35.4673	79.5597	131.9417	167.3598	207.9659	254.3456	320.1944	359.5696	407.9308	448.2158	500.5573	549.0912
99_1-Accuracy	1	0.6971	0.7817	0.5766	0.6536	0.7765	0.7407	0.6118	0.5561	0.6603	0.7341	0.7817
99_1-Time	28.6486	74.1524	110.3392	146.4531	219.8858	255.2044	318.1901	726.9125	1.72E+03	1.75E+03	1.79E+03	1.82E+03
100_1-Accuracy	1	0.8102	0.8549	0.7506	0.8393	0.6938	0.768	0.7452	0.8369	0.7256	0.84	0.6993
100_1-Time	46.8617	86.125	3.52E+03	3.57E+03	3.61E+03	3.67E+01	9.04E+01	144.3564	287.4589	327.5148	425.9718	488.3501
105_1-Accuracy	1	0.4895	0.6183	0.4587	0.5421	0.4683	0.6533	0.6294	0.5336	0.665	0.5367	0.5505
105-Time	36.2076	83.7004	119.425	185.0357	238.0145	292.1956	338.4829	382.6819	478.1571	524.6032	565.2332	611.1438
117-Accuracy	1	0.9214	0.9072	0.8343	0.807	0.739	0.7337	0.777	0.9418	0.8154	0.7239	0.8315
117-Time	53.2664	107.2927	144.7912	193.1801	265.9001	301.4709	373.7139	410.5057	451.3263	504.4192	538.4533	578.3649
126-Accuracy	1	0.5963	0.7478	0.5729	0.6782	0.4865	0.6728	0.7176	0.6149	0.796	0.5948	0.5601
126-Time	38.1257	84.1997	136.3943	174.4576	213.1031	250.6377	479.5425	596.3753	632.2526	670.3046	724.764	770.9432

130-Accuracy	1	0.5982	0.754	0.6368	0.6774	0.5039	0.7376	0.6753	0.6857	0.7113	0.7069	0.7069
130-Time	48.33	105.7244	189.9386	150.7996	240.1527	56.2718	125.827	179.4299	228.8394	323.9397	368.6199	432.0019
133-Accuracy	1	0.7934	0.8433	0.6669	0.7851	0.7967	0.793	0.6481	0.7438	0.6615	0.8033	0.705
133-Time	41.1185	92.635	142.7233	216.1707	253.3437	295.9338	353.8318	400.7903	448.67	504.3243	544.6217	703.9172
136-Accuracy	1	0.5544	0.6436	0.6963	0.7425	0.6845	0.7585	0.6072	0.6338	0.6747	0.5509	0.6826
136-Time	57.9315	140.2121	216.9536	331.4389	415.2766	497.1483	578.6797	645.3651	699.7053	756.6488	816.8392	895.1569

The average mean of the performance result for the fingerprint authentication and verification system using local feature extraction approach is shown in Figure 4.4. We can notice that the local approach works accurate in the matching results when it has been applied on the same fingerprint image which the accuracy results is (100%) when it is applied in the same view and image position. In contrast, the accuracy is different from the lower range which is (80%) to the higher range which is (90%) when it has been applied on the difficult situation like rotational and noisy fingerprint images.

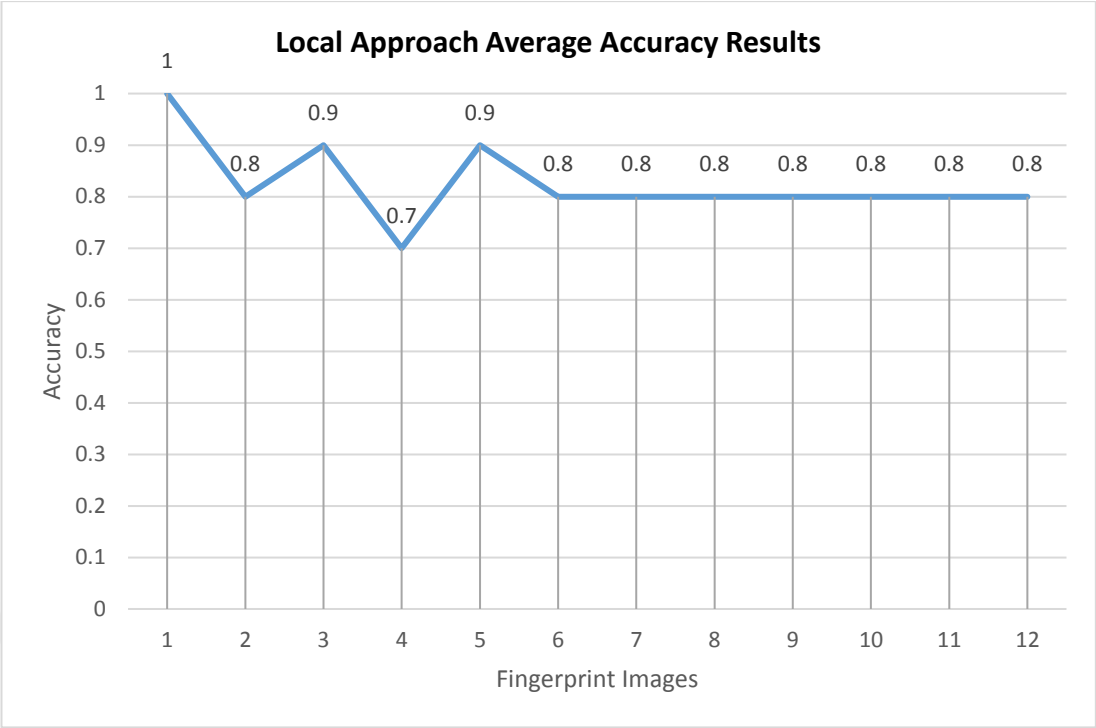


Figure 4.4: AVERAGE Accuracy result of the local approach for fingerprint authentication and verification system using FCV2006 dataset

Figure 4.5 shows the time consumption for the fingerprint authentication and verification system in local approach. We can notice that the local approach is highly time consuming since it needs a lot of preprocessing steps. In this approach which is the local fingerprint approach based on minutia feature extraction model, we can notice that in monastically increasing in time consuming since the samples of the fingerprint images have been different in the difficulties like rotational degree, noise, and other factors.

We can easily notice that there is a big jump between 5^{th} and 6^{th} images which is clearly seen that all the time consuming in monotonality increasing in the time consuming according to the fingerprint image samples complexity such as amount of noise, rotation and other distribution that have done in this dataset.

