

**PEOPLE 'S DEMORATIC REPUBLIC OF ALGERIA MINISTRY
HIGHER EDUCATION AND SCIENTIFIC RESEARCH
KASDI MERBAH UNIVERSITY OUARGLA
Faculty of new Technologies of Information and communications
DEPARTMENT OF ELECTRONICS AND TELECOMMUNICATIONS**



Memory

ACADEMIC MASTER

Domain: Sciences and Technologies Specialty: automatic and system

Submitted by:

BEKKOUCHE BOUTHEYNADEBBA KHAOULA

Theme

Secure voting on mobile phone using biometrics

Publically defended on: 19/09/2020

Board of examiners :

BEN SID Khaled	MCB	President	UKM Ouargla
KORICHI Maarouf	MAB	Examiner	UKM Ouargla
SMAHI Mokhtar	MAA	Director	UKM Ouargla

AcademicYear :2019/2020



Acknowledgments

Above all, we thank Allah for given the strength to undertake this work and praise to Him.

Gratitude goes to our mentor and supervision Dr. Smahi Mokhtar, for his assistance, meticulous comments and guidance.

Gratitude also goes to the members of the jury for accepting to read this work and for any remarks they provide to refine it.

Special thanks to all teachers of Electronics and Telecommunications department.

Last but not least, special gratitude goes to our families for their support, encouragement and patience. Finally, we would like to extend appreciations to all who helped us in one way or another to fulfill this work.

Bou. Bekkouche & KH. Debba





Dedication

*I dedicate this modest work to the one who gave me life, the symbol of
tenderness, who sacrificed itself for my happiness and my success, to my*

*mother ***Soriya Bekkouche***,*

*To my father ***Nadir Bekkouche***, who was my shadow for all Years of*

study and who has ensured

throughout my life to encourage me ,

To give me help and to protect me.

May God guard and protect them;

*I dedicate to my sister ***Sabrina***;*

*To my brothers ***Zakaria, Mohammed El hadi, AbdRaouf****

*To the **Bekkouche** family;*

*To my future husband ***Nidhal*** "iinsha' allah";*

*To my friend ***Maria*** for being alongside me;*

All my friends; To all those who are dear to me;

To all those who love me; to all those I love; I dedicate

This work

Bekkouche Boutheyn





Dedication

*I dedicate to my mother and my aunt Faiza may ALLAH have
mercy on them*

To my grandmother and my aunts Samia and Djamila

*To my dear father ELhachmi and my beloved
brothers Chouaib and Siradj and my dear sister Asia*

To my uncle Mohammed, Mabrouk, Nouaman and Hassan

And specially and most of all my lovely husband Youcef

*To everyone who was a reason to encourage me, to all friends
and loved ones to both families DEBBA and TATI*

DEBBA Khaoula



Abstract:

Personal authentication of individuals has applications in a variety of important areas, ranging from forensic science to commercial and government services. The biological characteristics of individuals have been used as an effective security system in what we call the biometric system.

These systems depend on the particular characteristics of the human body such as fingerprints, eye shape, walking, sound, etc. In these systems, fingerprints are important because of their advantages, such as ease of use, high security and simplicity. On the basis of all this, we have developed an identification system using fingerprint.

In all biometric systems, there are different techniques for extracting characteristics to describe texture information. Finally, we run the results of fuzzy logic on biometrics been using the Matlab program.

Key words: Biometrics system, Mobile vote, Fingerprint, Identification, fuzzy logic, palm print.

Résumé:

L'authentification personnelle des individus trouve des applications dans différents domaines importants, allant de la criminalistique aux services commerciaux et gouvernementaux. Les caractéristiques biologiques des individus ont été utilisées comme système de sécurité efficace dans ce que nous appelons le système biométrique.

Ces systèmes dépendent des caractéristiques particulières du corps humain telles que les empreintes digitales, la forme des yeux, la marche, le son, etc. Dans ces systèmes, les empreintes sont importantes en raison de leurs avantages, tels que la facilité d'utilisation, la haute sécurité et la simplicité. Sur la base de tout cela, nous avons développé un système d'identification par le biais des empreintes des articulations des doigts (Fingerprint).

Dans tous les systèmes biométriques, il existe différentes techniques d'extraction des caractéristiques pour décrire les informations de texture. Finalement, nous avons exécuté les résultats de la logique floue sur la biométrie en utilisant le programme de Matlab.

Mots clés: Traitement d'images, Biométrie, vote mobile, Reconnaissance de empreint digital, logic flou, La paume de la main, identification.

المخلص:

تجد عملية تحديد الهوية الافراد تطبيقات في مجموعة متنوعة من المجالات المهمة من الطب الشرعي الى الخدمات التجارية والحكومية، تم استخدام الخصائص البيولوجية للأفراد كنظام امان فعال فيما نسميه النظام البيو متري، تعتمد هذه الأنظمة على خصائص معينة للجسم البشري مثل بصمات الأصابع وشكل العين والمشى والصوت الخ. في هذه الأنظمة تعتبر بصمات الأصابع مهمة بسبب مزاياها مثل سهولة الاستخدام والأمان العالي والبساطة على هذا الأساس قمنا بتطوير نظام تحديد الهوية من خلال بصمة الاصبع.

في جميع النظم الحيوية، هناك تقنيات مختلفة لاستخراج الميزات لوصف معلومات النسيج في عملنا استخدمنا طريقة النمط الثنائي المحلي، يتم تطبيق عملنا على قاعدة بيانات معروفة في هذا المجال وقد حقق نتائج مقبولة.

الكلمات المفتاحية : بيو متري، التعرف على البصمة، النمط الغامض، التصوي ت المحمول، راحة اليد، التعرف على الهوية.

Table of content

Acknowledgement.....	I
Dedications.....	II
Abstract.....	III
List of figures and tables.....	IV
List of symbols etabreviations.....	V
General Introduction	01

CHAPTER 1: Biometric Fundamentals

1.1 Introduction	03
1.2 Person recognition.....	03
1.2.2 Something you have	03
1.2.3 Something you know	03
1.2.3 Something you are.....	03
1.3 Biometrics.....	04
1.3.1 Physiological traits.....	04
1.3.2 Behavioral traits.....	05
1.4 Biometric system	05
1.4.1 Biometric system component	05
1.4.2 Recognition (fingerprint and face).....	06
1.5 Biometric functionalities	09
1.5.1 Verification.....	09
1.5.2 Identications.....	09
1.6 Performance errors	10
1.6.1 Performance mesures of a biometric system	10
1.6.1 Performance mesures graphic.....	11
1.7 Evaluation of a biometric system	12
1.8 Applications of biometric systems	13
1.8.1 Commercial applications	14

1.8.2 Government applications	14
1.8.3 Forensic applications	14
1.9 Conclusion	14

CHAPTER 2 :Electronic Voting

2.1 Introduction	15
2.2 Electronic voting	15
2.2.1 Definition.....	15
1.6.1 History	15
1.6.1 Types of electronic voting system	15
2.3 –Requirements analyses and system design	18
2.3.1 Requirements definition for the secure E-voting system.....	18
2.3.2 Architecture of secured model for E-voting system.....	19
2.3.3 Requirements electoral system	20
2.4 Advantages of electronic system	20
2.5 Applications.....	20
2.6 Conclusion.....	21

CHAPTER 3 :Using mobile phone

3.1 Introduction	22
3.2 Mobile voting	22
3.3 Advantage of mobile phone	22
3.3 System design and architecture	22
3.5 System requirements	25
3.6 Matlab implementation of fingerprint recognition or palmprint recognition using (fussy login feature extraction)	25
3.6.1 Fundamental steps of digital image processing.....	26
3.6.2 Feature extraction by fuzzy login	27
3.6.3 Matching.....	29
3.7 Conclusion.....	30

CHAPTER 4 :Simulation and Results

4.1 Introduction	31
4.2 Recognition palm print	31

Liste of figures and tables

4.2.1 Definition of palm print.....	31
4.2.1 Why palm print.....	31
4.2.3 Feature of palm print	31
4.2.4 System of palm print recognition	32
4.2.5 Data base of palm print.....	32
4.2.6 Separation of data bases	33
4.3 General view blurred form	34
4.4 Conclusion.....	36
4.5 Recommendations	36
General Conclusion	37
Références	