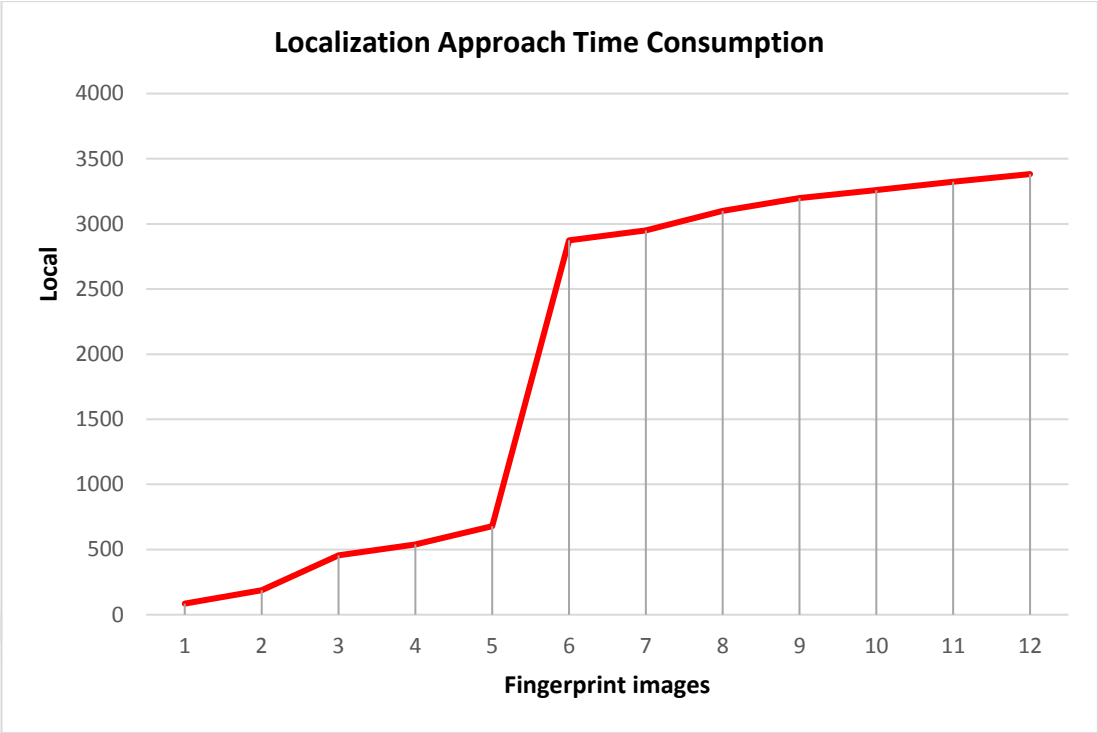


Figure 4.5: Time consumption of the local approach for fingerprint authentication and verification system using FCV2006 dataset

4.6.2 Comparison with Previous Studies

In term of comparing the standard approach of the fingerprint authentication and verification system using local approach which depends on using minutia feature extraction approach. Table 4.3 compares the recognition results obtained by our proposed method with previous studies that have been applied on the same task which is fingerprint authentication and verification using FCV2006 dataset, where in these studies the same database and same local approach but different preprocessing methods have been used.

Table 4.3: FCV2006 Datasets Information

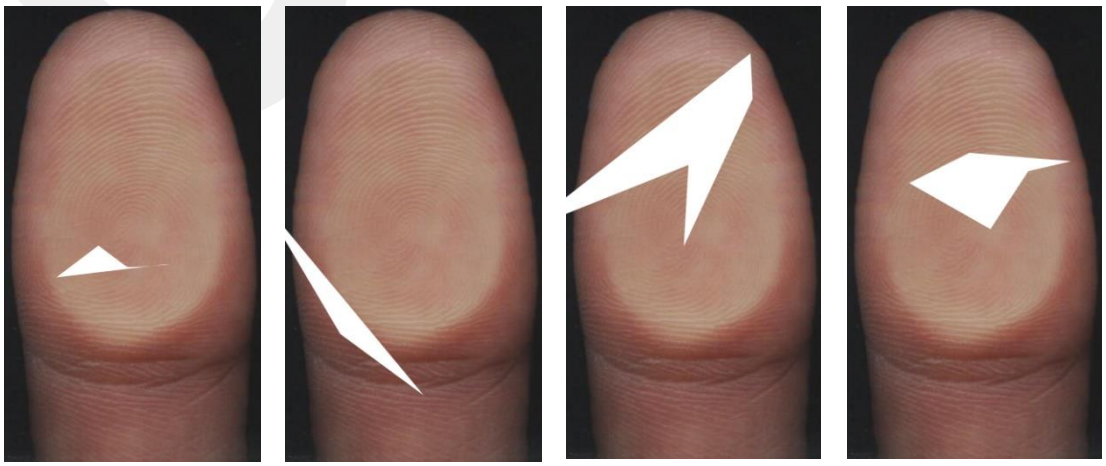
No	Method	Recognition Rate (%)
1	[72]	95.82%
2	[73]	92.24%
3	[74]	93.21%
4	[75]	96.36%

4.7 Incomplete Fingerprint Authentication Experimental Results

In term of using a different dataset that has such a problem that we proposed system to solve such fingerprint images identification and verification challenges. In this section, we use the incomplete fingerprint images as a challenge task to study the weakness and the strongest points of the local approach as well as our proposed system to solve the incomplete fingerprint identification and verification challenges.

In this section, we will explain the experiential results for the fingerprint authentication and verification system depending on two different approaches the local and global approach. In term of fair fingerprint image random selection satisfaction, we generate some random cases by design and implementation a MATLAB code to generate random shapes that are used later to generate random incomplete fingerprint images. To do that, we use one case of color fingerprint image and generate the rest cases depending on this image. In this case, we have generated about 1200 random case, and then we reordered those cases according to the size of the random cut on each image into 10 groups. Then, we used a random fingerprint image selection from each group to select 3 random fingerprint images to be tested on our thesis which depends on study the comparison between the local and global for fingerprint authentication and verification approach for incomplete fingerprint images.

Figure 4.6 shows some example of the random incomplete fingerprint images that have been tested in our approach which is a global approach for fingerprint image authentication and verification approach.