List of figures

Figure 1.1: Three basic approaches to person recognition.....	03
Figure 1.2: Types of biometrics.....	04
Figure 1.3 : Two phase of system biometrics.....	06
Figure 1.4 :Flowchart of fingerprint recognition.....	07
Figure 1.5: fingerprintsensing.....	07
Figure 1.6 :Different feature extraction algorithms may have different flowcharts.....	08
Figure 1.7 :Flowchart of Minutiae matching.....	08
Figure 1.8 :Biometric face recognition-how does it work.....	09
Figure 1.9 :The difference between verification and identification.....	10
Figure 1.10 :Example of a ROC curve: FAR against FRR.....	11
Figure 1.11:Examples of CMC curves of three biometric systems.....	12
Figure 2.1: La A traditional means of voting by paper	16
Figure 2.2 :Kiosk	16
Figure 2.3 :Punched card voting	17
Figure 2.4 :Optical Scanner	17
Figure 2.5 :Electronic voting machine(EVM).....	17
Figure 2.6 :Online voting.....	18
Figure 2.7:Secure Electronic System Architectural Diagram.....	19
Figure 3.1 :Architecture of Proposed System.....	23
Figure 3.2 :Methodology of the system.....	26
Figure 3.3 :Fundamental Steps of Digital Image Processing.....	27
Figure 3.4 :Fuzzy logic architecture.....	28
Figure 4.1 :Palm print features.....	32
Figure 4.2 :MATLAB interface.....	34
Figure 4.3 :Fuzzy logic image.....	34
Figure 4.4 :Shades of grey.....	35
Figure 4.5:Relation genuine and impostor of threshold.....	37
Figure 4.6:Relation FAR and FRR.....	37
Figure 4.7: ROC Curve.....	38
Figure 4.8: ROC Curve relation FAR and FRR.....	38
Figure 4.9: CMC Curve	39

List of tables

Table.I.1: Comparison of different biometrics.....13
Table1.2 : Les Different applications of biometrics system.....14
Table3.1 :Sytemrequirments.....25
Table 4.1: Results of uni_modal systems for the Threshold challenges.....36

ICT:	Information And Communication Technology.
PIN:	Password Identification Number.
FVR:	Finger Vein Recognition.
FVA:	Finger Vein Authentication.
FMR:	False Marche Rate.
FAR:	False Accept Rate.
FNMR:	False Non-March Rate.
FRR:	False Reject Rate.
EER:	Equal Error Rate.
GAR:	Genuine Accept Rate.
ROC:	Receiver Operating Curve.
CMC:	Cumulative Match Characteristic Curve.
EV:	Electronic vote.
ATM:	Automated Teller Machine.
OASIS:	Organization For The advancement of-Structured Information Standards.
MVC:	Mobile Vote System .
MPV:	Mobile Phone Vote .
LBP:	Local Binary Variance Pattern.
FVC:	Fingerprint Verification Competition.

General Introduction

Voting for any social issue is essential for modern democratic societies that is more easy and efficient; nowadays it is becoming very important to make the voting process that is late in its time in respect of the usage of modern ICT.

Today area, there is a need for this process to be linked with most advanced technologies against traditional way of voting where people go to an election office and verify their identity with identification card where we believe that their names are already available, and if so after authentication, a ballot may be a simple scrap of paper preprinted to protect the secrecy of the votes.

The voter casts their ballot in a box at a polling station electoral ink is applied to the forefinger (usually) of voters during elections in order to prevent electoral fraud such as double voting. After the voting Schedule is complete, booth officials will then take the ballot boxes to a centralized place, then declare the voting results by manually and tally the counts, these processes are often lengthy and inaccurate; the manual process leaves scope for errors to creep in political dishonesty and political fraud.

With all these problems in mind, we are here proposing a novel Mobile voting technique. With the hope that this biometric based on technology will erase the above mentioned issues and increase the level of safety compared to the popular method.

Therefor the need to design a secure voting system is very important. Also, another factor to take into consideration, is mobility; that in modern society affects almost all ages categories, and this leads to a dependency on our devices like smart-phones and tablets.

Secure mobile voting system by using encryption and biometrics is used to keep the privacy of voting choice and also to secure the communication between mobile application and server.

As students, we see an opportunity to explore a very complex topic and to share our solution with others; As an Algerian citizen, We are very interested in ensuring that our vote is taken in to consideration and also we are very interested to make sure that all of eligible voters from inside the country and outside have the possibility to vote and do not depend on election offices speed of validating voters.

In the first chapter, we provided some definitions of biometrics and different biometric methods, then we detail the method of fingerprint and facial recognition for identification by someone.

In the second chapter, we present the design and development of secure e-voting to ensure a free, fair and credible election, to improve voter authentication distinctiveness attribute to secure electorates from identity theft, fingerprint biometrics authentication has been adopted.

In the third chapter, we will suggest using the mobile phone with biometrics to fingerprint and ensure the integrity of elections and we study fingerprint as a database.

We have suggested a very modern and effective way to recognize finger print or palm print. This is the approach is called the fuzzy logic the reasons the pressure to use the fuzzy logic method is due to its impressive performance of fingerprint, efficiency and simplicity of calculation, it is well suited for difficult tasks Image analysis.

The last part of the last chapter covers the various tests and results obtained after that evaluate our system. As well as modeling the application to the programMatlab.

In the end, we will end with a conclusion and views regarding the work done.



CHAPTER 1



*Biometric
Fundamentals*

1.1 Introduction :

In human identification biometrics is one of the biggest tendencies. Nowadays, in many real applications like security, forensic and other identification and recognition purposes, biometrics is widely used.

Here we have discussed and compared different biometric features along with their use.

1.2 Person Recognition:

The fundamental task in identity management is to establish the association between an individual and his personal identity. One must be able to determine a person's identity or verify the identity claim of an individual whenever required. This process is known as person recognition. [1] A person can be recognized based on the following three basic methods (see Figure 1.1):

1.2.1 Something you have:

Key.

Card or badge.

1.2.2 Something you know:

Password.

Pin.

A memory (unique) to you.

1.2.3 Something you are:

Biometric (physiological and behavioral).

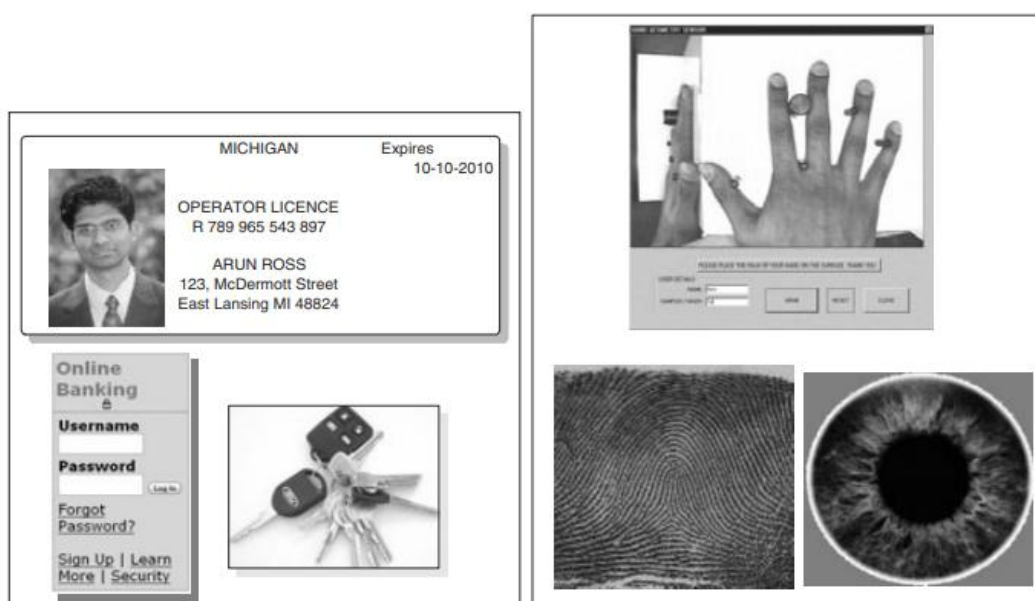


Figure 1.1 Three basic approaches to person recognition

1.3 Biometrics:

Biometrics is the science and technology of measuring and analyzing biological data of human body. It is the automated use of physiological or behavioral characteristics to determine or verify identity.