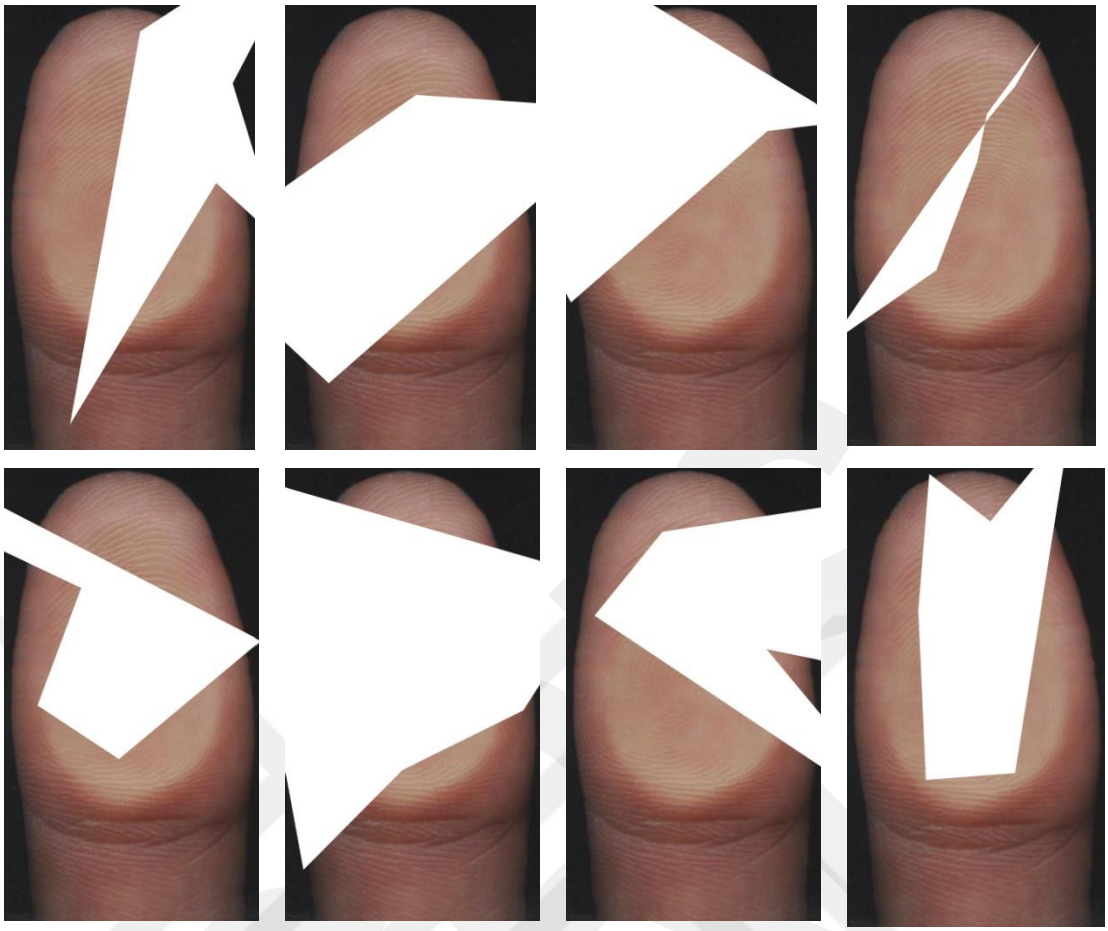


Figure 4.6: Some examples of random incomplete fingerprint image that have been randomly generate using one fingerprint case image

4.7.1 Local Approach Experimental Results

In the first step, we used the local approach which depends on the find and extract the minutiae features then compute the minimum distance to find the accurate matching results. The performance results of the local approach on the incomplete images for fingerprint authentication and verification system using local approach is shown in Table 4.4.

Table 4.4: Local Approach Performance result for the incomplete fingerprint image authentication and verification

Group No.	Fingerprint No.	Time consuming in (Sec.)	Matching Accuracy	Authorization
1	01 (15)	2.54E+03	0.9931	Yes
1	01 (48)	1.70E+03	0.846	Yes

1	01 (50)	3.32E+03	0.9382	Yes
2	02 (39)	4.03E+03	0.8497	Yes
2	02 (77)	4.61E+03	0.891	Yes
2	02 (143)	3.56E+03	0.7121	No
3	03 (56)	3.99E+03	0.7598	No
3	03 (7)	4.60E+03	0.7016	No
3	03 (104)	5.09E+03	0.7885	No
4	04 (16)	5.45E+03	0.5647	No
4	04 (200)	5.81E+03	0.6169	No
4	04 (21)	6.18E+03	0.6161	No
5	05 (3)	6.46E+03	0.5555	No
5	05 (29)	6.74E+03	0.6112	No
5	05 (18)	7.01E+03	0.6286	No
6	06 (17)	7.24E+03	0.6047	No
6	06 (2)	7.42E+03	0.5217	No
6	06 (40)	7.64E+03	0.5526	No
7	07 (6)	7.85E+03	0.4883	No
7	07 (39)	8.06E+03	0.4317	No
7	07 (14)	8.23E+03	0.5725	No
8	08 (5)	8.34E+03	0.3008	No
8	08 (7)	8.49E+03	0.4402	No
8	08 (12)	8.56E+03	0.4456	No
9	09 (9)	8.69E+03	0.3947	No
9	09 (4)	8.78E+03	0.4445	No
9	09 (1)	8.90E+03	0.4147	No
10	10 (3)	9.00E+03	0.2479	No
10	10 (5)	9.65E+03	0.2324	No
10	10 (8)	100.897	0.2753	No

We can notice that the final accuracy of the local approach is about (16.66%) just for the first three cases while the rest are authorized and have not been verified. The reason for that is since the local approach relies on the minutia features which are very sensitive for any missing or incomplete image, we notice that just the first three cases have been successfully authorized since the rest are not.

Figure 4.7 shows the time for the fingerprint preprocessing, feature extraction and authentication that have been consumed through the local approach. Where the average time for the local approach is (6270 sec.).