The automated use of behavioral (e.g. Voice, Dynamic Signature) and physiological (e.g. Face recognition, Fingerprint recognition, etc.) .Characteristics are regularly used to manually verify or determine identity, these physiological or behavioral characteristics can be used for automated recognition. **Figure1.2[2]**

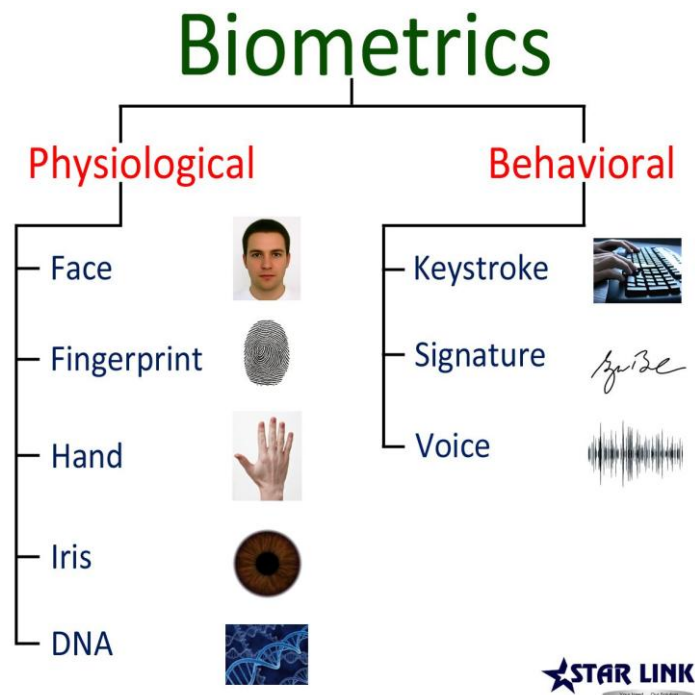


Figure1.2Types of biometrics

1.3.1Physiological traits:

- **Fingerprint:** Visual Biometric the use of the ridges and valleys found on the surface tips of a human finger to identify an individual. [3]
- **Hand:** Visual/Spatial Biometric The use of the geometric features of the hand such as the lengths of fingers and the width of the hand to identify an individual [3].
- **Face:** Visual Biometric The analysis of facial features or patterns for the authentication or recognition of an individual's identity. Most face recognition systems use local featureanalysis[3].
- **Iris:** Analysis of the iris of the eye, which is the colored ring of tissue that surrounds the pupil of the eye. Based on visible features and widely

regarded as the most safe, accurate biometrics technology and high speeds, High accuracy.

1.3.2 Behavioral traits:

- **Typing Rhythm:** The rhythms with which one types at a keyboard are sufficiently distinctive to form the basis of the biometric technology known as keystroke dynamics.
- **Voice:** A more behavioral individual aspect of humans are their voices. Everybody has a special mode and tone while speaking. Voice recognition tries to analyze these features and use them to identify a person [4].
- **Signature:** Another behavioral aspect of a person usable by biometrical analyses is the signature. Not only the form but also the dynamic aspects movable biometric input could be the rhythm and pattern of a person's walk.[1]can be seen as a set of unique features of a person. Other possible

1.4 Biometric systems:

A biometric system measures one or more physical or behavioral characteristics; these characteristics are referred to different terms such as traits, indicators, identifiers, or modalities. [1]

This process consists of two main phases namely, enrollment and recognition.(See figure1.3)

During the enrollment phase, the biometric data are acquired from the individual and stored in a database along with the person's identity.

During the recognition phase, the biometric data are reacquired from the individual and compared against the stored data to determine the user identity.

Thus, a biometric system is consisting of four basic building blocks namely, sensor, feature extractor, database, and matcher.

1.4.1 Biometric system components:

Sensor module:

It is the interface between the real world and the system. The biometric sensor or reader is needed to measure or record the raw biometric data of the user, collects data and converts the information to a digital format.

Feature extraction module:

Feature extraction takes place during enrollment and verification-any time a template is created. The feature extraction process perform quality control activities and develop the biometric template.[5]

✚ *Database module:*

The biometric system database acts as the repository of biometric information. During the enrollment process, the feature set extracted from the raw biometric sample (i.e., the template) is stored in the database along with some personal identity information (such as name, Personal) Identification Number (PIN), address, etc.) Characterizing the user.[1]

✚ *Matching module:*

Compares the new biometric templates to one or more templates in data storage.[5] During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Local binary variance pattern).

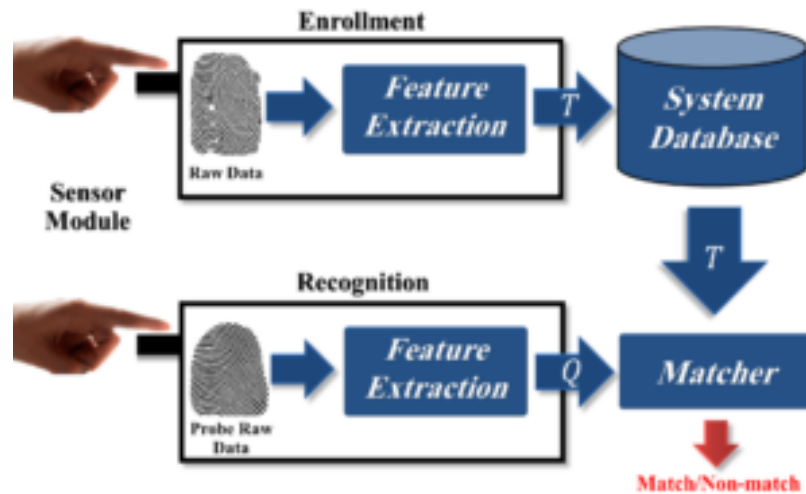


Figure1.3Two phase of system biometrics

1.4.2 Recognition (fingerprint and face)

✚ *Fingerprint recognition:*

Use technologies of sensor, image processing, and pattern recognition to automatically or semi-automatically determine if two fingerprints are matched or not.[5]

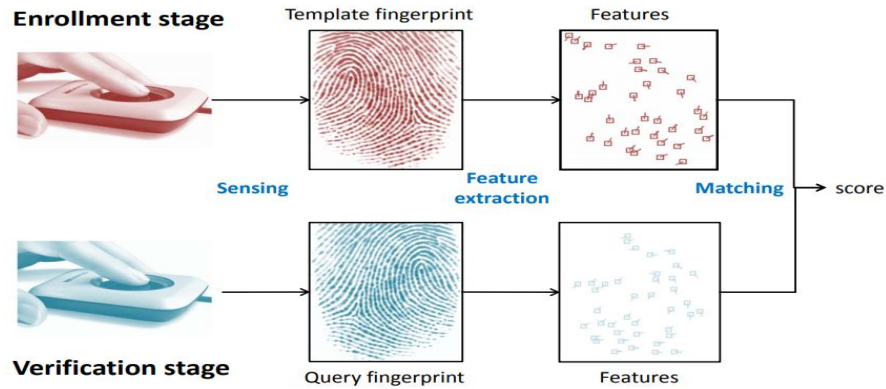


Figure1.4Flowchart of fingerprint recognition

❖ *Fingerprint sensing:*

The process of capturing and digitizing the fingerprint of an individual.

Digital images of the fingerprints can be acquired using Off-line method – on-line method.[5]



Figure1.5Fingerprint sensing

❖ *Fingerprint features:*

A fingerprint can be described at 3 levels from coarse to fine.

Coarse level representation can be derived from finer level representations.

- Level 1: ridge orientation and frequency (singularity is a compact but lossy compression of ridge orientation field)
- Level 2: ridge skeletons (minutiae set is a compact but lossy compression of ridge skeletons)
- Level 3: outer and inner contours of ridges.[6]

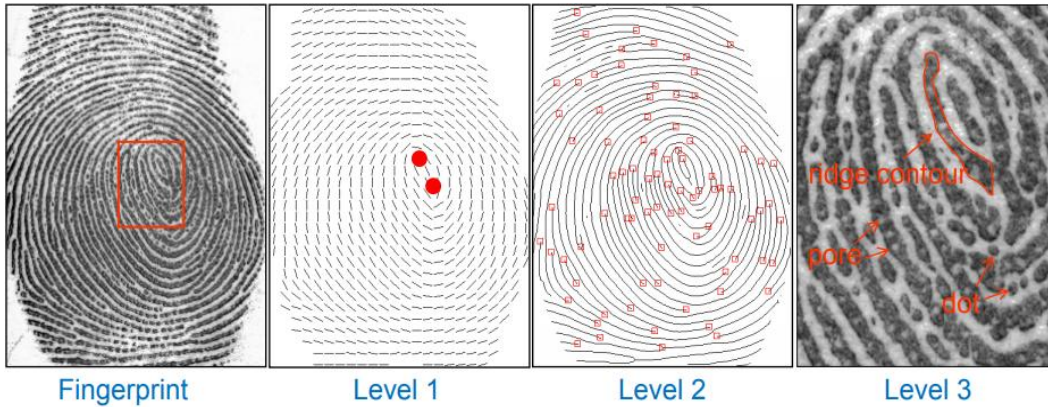


Figure 1.6 Different feature extraction algorithms may have different flowcharts

❖ *Minutiae matching:*

Almost all fingerprint matchers are based on minutiae matching.

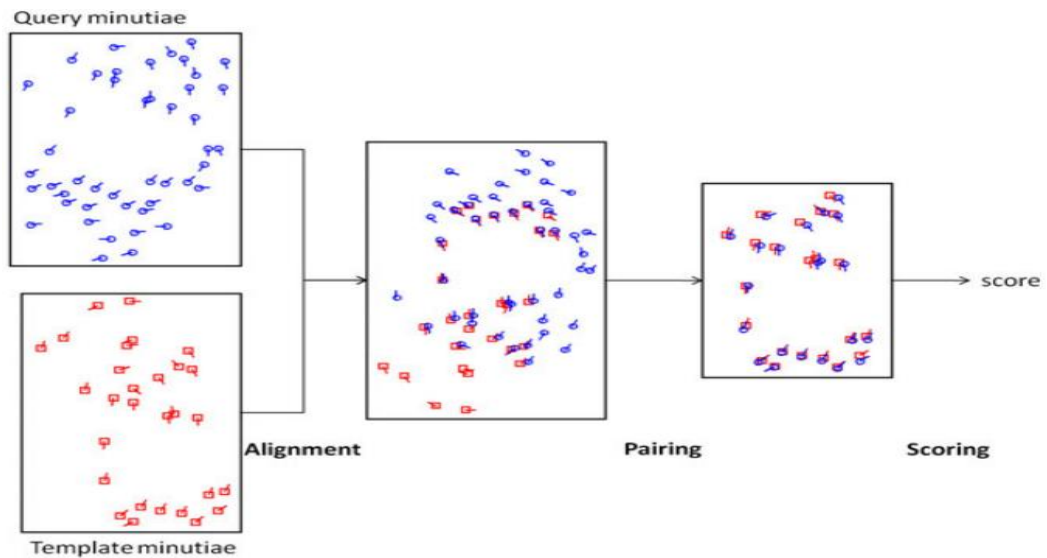


Figure 1.7 Flowchart of Minutiae matching

✚ *Face recognition:*

Face recognition can be defined as the process of establishing a person's identity based on their facial characteristics. In its simplest form, the problem of face recognition involves comparing two face images and determining if they are of the same person.

Face images of a person may have variations in age, and facial expressions, as well as exhibit changes in appearance due to make-up, facial hair, or accessories, there may be similarities between the face images of different persons, especially if they are genetically related (e.g., identical twins, father and son, etc.). Such inter-class similarities further compound the difficulty of recognizing people based on their faces.

Techniques for automated face recognition have been developed for the purpose of person recognition from still 2-dimensional (2D) images, video (a sequence of 2D images), and 3D range (depth) images[1]

Capturing: the foremost requirement is to capture the image and that can be done by scanning existing images or using cameras.

Extracting: unique facial data is then extracted from the sample.

Comparing: the data is then compared with the database.

Matching: the software then decides whether the sample matches any picture in the database or not.

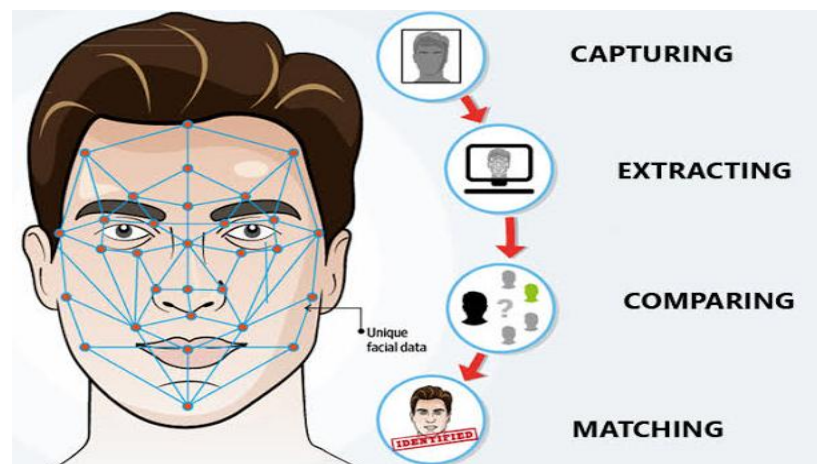


Figure1.8 Biometric face recognition-how does it work

1.5 Biometric Functionalities:

1.5.1 Verification:

Is a method that specifies a template for the person to be authenticated and compares with their actual finger placed on the FVR device, it is often referred to as 1:1 (one-to-one).

The process of providing a username and biometric data is referred to as authentication.

1.5.2 Identification:

Picks up one person from up to 10000 reenrolled templates just placing a finger on the FVA device. This method has superior user-friendliness as no specification is identification is needed. Identification is often referred to as 1:N(one-to-N or-to-many),because a person's biometric information is compared against multiple(N) records.

✚ **Closed-set identification:** The person is known to exist in the database.

- ✚ **Open-set identification:** Person is not guaranteed to exist in the database. System determines if the person is in the database. [5]

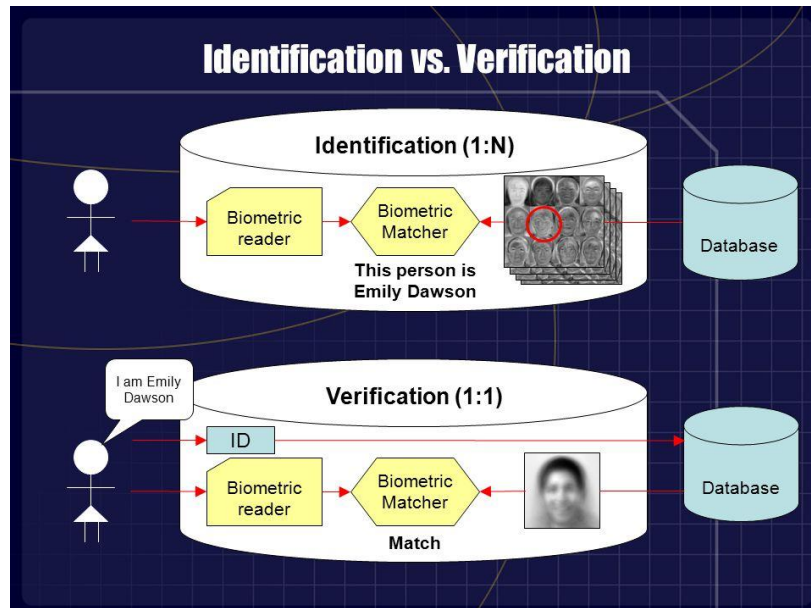


Figure 1.9 The difference between verification and identification

Verification systems are generally faster and more accurate than identification systems. Identification systems require more computational power than verification systems, because more comparisons take place before a match occurs. [2]

1.6 Performance Errors:

Wrong performance by system is termed as decision error. Performance errors are divided into two categories, false accept and false reject. [7]

1.6.1 Performance measures of a biometric system:

- ✚ **False match rate (FMR, also called FAR = False Accept Rate):**

The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs that are incorrectly accepted. In case of similarity scale, if the person is an imposter in reality, but the matching score is higher than the threshold, then he is treated as genuine. This increases the FMR, which thus also depends upon the threshold value.

This rate represents the percentage of people who are supposed to be unrecognized but who are nonetheless accepted by the system Eq(1).

$$FAR = \frac{\text{number of imposter transaction attempts accepted}}{\text{total number of imposter transaction attempts.}}$$

✚ **False non-match rate(FNMR, also called FRR = False Reject Rate):**

The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs that are incorrectly rejected.