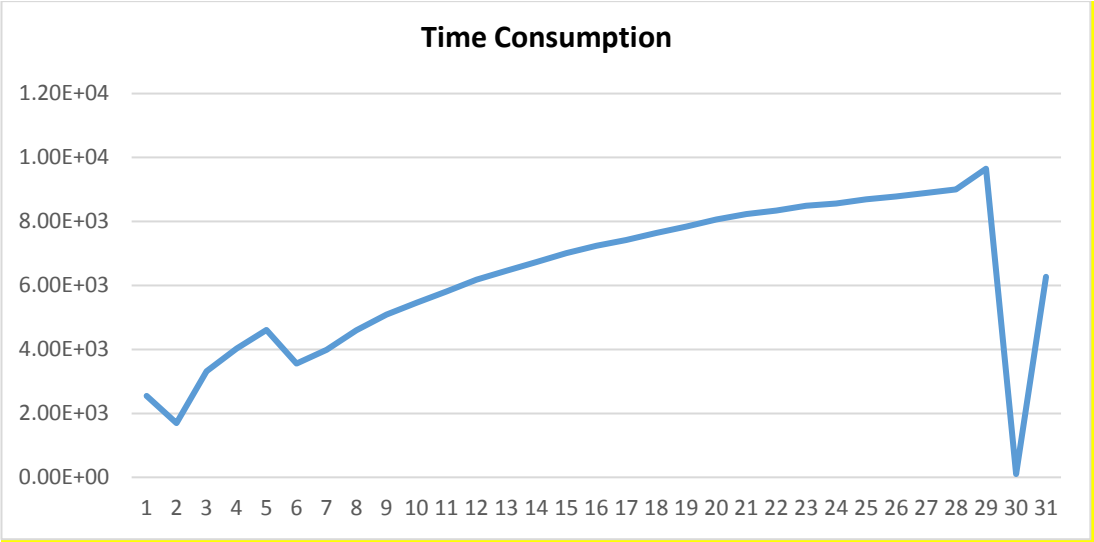


Figure 4.7: Time consumption of the local approach for fingerprint authentication

We can notice that from the figure above the time consuming is increasing according the fingerprint sample complexity which here the missing part of the image that effect on the local approach to detect the features as well as to remove the false minutia feature. These steps as the preprocessing stage which is required by the local approach to verify the minutia feature in the matching step. We notice that as much as the fingerprint has big part missing in the image the more time that is require verifying and identify the tested fingerprint image.

Figure 4.8 shows the authentication ratio for the fingerprint authentication and verification approach using local approach. In this stage, we define a decision threshold for the tested fingerprint images that we want to verify and identify. Th decision threshold depends of the system application to determine there is no such a condition to set this value but typically it has been selected from the range of [90-100] according to the strongest of the identification and verification system. In our case we use a threshold value 98 and above to be set as an authorized fingerprint image and lower than this threshold it will be not authorized.

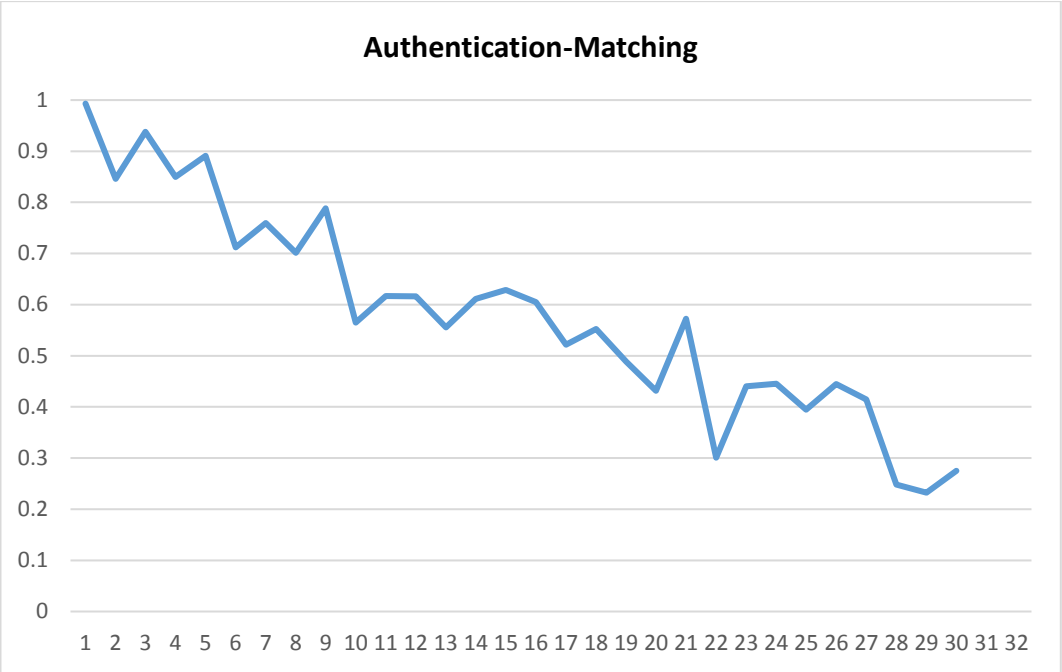


Figure 4.8: Authentication Ration for the Local approach

4.7.2 Global Approach Experimental Results

In the second step, we used the global approach instead of the local approach to solve the incomplete fingerprint image authentication and verification problem. Our proposed approach depends on extract the global features instead of the local one to jump out the minutia features sensitivity. This approach relies on extract and calculate the seven moment features as it has been explain in chapter 3.

The performance results of our proposed system fingerprint authentication and verification system for incomplete fingerprint images using local approach is shown in Table 4.5.

Table 4.5: Global Approach Performance result for the incomplete fingerprint image authentication and verification

Group No.	Fingerprint No.	Values of Moment							Time	Ratio	Authorized
		1	2	3	4	5	6	7			
1	01 (15)	1.070059	2.278212	4.020444	3.852808	7.788711	4.991321	6.55039	31	99.939964	Yes
1	01 (48)	1.063054	2.260424	3.993016	3.830225	7.741193	4.959881	6.48055	31	99.224754	Yes
1	01 (50)	1.04579	2.236768	3.957866	3.788373	7.660861	4.906298	6.392888	75	98.074669	Yes
2	02 (39)	1.040886	2.217025	3.929675	3.768537	7.617019	4.876571	6.346479	31	97.445358	Yes
2	02 (77)	1.057438	2.2485	3.976276	3.814944	7.709907	4.938669	6.447443	62	98.768837	Yes
2	02 (143)	1.035232	2.214431	3.92781	3.753085	7.592727	4.859693	6.377894	47	97.26535	Yes
3	03 (56)	1.066203	2.274675	4.015893	3.843143	7.77191	4.979843	6.541974	41	99.732384	Yes
3	03 (7)	1.062407	2.260414	3.991849	3.830137	7.740563	4.959861	6.449414	100	99.142563	Yes
3	03 (104)	1.055092	2.243869	3.963779	3.809047	7.695061	4.930637	6.327042	32	98.329872	Yes