This rate represents the percentage of people who are supposed to be recognized who are rejected by the system .Eq(2).

$$FRR = \frac{\text{number of genuine transaction attempts rejected}}{\text{total number of genuine transaction attempts.}}$$

✚ **EER(EqualError Rate):**

This rate is calculated from the first two criteria and constitutes a measurement point for current performance. This point corresponds to where FRR=FAR.Eq(3), the best compromise between false rejections and false acceptances.

$$EER = \frac{\text{number of false rejections} + \text{number of false acceptances}}{\text{total number of transaction attempts.}}$$

✚ **GenuineAccept Rate (GAR):**

In addition to the above parameters there is Genuine Accept Rate (GAR) Eq4).

$$GAR=1-FRREq(4)$$

1.6.2 Performance measuresgraphics:

✚ **ROC (Receiver operating characteristic curve):**

Plot of the rate of FMR as well as FAR (i.e., accepted impostor attempts) on the x-axis against the corresponding rate of FNMR as well as FRR (i.e., rejected genuine attempts) on the y-axis plotted parametrically as a function of the decision threshold. An illustration of a ROC curve is presented in **Figure 1.9. [8]**

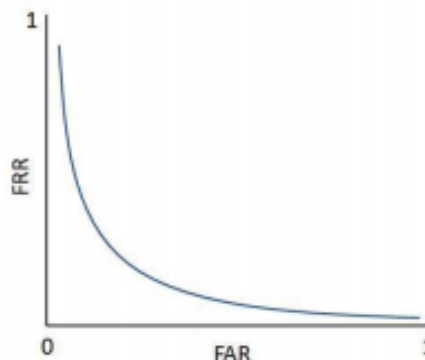


Figure1.10Example of a ROC curve: FAR against FRR

✚ CMC(Cumulative match characteristic curve):

Graphical presentation of results of an identification task test, plotting rank values on the x-axis and the probability of correct identification at or below that rank on the y-axis. Examples of CMC curves are given in **Figure 1.10**. [8]

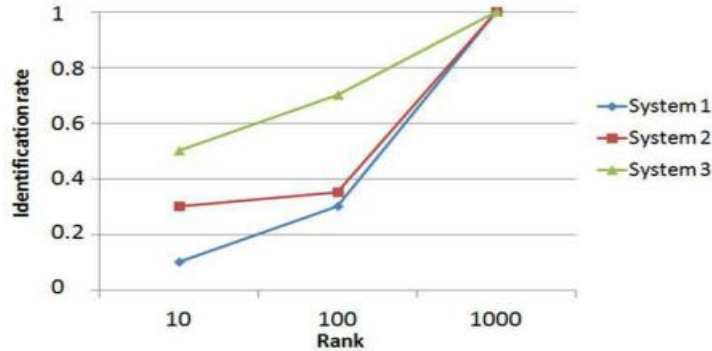


Figure 1.11 Examples of CMC curves of three biometric systems

1.7 Evaluation of biometric systems:

❖ Biometric modalities:

Each biometric information that can discriminate individuals is considered as a biometric modality. An ideal biometric information should respect the following properties [8]:

- **Universality:** all individuals must be characterized by this information.
- **Uniqueness (distinctiveness):** this information must be as dissimilar as possible for two different individuals.
- **Permanency:** it should be present during the whole life of an individual.
- **Collectability:** it can be measured in an easy manner.
- **Acceptability:** it concerns the possibility of a real use by users.
- **Circumvention:** Circumvention relates to the ease with which a trait might be imitated using an artifact or substitute.
- **Performance:** Performance relates to the accuracy, speed, and robustness of technology used (see performance section for more details).

Table 1.1: Comparison of different biometrics.

Biometric-s identifier	Universality	Uniqueness	Permanency	Collectability	Acceptability	Circumvention	Performance
Fingerprint	M	H	H	M	M	M	H
Face	M	L	M	H	H	H	L
Iris	H	H	H	M	L	L	H
DNA	H	H	H	L	L	L	H
Voice	M	L	L	M	H	H	L
Signature	L	L	L	H	H	H	L
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	L	M

According to the International Organization for Standardization, the quality assessment of biometric raw data is divided into three points of view:

- **Character:** Refers to the quality of the physical features of the individual.
- **Fidelity:** Refers to the degree of similarity between a biometric sample and its source.
- **Utility:** Refers to the impact of the individual biometric sample on the overall performance of a biometric system.

1.8 Applications of Biometric Systems:

Establishing the identity of a person with high confidence is becoming critical in a number of applications in our vastly interconnected society.

The need for reliable user authentication techniques has increased in the wake of heightened concerns about security, and rapid advancements in networking, communication, and mobility. Thus, biometric recognition is being increasingly incorporated in several different applications. These applications can be categorized into three main groups (see **Table 1.2**): [1]

1.8.1 Commercial applications:

Commercial applications such as computer network login, electronic data security, e-commerce, Internet access, ATM (Automated Teller Machine) or credit card use, physical access control, mobile phone, PDA, health record management, distance learning, etc.

1.8.2 Government applications:

Government applications such as national ID card, managing inmates in a correctional facility, driver's license, social security, welfare-disbursement, border control, passport control, etc.

1.8.3 Forensic applications:

Forensic applications such as corpse identification, criminal investigation, missing children, parenthood determination.

Table 1.2 Different applications of biometrics system.

FORENSICS	GOVERNMENT	COMMERCIAL
Corpse identification	National ID card	ATM
Criminal investigation	Drivers License; voter registration.	Access control; computer login
Parent-Hood détermination	Welfare désabusement	Mobile phone
Missing children	Border crossing	E-commerce; Internet; banking; smart card

1.9 Conclusion:

In this chapter, we have discussed some basic conception and definitions as; the biometrics and their various technique along with the main modules of biometrics systems and the performance in addition to the application areas.



CHAPTER 2



Electronic Voting

2.1 Introduction :

The conventional voting scheme employs paper-based ballot to verify votes. This voting scheme is insecure due to these attributed election irregularities.

In this chapter, we present the design and development of secure e-voting to ensure a free, fair and credible election, to improve voter authentication distinctiveness attribute to secure electorates from identity theft, fingerprint biometrics authentication has been adopted. [9]

2.2 Electronic voting:

2.2.1 Definition:

It is also known as electronic voting is a term encompassing several different types of voting, embracing both electronic means of casting a vote and electronic means of counting votes[10].

Electronic voting technology can include various types of voting such as kiosks, the Internet, telephones, punch cards, and mark sense or optical scan ballots.

The Council of Europe recommendations defined electronic voting (e-Voting) as “the use of electronic means in at least the casting of the vote” (Krimmer, et al., 2007). [4]

2.2.2 History:

The world is in the midst of a revolution in the way they vote. This revolution began in the 1960's with the introduction of punched-card ballots, continued with the introduction of optical mark-sense ballots and direct-recording electronic voting machines in the 1970's. By 2000, they continued and started tentative experiments with Internet voting.

2.2.3 Types of Electronic Voting Systems:

There are two types of e-voting systems: On-Line and Offline. On-line, e.g. via Internet, and offline, by using a voting machine or an electronic polling booth.

Electronic voting techniques (off-line):

There are five broad classes of voting technology in use today:

- ✓ *Paper ballots:*The paper-based voting system can be described as the traditional means of voting that has been in used over the ages [4].



Figure2.1A traditional means of voting by paper

- ✓ *In Info-kiosk schemes:* (i-voting), voting machines are located away from traditional polling places. The i-voting platform and physical installation should be under the control of election officials and should also be appropriately monitored in order to meet security and privacy requirements and to prevent intervention (e.g. coercion) [11].



Figure2.2kiosk

- ✓ *Punched Card Voting:* punch cards is a piece of stiff paper that can be used to store information by the presence or absence of holes in specific locations. The votomatic system of voting on punched cards was first used in Georgia in 1964, using IBM's Port-punch punch mechanism [11].

Perforated cards played an important role in processing information automatically during the second half of the twentieth century. People used to keep computer programs at that time in the form of piles of perforated cards, as there were no alternatives such as quick memories other than magnetic tapes in their primitive dress.



Figure 2.3 Punched card voting

- ✓ **Optical and digital scanning (Markesense):** In an optical scan voting system, each voter's choices are marked on one or more pieces of paper, which then go through a scanner.

The scanner creates an electronic image of each ballot, interprets it, creates a tally for each candidate, and usually stores the image for later review.



Figure 2.4 Optical Scanner

- ✓ **Direct Recording Electronic computers (DREs):** These are machines or computers normally installed at a polling station, which record and simultaneously store the vote [12].



Figure 2.5 Electronic voting machine (EVM)

Internet Voting System (on-line):

Internet voting is defined as an election system that utilizes the internet to ensure access to a website or domain which makes use of electronic ballots. It is a secure system that allows for eligible voters to cast their votes from any (remote) location [4].

The online system procedures are very easy, transparent and most secure than electronic voting. The most common way for the remote voting system is postal voting system, where voters cast their votes through their cell Phones [13].



Figure 2.6 Online voting

2.3 Requirements Analyses and System Design:

As students at University Kasdi Merbah hope to replace electronic voting instead of traditional voting for saving university resources and time. The main goal of e-Voting is to provide voters (students or professors) a good environment so that students can cast their votes with minimum cost and efforts.

2.3.1 Requirements Definition for the Secure E-voting System:

There are so many properties have been proposed to make the e-Voting secure process:

- **Eligibility:** Only eligible voters are permitted to cast their ballots.
- **Privacy:** There is no association between voter's identification and a marked ballot.
- **Uniqueness:** No voter can cast his ballot more than once.
- **Completeness:** No one can forge a valid ballot and a voter's ballot cannot be altered, the valid ballots are counted correctly.
- **Fairness:** No one can falsify the result of voting.
- **Verifiability:** Voters can verify that their ballots are counted correctly.