4	04 (16)	1.052481	2.279921	4.029964	3.827465	7.755051	4.96671	6.613631	116	99.371574	Yes
4	04 (200)	1.03594	2.196327	3.897562	3.745674	7.566759	4.843387	6.261693	69	96.679153	Yes
4	04 (21)	1.033497	2.199722	3.900209	3.745645	7.568098	4.845126	6.237393	86	83.048378	Yes
5	05 (3)	1.024334	2.278396	4.020353	3.791044	7.695869	4.929882	6.498667	100	98.642967	Yes
5	05 (29)	1.046911	2.256598	3.992301	3.808987	7.708938	4.936914	6.461321	115	98.737335	Yes
5	05 (18)	1.050364	2.248501	3.978081	3.80211	7.691437	4.925783	6.466516	22	98.604088	Yes
6	06 (17)	0.990765	2.304692	4.050393	3.768575	7.676522	4.920735	6.602204	100	84.629822	Yes
6	06 (2)	1.013455	2.310879	4.071925	3.805342	7.742929	4.960573	6.584958	31	84.926147	Yes
6	06 (40)	1.077446	2.29478	4.04395	3.872592	7.829965	5.019268	6.638789	118	99.347496	Yes
7	07 (6)	1.036483	2.261777	3.996868	3.789633	7.682092	4.920018	6.463423	100	98.482117	Yes
7	07 (39)	1.022133	2.20301	3.909562	3.734402	7.556011	4.835666	6.173761	22	82.859627	Yes

7	07 (14)	1.091632	2.327681	4.091371	3.916728	7.920054	5.079894	6.681378	31	98.216354	Yes
8	08 (5)	1.052989	2.314821	4.077151	3.849525	7.811243	5.006058	6.748385	31	98.866814	Yes
8	08 (7)	1.042858	2.299216	4.058272	3.826184	7.767167	4.975136	6.64693	100	98.994415	Yes
8	08 (12)	1.179152	2.566371	4.457623	4.209573	8.540823	5.491155	7.558987	116	N.A.	No
9	09 (9)	0.936381	2.233598	3.936305	3.664802	7.465288	4.781355	5.713684	16	N.A.	No
9	09 (4)	1.013192	2.282084	4.030596	3.784662	7.691638	4.925538	6.430631	104	84.751724	Yes
9	09 (1)	1.031787	2.300173	4.050463	3.867657	7.82667	5.017449	5.991196	82	84.786438	Yes
10	10 (3)	1.091556	2.532945	4.377211	4.073602	8.298317	5.340003	7.050022	116	N.A.	No
10	10 (5)	0.932403	2.235179	3.940673	3.713837	7.535567	4.826897	6.741099	494	83.291367	Yes
10	10 (8)	1.215318	2.686804	4.620504	4.351065	8.835661	5.693805	7.705384	101	N.A.	No

We can notice that the final accuracy of our proposed system which is the global approach is about (86.7%). Figure 4.8 shows the time for the fingerprint preprocessing, feature extraction and authentication that have been consumed

through the local approach. Where the average time for the local approach is (10.084 sec).

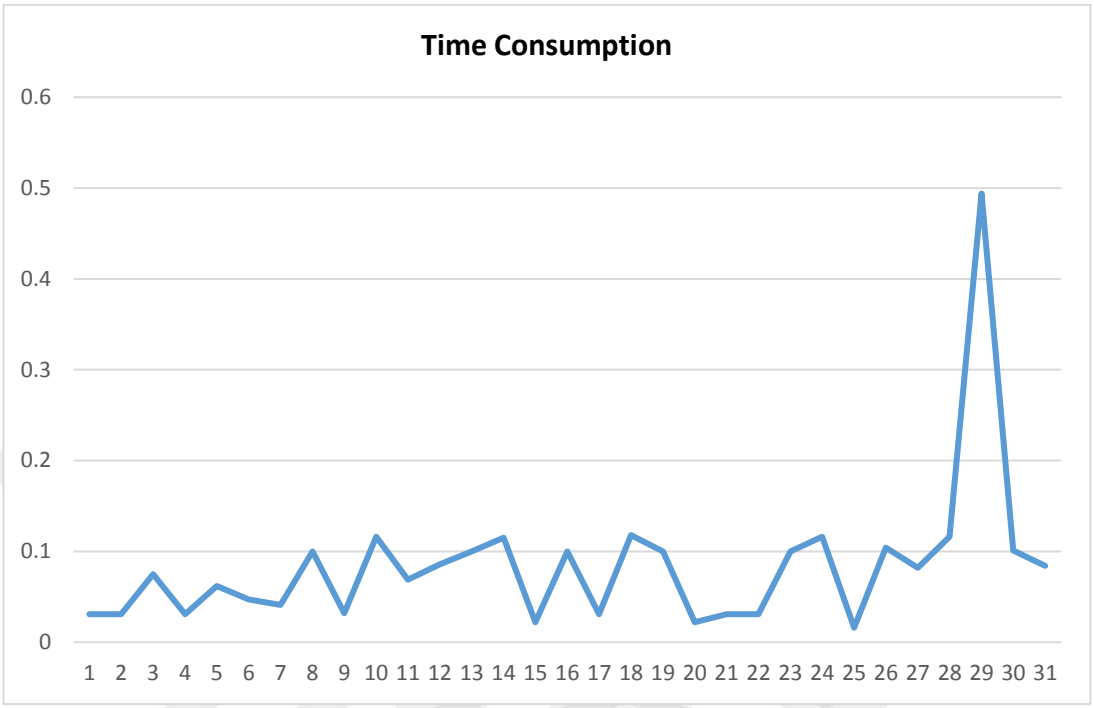


Figure 4.9: Time consumption of the Global approach for fingerprint authentication

Figure 4.8 shows the authentication ratio for the fingerprint authentication and verification approach using local approach.

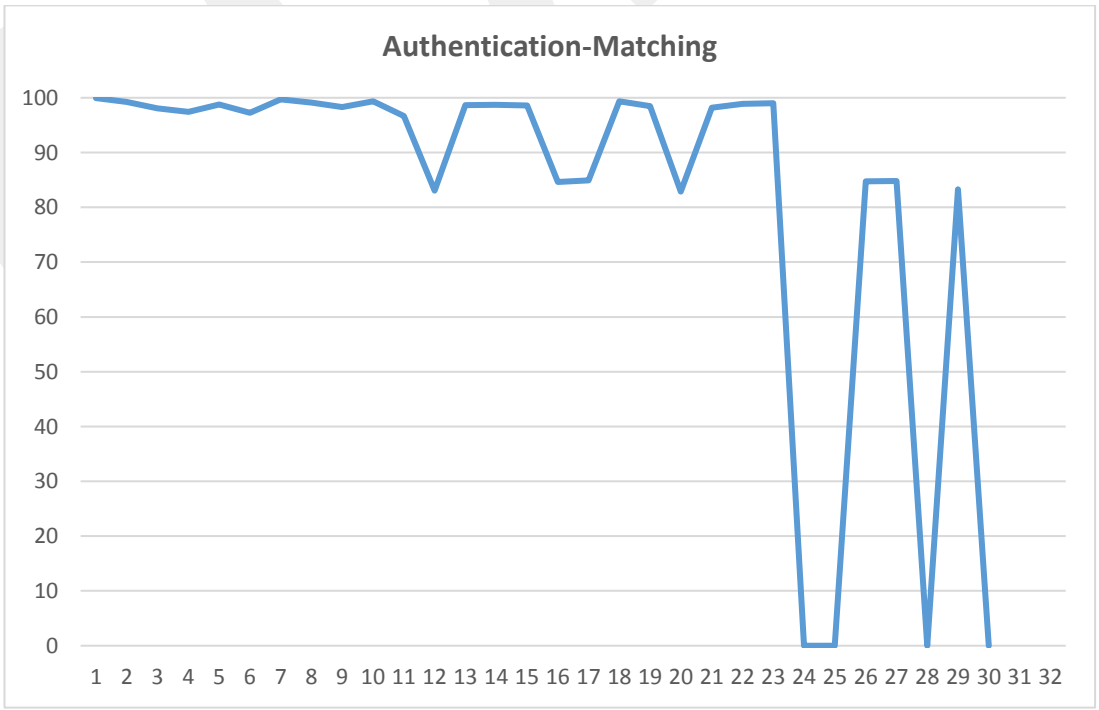


Figure 4.10: Authentication Ration for the Global approach

We can notice that there is some effective factor that effect on the matching ration of the global approach that depends on the ration that has been explained in chapter 3 which is the ration between the moment feature vector that is been extracted and the moment feature vector stored in the database. The size of the incomplete part of the fingerprint image effect in this ration in some who that make some fingerprint images are not authorized like the fingerprint image sample number 23.

4.8 Local and Global Comparing Results

From the results above, we can easily notice that the global approach has achieved about (86.7%) while the local approach has achieved (16.7%) which the global approach enhances the fingerprint authentication and verification system for the incomplete image by (70%). The reason for that is the moment function relies on the whole image for extract the seven moment values. This seven values have been computed depending on the white line above the black background for the fingerprint image which those lines are already constructed by the fingerprint lines and features. Any cut in the fingerprint image the moment function can substitute by another value of the moment value instead of relying on the local features which are missed and effected by the image cutting. For this reason, the global approach is more robust that the local approach for incomplete fingerprint identification and verification task.

Figure 4.11 shows a comparing authentication ratio result between the local and the global approach for fingerprint authentication and verification task.

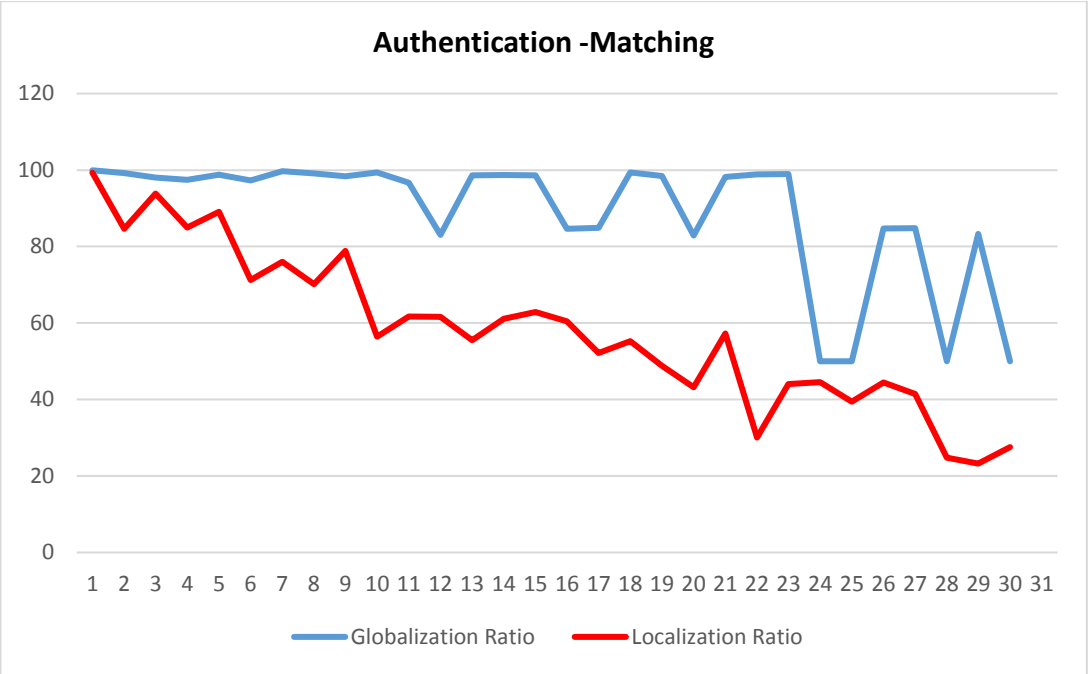


Figure 4.11: Comparing between local and global approach for Authentication Ration

It is easily to see that the matching accuracy (Authentication) for the Global approach is more efficient that the Local approach in the mean average. In the most cases of the Local approach we have notice from the matching accuracy that it is below 80% while the most cases of the incomplete image that have been tested in the Global approach is above 80% which gives us an indentation about the different of the robustness behavior between the Local and the global approaches for the incomplete fingerprint image identification and verification task.

CHAPTER 5

CONCLUSION AND SUGGESTION FOR FUTURE WORKS

In this chapter, we will summarize the achievements of this thesis and several conclusions that have been deduced from the obtained test results.