- **Uncoercibility:** No voter can prove what he voted to others to prevent bribery.
- **Efficiency:** The computations can be performed within a reasonable amount of time.
- **Mobility:** The voter can vote anytime and anywhere through internet. (Kashif H.M et al, 2011).
- **Transparency:** Voters should be able to possess a general knowledge and understanding of the voting process.

2.3.2 Architecture of Secured Model for E-Voting System:

The system architecture is adapted from the 3-layered Organization for the advancement of Structured Information Standards (OASIS):

The pre-electoral phase, electoral phase and post-electoral phase. The architecture is shown in **Figure 2.7**.

- In the pre-electoral phase an intending voter fingerprint and personal data are captured and stored into the system.

The system spontaneously assigns a serial ID to that voter in the system. All registration details are saved in the data-base.

- At electoral phase, the voter is granted access into the voting system by fingerprint verification, and if valid he/she is allowed to vote. The encoded vote is embedded into a cover photo which is then directed into the database to be sorted at the post-electoral phase.
- The final phase is the post-electoral phase where votes casted are verified to satisfy they are unaltered during embedding process. The casted votes are retrieved and sorted, which is published for the electorate [9].

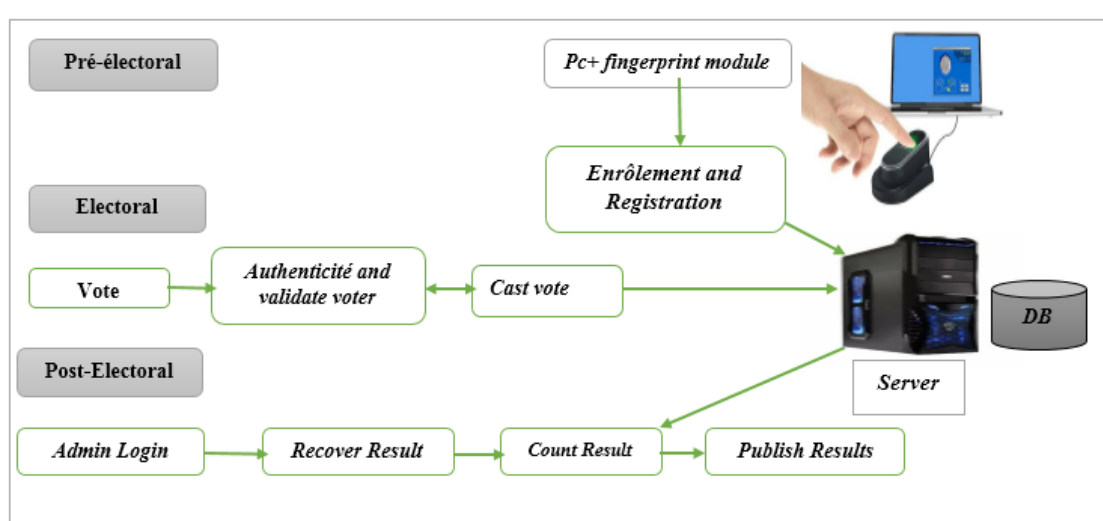


Figure 2.7 Secure Electronic System Architectural Diagram

2.3.3 Requirements of Electoralsystems:

The success of any democratic system in the world depends upon the faith of the voters in the system itself. Therefore, any voting system or technology must address and adhere to the electoral requirements. The requirements are as follows[4]:

- ❖ **Accessibility:** This seeks to accommodate all eligible voters in terms of ensuring that they all have access to a user-friendly system.
- ❖ **Fairness:** All eligible voters should be counted in the final tally.
- ❖ **Timeliness and accuracy:** Timeliness is based on the need to ensure that information is recorded and available results released as quickly as possible, while accuracy focuses on the ability to ensure that each individual's vote is recorded and counted.
- ❖ **Secrecy and privacy:** All participants must be permitted to vote in secret. It must also discourage both vote-buying and coercion.
- ❖ **Security:** Usually, human beings operate computer machines. Therefore, it may be easy for them to manipulate and interfere with the whole system.
- ❖ **Authentication and verification:** With regard to authentication, it should be ensured that individuals cannot be impersonated during voting. The need for verification emphasizes that the e-voting system must be able to independently verify that all voters have been correctly counted in a system (Akinyemi A.E., 2014).

2.4 Advantages of electronicvoting:

- The system can be used anytime and from anywhere by the employees.
- It excludes the use of manual voting process.
- Employees can keep themselves updated with all things going on in the organization.
- No one can cast votes on behalf of others and multiple times.
- Saves time and reduces human intervention.
- Increase the security and reliability of elections.
- Admin can get instant result.
- The system is flexible and secured to be used.[14]

2.5 Applications:

This project can be used in commercial organizations, corporations. It can also be used in schools, colleges, institutes, banks.[14]

2.6 Conclusion:

This chapter we introduction about Electronic voting and its variation, Issues of EV, Taxonomy, and Biometric based EV. Our efforts to understand electronic voting systems leave us optimistic, but concerned. This chapter suggest that the Electronic system has to be further studied and innovated to reach all level of community, so that the voter confidence will increase and election officials will make more involvement in purchasing the innovated electronics' for conduct smooth, secure, tamper resistant Elections.



CHAPTER 3



Using Mobile Phone

3.1 Introduction :

As introduced in the first chapter there are several biometrics modalities applied in the domain of identification and authentication, including fingerprints and face.

On this chapter we will suggest using the mobile phone with biometrics to facilitate and ensure the integrity of elections.

3.2 Mobile vote :

Mobile Voting System (MVS) is a very secure, efficient and easy way to casting of vote. Mobile Voting

System creating Online Voting System. All user will enter their details in verification form, server will check whether they are valid user or not. If it is valid, user server provide user Id and Password.

3.3 The advantage of mobile phone vote :

- ✓ Promises an increase in participation and offers voters more options.
- ✓ The system surely offers convenience to the voter, encourages more voters to cast their votes remotely, and has great potential to stimulate higher voter turnout.
- ✓ Reduced logistical and administrative costs – the system will reduce the materials required for printing and distributing ballots.
- ✓ The personnel required to assist in voting stations will also reduce.
- ✓ Casting and counting votes is much faster and more accurate, with this system by default there are no invalid or unclear ballots and the automatic gathering.
- ✓ This system MPV is counting of ballots reduces the amount of time spent counting votes and delivering the results.
- ✓ Greater accessibility for the old and disabled people this system will be perfect for the disabled and the older citizens as they will cast their votes comfortably at their own homes.[15]

3.4. System design and architecture:

The proposed system has 3 main entities as follows:

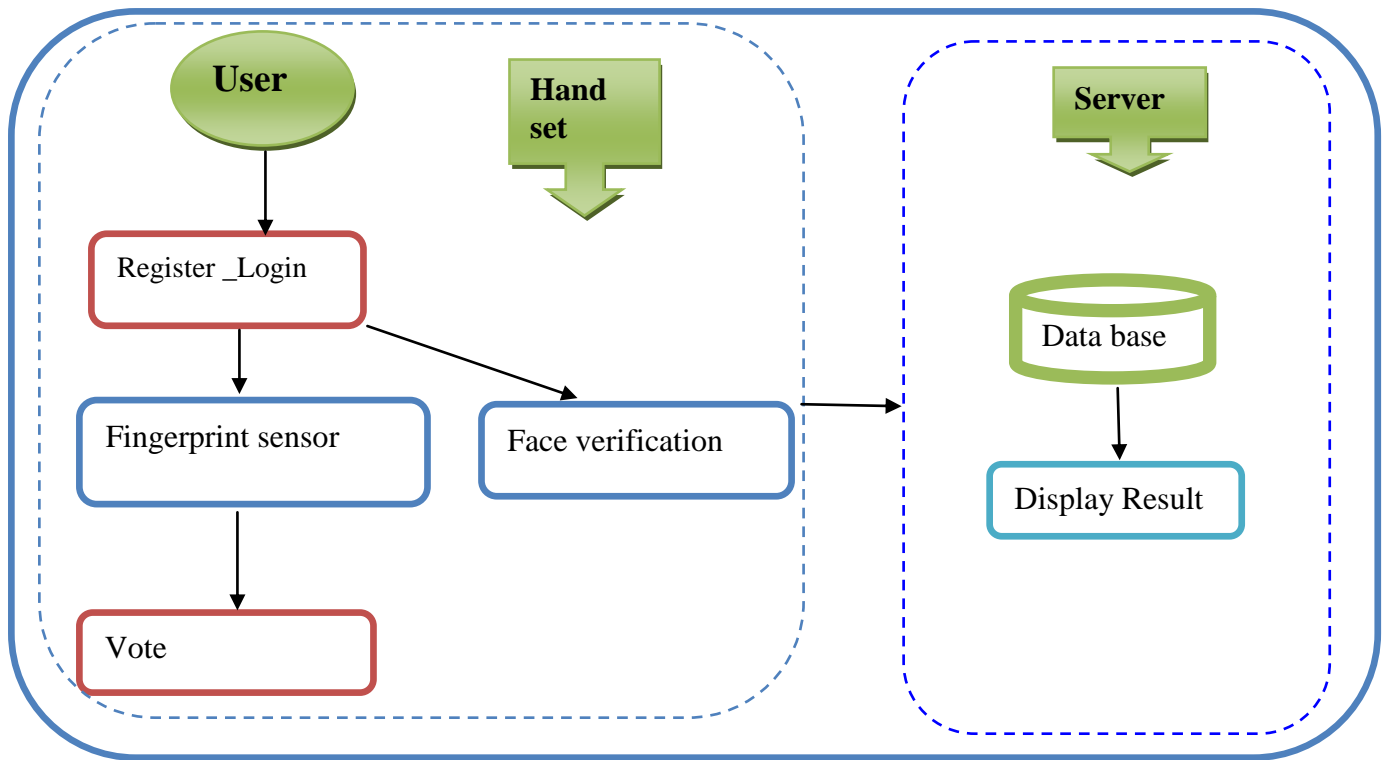


Figure3.1 Architecture of Proposed System

❖ **User:**

The user enters his/her details in the handset so that the system can verify the user in future and all data will be saved in the firebase database. The user provides name, date of birth, ID card number and phone number details. The module checks whether the entered user is valid or not by comparing it to the ID card database.

❖ **Hand set**

- **Register:** In the proposed system, the user registers with the following fields: name, date of birth, phone number, ID card number. On triggering the register button, the user details shall be stored in the database.
- **Login:** While logging in, the user have to enter the password which was set during the registration. Once the password is approved, it asks for fingerprint or face scan of user as the second stage of security.
- **Fingerprint sensor and face verification**
- **Fingerprint sensor:** After successful login, the next step is to verify the Users fingerprint. The user will have to give the fingerprint and will match the system fingerprints from the mobile database and the fingerprint

provided by the user. If the fingerprint match, it will give move to the next step for the vote.[16]

- **Face verification:** For the face verification, the system will use the camera on the handset. The database will already have the face of the user from the database. The proposed system will match the input face with that stored in the database. If matched, it will confirm that the user is verified and is valid to vote for the candidates.[16]
- **The vote:** Once verified and logged in, a list of candidates will be present on the screen. The voter must select one of them to vote for. Once a vote is cast, a confirmation dialog appears to ensure that the selection was purposeful. Finally, the vote is accepted and the tally for that candidate is incremented in the database. Then the voter is automatically logged out.

❖ **The server:**

The server will have 2 levels

- **Constituency level database (Level 1):** This database will be able to view data pertaining to voters and politicians within the respective constituencies. Each constituency will have the same database and allow ballot casting and counting. [13]
- **General or main level Database (Level 2):** This database in the Architecture is called the General (or main) Database. This database is like a watchdog. It monitors the validity of the information it captures like the Fingerprint or face and Voter id. It communicates with all the constituency level databases to ensure that person doesn't vote in more than one constituency. [13]

3.5 system requirements :

Table 3.1 Sytemrequirments

Hardware requirements	Software requirements
<ul style="list-style-type: none"> ✓ Computer ✓ Operating System_ Windows XP ✓ Intel Core 2 Duo Processor 1.8 GHz ✓ 1GB RAM, 100 GB HDD ✓ Any Smartphone running ✓ Android Operating System ✓ ver4.1 and above 	<ul style="list-style-type: none"> ✓ Language-Java and Android ✓ Java Development Kit ✓ Android SDK and ADT Plugin ✓ IDE- Eclipse , SQL Front ✓ Database- MySQL ✓ Web-Service- SOAP or RESTFUL ✓ Server- Apache Tomcat

3.6 Matlab implementation of fingerprint recognition or palm print recognition using (fuzzy login feature extraction) :

The Methodology of the system covering different steps start from collect the data from the dataset and preform the steps to remove the noise and make the images clear for extract the features by using fuzzy logic feature extraction method which related to extract the texture feature from fingerprint or palm print . Finally the feature was stored in dataset as template for matching stage which preform the matching between the test images and template in database and store the similarity score between them in matrix which called matching score. Figure 3.2 shows the block diagram of the fingerprint identification system.

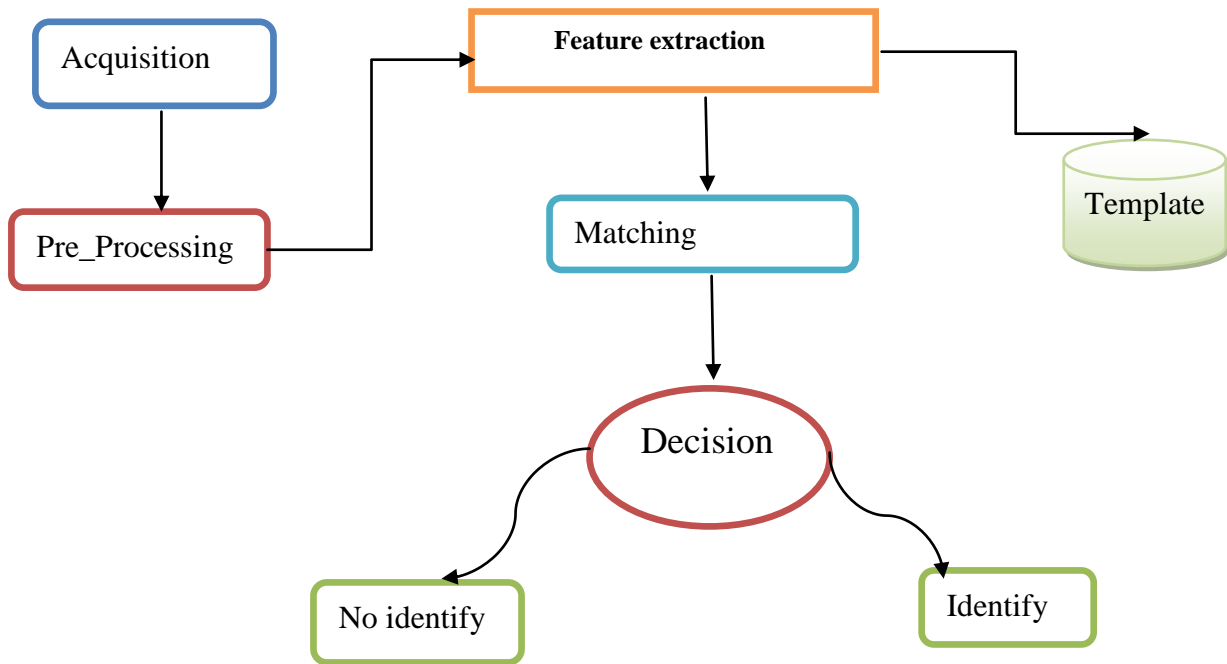


Figure 3.2 Methodology of the system

3.6.1 Fundamental Steps of Digital Image Processing:

There are some fundamental steps in digital image processing. Such as image acquisition, image enhancement, image binarization, image thinning, image extraction, image segmentation and image matching.

✚ Acquisition of Fingerprint

This is the first step or process of the fundamental steps of digital image processing. The Image Acquisition stage is the process to obtain images by different ways. There are two ways to capture fingerprint image online (Live scan) or offline (ink). In the online fingerprint identification the optical fingerprint reader is used to capture the image of fingerprint show figure 3-1 (a).

✚ Preprocessing

The fingerprint image is first pre-processed to extract the proper feature from any fingerprint images, these images have to be under clarity and quality measures. The pre-processing stage which leads to remove the noise and unwanted data by using enhancement techniques.

The fingerprint image pre-processing is used to increase the clarity of ridge structure. There are many steps for doing this process, such as Image Segmentation, binarization, Elimination of noise, smoothing and thinning which are used to

enhance the fingerprint image. **Figure 3-3 (b)** shows the preprocessing with first and second enhancements.

✚ Binarization

Binarization step of fundamental steps is binarization of fingerprint image which is a process to transform the image from 256 levels to two levels (0, 1) where the 0 corresponding to black, and 1 corresponding to white, the result of binarization **figure 3-3 (c)**.