5.1 Conclusions

In this thesis, we considered a global approach for fingerprint authentication and verification based on moment function feature extraction to identify and verify the incomplete fingerprint images on which the classical approach which is the local minutiae feature extraction based method accuracy scores are not satisfactory. Local based munities feature extraction and global based moment function for feature extraction have been tested on random regenerated incomplete images that we randomly generated and selected. The testing results show that the global approach enhance the fingerprint authentication and verification system by 70% more than the local approach which the global archives about 86.7% authentication accuracy. Different feature extraction approach that we have proposed by considering the ineffectiveness of the local approach which depends on the sensitivity of the minutia features allows us to deal with the incomplete fingerprint image authentication and varication problem. Global approach relies on the whole structure features of the fingerprint to translate them to seven moment function that will be used later in the matching stage.

This technique which is a global feature vector using moment function give a strong point to emphasize on the global approach to find a substitutional feature ration to fairly authenticate the incomplete fingerprint image by computing the matching score while depending on the global features instead of the local ones.

Finally, our final conclusion detects the incomplete fingerprint image identification and verification task suing our proposed system (Global Approach) gives a higher matching score that the standard one (Local Approach) since our proposed approach depends on the global feature vector using moment function instead of the local feature using minutia features which gives us an intensive way to jump put the missing feature that the local approach has felt to detected and extracted.

As a conclusion, our approach (global feature extraction based approach) has achieved better performance results when it has been compared with the local approach (minutia based feature extraction approach) in two points:

1- Our approach (Global feature vector) has improved the performance result of the incomplete fingerprint identification and verification task by (70%) more than the local approach (local minutia based feature vector).

2- Our global approach is faster that the local approach in the incomplete fingerprint identification and verification approach which the global approach has consumed (10.0854 sec.) as the mean average time for the preprocessing, feature extraction (moment function values), and matching stage, while the local approach has consumed (6270 sec.) as the means average consuming time for the preprocessing, feature extraction (minutia features detection and extraction) including minutia false feature detection and evaluation, and matching stage.

3- In both cases (average accuracy and average time consuming) our proposed approach (global feature extraction based approach) has acted better than the local approach (minutia based feature extraction approach) when both cases have been applied on the same problem which is the partial or incomplete fingerprint image identification and verification task.

5.2 Suggestions for Future Work

In our future work, we have suggested some point the will be our plan for the future work for the fingerprint

1. Enhance the proposed approach to cope with the rotation sensitivity.

2. Using another matching method instead of moment match ratio algorithm such as intelligent techniques which may apply during matching phase like Neural Networks or another algorithm.

3. An electronic device could be plugged to monitor system for real-time fingerprint acquisition and authentication or identification which will cause another problem for the fingerprint scanning image that must be solved.

4. Using different types of database that have other challenges and compare between the Local and Global approach to conclude another advantages and disadvantages though them.

REFERENCES

[1]. Ross A., "Information fusion in fingerprints authentication", thesis, Michigan State University, 2003.

[2]. Jain A., Hong L.,Pankanti S., Bolle R., “An Identity Authentication System Using Fingerprints”, Pattern Recognition and Image Processing Laboratory, Michigan State University, 2007.

[3]. M.H. Bhuyan, S. Saharia, and D.K. Bhattacharyya, "An Effective Method for Fingerprint Classification", International Arab Journal of e-Technology, Vol. 1, No. 3, pp. 89-97, 2010.

[4]. M. Tico, "On Design and Implementation on Fingerprint-Based Biometric Systems", Ph.D Dissertation, Tampere University of Technology, 2001.

[5]. S. Kumar, K.B. Raja, R.K. Chhotaray, and S. Pattanaik, "DWT Based Fingerprint Recognition Using Non-Minutiae Features", International Journal of Computer Science Issues, ISSN (Online): 1694-0814, Vol. 8, Issue 2, March 2011.

[6]. V.L. Lorenzo, P.H. Pellitero, J. I.M. Torre, and J.C. Villar, "Fingerprint Minutiae Extraction Based on FPGA and MatLab", Proceedings of the Conference on Design of Circuits and Integrated Systems, this work has been supported by the Spanish PROFIT and Medea Programme under FIT, 2005.

[7]. Q. Zhao, J. Feng, and A.K. Jain, "Latent Fingerprint Matching: Utility of Level 3 Features", MSU Technical Report, MSU-CSE-10-14, 2010.

[8]. M.H. Bhuyan, S. Saharia, and D.K. Bhattacharyya, "An Effective Method for Fingerprint Classification", International Arab Journal of e-Technology, Vol. 1,No. 3, pp. 89-97, 2010.

[9]. C. Ryu, S.G. Kong, and H. Kim, "Enhancement of Feature Extraction for Lowquality Fingerprint Images Using Stochastic Resonance", Pattern Recognition Letters, Vol. 32, No. 2, pp. 107–113, 2011.

[10]. S.J. Xie, J. Yang, D.S. Park, S.Yoon, and J. Shin (2011), "Fingerprint Quality Analysis and Estimation Approach for Fingerprint Matching"; In: J. Yang, and L. Nanni (Eds.), State of the art in Biometrics, In Tech, 2011.

[11]. D. Maltoni, "A Tutorial on Fingerprint Recognition", M. Tistarelli, J. Bigun, and E. Grosso (Eds.): Biometrics School 2003, Lecture Notes In Computer Science 3161, pp. 43-68, 2015.

[12]. N. Ratha, and R. Bolle (Eds.), Automatic Fingerprint Recognition Systems, Springer, New York, 2014.

[13]. Nandakumar, K., and A. K. Jain, “Local Correlation-Based Fingerprint Matching”, Proceedings Indian Conference on Computer Vision, Graphics & Image Processing, pp. 503-508, Kolkata, 2014.

[14]. Z. Shi, and V. Govindaraju, “Fingerprint Image Enhancement Based on Skin Profile Approximation”, 18th International Conference on Pattern Recognition, ISBN 0-7695-2521-0, Vol. 3, pp. 714-717, 2016.

[15]. C. Wu, "Advanced Feature Extraction Algorithms for Automatic Fingerprint Recognition Systems", Ph.D Dissertation, University of New York, 2007.

[16]. S. Theodoridis, and K. Koutroumbas, "Pattern Recognition", Third Edition, Academic press, 837 pages, hardbound, ISBN 0-12-369531-7, 2006.

[17]. M. Tico, "On Design and Implementation on Fingerprint-Based Biometric Systems", Ph.D Dissertation, Tampere University of Technology, 2011.

[18]. M.H. Bhuyan and D.K. Bhattacharyya, "An Effective Fingerprint Classification and Search Method", International Journal of Computer Science and Network Security, Vol. 9, No.11, pp. 39-48, 2009.

[19]. N. Short, A.L. Abbott, M. Hsiao, and E. Fox, "Robust Feature Extraction in Fingerprint Images using Ridge Model Tracking", Biometrics: Theory, Applications and Systems, 2012 IEEE Fifth International Conference on, DOI:10.1109/BTAS.2012.6374587, pp. 259-264, 2012.

[20]. S.D. Singh, and S.P. Majhi, "Fingerprint Recognition: A Study on Image Enhancement and Minutiae Extraction", M.Sc Thesis, submitted to National Institute of Technology Rourkela, 2010.

[49]. A.M.A. Al-Kateeb, "Fingerprint Matching Using Matlab", M.Sc. thesis, University of Technology, 2005.

[50]. C. Gottschlich*, P. Mihailescu, and A. Munk, "Robust Orientation Field Estimation and Extrapolation Using Semilocal Line Sensors", IEEE Transactions on Information Forensics and Security, Vol. 4, Issue 4, pp. 802-811, 2009.

[51]. A.M.A. Al-Kateeb, "Fingerprint Matching Using Matlab", M.Sc. thesis, University of Technology, 2005.

[52]. A. Ackerman, "Fingerprint Recognition", Professor Ostrovsky, Journal of Pharmaceutical and Biomedical Analysis, Vol. 48, pp. 554-561, 2008.

[53]. K. Treash and K. Amaratunga, "Automatic Road Detection in Grayscale Aerial Images", American Society of Civil Engineers, Vol. 14, No. 1, P. 60-69, 2000.

[54]. M.H. Bhuyan and D.K. Bhattacharyya, "An Effective Fingerprint Classification and Search Method", International Journal of Computer Science and Network Security, Vol. 9, No.11, pp. 39-48, 2009.

[55]. M.H. Bhuyan, S. Saharia, and D.K. Bhattacharyya, "An Effective Method for Fingerprint Classification", International Arab Journal of e-Technology, Vol. 1, No. 3, pp. 89-97, 2010.

[56]. D. Rutovitz, "Pattern Recognition", J. Royal Statistic Society, Vol. 129, Series A, pp. 504–530, 1966.

[57]. F. Zhao, and X. Tang, "Preprocessing and Postprocessing for Skeleton-Based Fingerprint Minutiae Extraction", Pattern Recognition, Vol. 40, No. 4, pp. 1270–1281, 2007.

[58]. S.D. Singh, and S.P. Majhi, "Fingerprint Recognition: A Study on Image Enhancement and Minutiae Extraction", M.Sc Thesis, submitted to National Institute of Technology Rourkela, 2010.

[59]. V.L. Lorenzo, P.H. Pellitero, J. I.M. Torre, and J.C. Villar, "Fingerprint Minutiae Extraction Based on FPGA and MatLab", Proceedings of the Conference on Design of Circuits and Integrated Systems, this work has been supported by the Spanish PROFIT and Medea Programme under FIT, 2005.

[60]. S. Kim, D. Lee, and J. Kim, "Algorithm for Detection and Elimination of False Minutiae in Fingerprint Images", Proceedings of Third International Conference on Audio- and Video-Based Biometric Person Authentication, ISBN: 3-540-42216-1, pp. 235-240, Springer, Lecture Notes in Computer Science 2091, 2001.

[61]. M. Tico, "On Design and Implementation on Fingerprint-Based Biometric Systems", Ph.D Dissertation, Tampere University of Technology, 2001.

[62]. F. Zhao, and X. Tang, "Preprocessing and Postprocessing for Skeleton-Based Fingerprint Minutiae Extraction", Pattern Recognition, Vol. 40, No. 4, pp. 1270–1281, 2007.

[63]. Alessandro F., Zsolt M.k., alberto L., "Fingerprint minutiae extraction from skeletonized binary images", university of bologna, italy, 1998.

[64]. Coetzee L., “Fingerprint Recognition”, Pattern Recognition,Vol 22, no.1, pp. 45-65, 1992.

[65]. Ng Ho Wa, Ng Ka Lung, Lui Siu Tat, "image processing project/fingerprint analysis", IEEE transactions on pattern analysis and machine intelligence, Vol.21, No.1, 1998.

[66]. Umbaugh S.E.," Computer Vision and Image Processing", Prentice Hall Ptr., 1998.

[67]. Gonzalez R.C., "Digital Image Processing", Addison-Wesley Publishing Company Inc., 1982.

[68]. Ying-han Pang, Andrew T.B.J, David N.C.L, Hiew Fu San"Palmprint Verification With Moments",Vol.12, no.1-3, 2004.

[69]. Kosuke Imai," Expectation and Functions of Random Variables", Department of Politics, Princeton University March 10, 2006.

[70]. Laura Keyes, BAdam Winstanley," USING MOMENT INVARIANTS FOR CLASSIFYING SHAPES ON LARGE_SCALE MAPS", Department of Computer Science, National University of Ireland Maynooth Co. Kildare Ireland.

[71]. Satish S. Bhairannawar,1 K. B. Raja,2 and K. R. Venugopal3," An Efficient Reconfigurable Architecture for Fingerprint Recognition", Hindawi Publishing Corporation VLSI Design Volume 2016.

[72]. A.N. Ouzounoglou, P.A. Asvestas and G.K. Matsopoulos, "A New Approach in Fingerprint Matching based on a Competitive Learning Algorithm", International Journal of Information and Communication Technology Research, Vol. 2, No.9, pp. 723-731, 2013.

[73]. H.Zhang, Y.Yin and G.Ren, "An Improved Method for Singularity Detection of Fingerprint Images", Book Advances in Biometric Person Authentication, Springer Berlin/Heidelberg, Vol. 3338/2015, pp.516-524, ISBN 978-3-540-24029-7.

[74]. A. T. B. Jin, D. N. C. Ling, and O. T. Song, "An efficient fingerprint verification system using integrated wavelet and Fourier–Mellin invariant transform," Image and Vision Computing, vol. 22, 2014.

[75]. Ravinder Kumar, Pravin Chandra, and Madasu Hanmandlu," A Robust Fingerprint Matching System Using Orientation Features",J Inf Process Syst, Vol.12, No.1, pp.83~99, March 2016.