✚ Thinning

The fourth step of the fundamental steps of digital image processing is thinning which shows in **Fig. 3-3 (d)** it is also called (skeletonization). To enhance the binary image the thinning algorithm is used to reduce the ridges of fingerprint images.

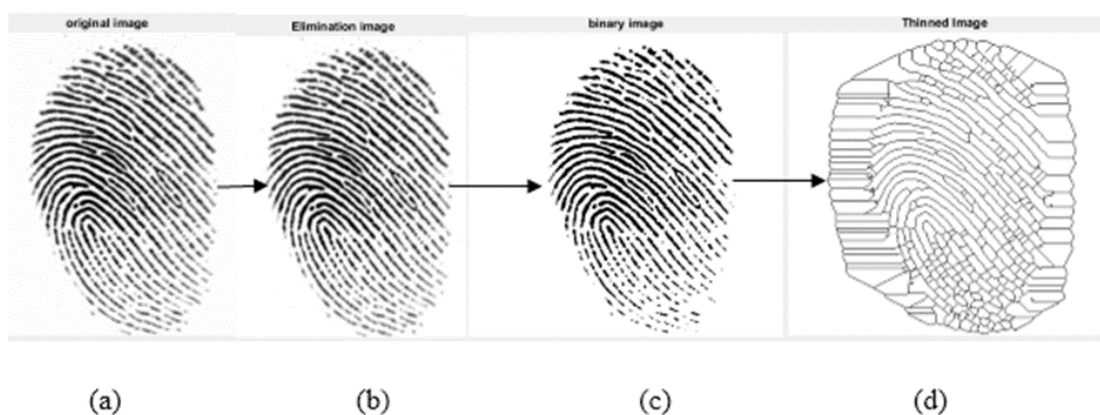


Figure 3.3 Fundamental Steps of Digital Image Processing

3.6.2 Feature extraction by fuzzy logic:

Fuzzy logic is relatively efficient and advanced theory, at present wide use of fuzzy logic is in the classification of remotely sensed images. A branch of biometric, palm print authentication have increasing attention because palm print is unique, permanent, measurable characteristics having voluminous of the line features.

This method use sub image based principle line feature extraction technique in low resolution palm print images. Image is divided into sub images and feature obtained from these sub images are combined to generate a single feature vector for the palm print image.

This vector is provides to fuzzy inference system as input.

✚ Fuzzy logic architecture

Its Architecture contains four parts:

- ❖ Rule Base: It contains the set of rules and the IF-THEN conditions provided by the experts to govern the decision making system, on the basis of linguistic information.

Recent developments in fuzzy theory offer several effective methods for the design and tuning of fuzzy controllers. Most of these developments reduce the number of fuzzy rules [17].

- ❖ **Fuzzification:** It is used to convert inputs i.e. crisp numbers into fuzzy sets. Crisp inputs are basically the exact inputs measured by sensors and passed into the control system for processing, such as temperature, pressure, rpm's, etc.[17]
- ❖ **Inference engine:** It determines the matching degree of the current fuzzy input with respect to each rule and decides which rules are to be fired according to the input field. Next, the fired rules are combined to form the control actions.[17]
- ❖ **Defuzzification:** It is used to convert the fuzzy sets obtained by inference engine into a crisp value. There are several defuzzification methods available and the best suited one is used with a specific expert system to reduce the error.[17]

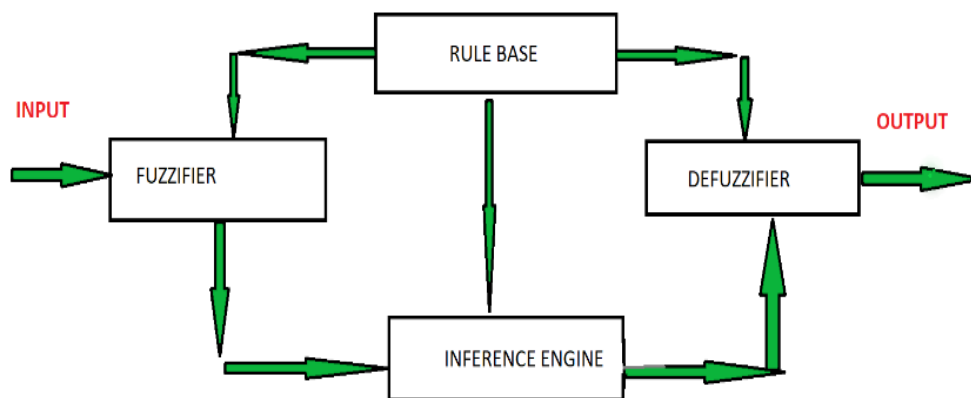


Figure 3.4 Fuzzy logic architecture

Membership function

❖ Definition

A graph that defines how each point in the input space is mapped to membership value between 0 and 1. Input space is often referred as the universe of discourse or universal set (u), which contain all the possible elements of concern in each particular application.

There are largely three types of fuzzifiers:

- Singleton fuzzifier
- Gaussian fuzzifier
- Trapezoidal or triangular fuzzifier

❖ Advantages of Fuzzy Logic System

- This system can work with any type of inputs whether it is imprecise, distorted or noisy input information.
- The construction of Fuzzy Logic Systems is easy and understandable.
- Fuzzy logic comes with mathematical concepts of set theory and the reasoning of that is quite simple.
- It provides a very efficient solution to complex problems in all fields of life as it resembles human reasoning and decision making.
- The algorithms can be described with little data, so little memory is required.[17]

❖ Disadvantages of Fuzzy Logic Systems

- Proof of its characteristics is difficult or impossible in most cases because every time we do not get mathematical description of our approach.
- As fuzzy logic works on precise as well as imprecise data so most of the time accuracy is compromised.

3.6.3 Matching:

In this section, the features were received from feature extraction stage and the matching start by comparing the feature vector from input (query image) with feature vector of template which was taken at enrollment stage, and the matching score was generated for each subjects. The matching scores either similarity score or distance between two feature vectors. Afterward, the score stored as matrix for decision purpose. In this work the Euclidean distance was used to perform the matching between query image and template.

Suppose there are two vectors one for fingerprint FV for which define as $FV = \{FV_1, FV_2, \dots, FV_n\}$ Hence, the Euclidean distance can be defined as Eq (3)

$$d(FV) = \sqrt{\sum_{i,j=1}^n (FV_i - FV_j)^2}$$

🚦 Decision

In this stage, final decision for identify the person by his /her biometrics data was taken either identify or non-identify (Accepted or Rejected). The genuine score and impostor score can be separated from the score matrix with the help of threshold values (T0) which were generated for each subject of the score matrix at the matching stage. The decision can be determined by Eq. (4) [18].

$$\text{Decision} = \begin{cases} \text{Accepted,} & \text{if Score} \geq T_0 \\ \text{Rejected,} & \text{if Score} < T_0 \end{cases} \quad (4)$$

3.7 Conclusion:

In this chapter, we suggested methodology our mobile phone based voting application by biometrics and the classification palm print or finger print images using fuzzy logic for different security aspects, It provides a very efficient solution to complex problems in all fields of life as it resembles human reasoning and decision making.

After implementing the recognition program under MATLAB, we will subsequently interpret the results of this application step by step in order to highlight the performance of this system.



CHAPTER 4



*Simulation
And
Results*

4.1 Introduction:

As he introduced in the first chapter, there are several biometric modalities applied in the area of identification and authentication. Among these modalities, we find that the palm print is a relatively new biometry. Our goal is to apply the fuzzy logic learning method to a system biometric based on the palm print modality.

4.2 Recognition palm print:

4.2.1 definition of palm print:

The palm print system is a hand-based biometric technology. Palm print is concerned with the inner surface of a hand. A palm is covered with the same kind of skin as the fingertips and it is larger than a fingertip in size.[19]

4.2.2 Why palm print:

- High Distinctiveness.
- High Permanence (duration).
- High Performance.
- Medium Collectability.
- Medium Acceptability.
- Medium Universality.
- Medium Circumvention (fooling).

4.2.3 Feature of palm print:

- **Geometry Features:** According to the palm's shape, we can easily get the corresponding geometry features, such as width, length and area.
- **Principal Line Features:** Both location and form of principal lines in a palm print are very important physiological characteristics for identifying individuals.
- **Wrinkle Features:** In a palm print, there are many wrinkles which are different from the principal lines in that they are thinner and more irregular.
- **Delta Point Features:** The delta point is defined as the center of a delta-like region in the palm print. Usually, there are delta points located in the finger-root region.
- **Minutiae Features:** A palm print is basically composed of the ridges, allowing the minutiae features to be used as another significant measurement.[19]

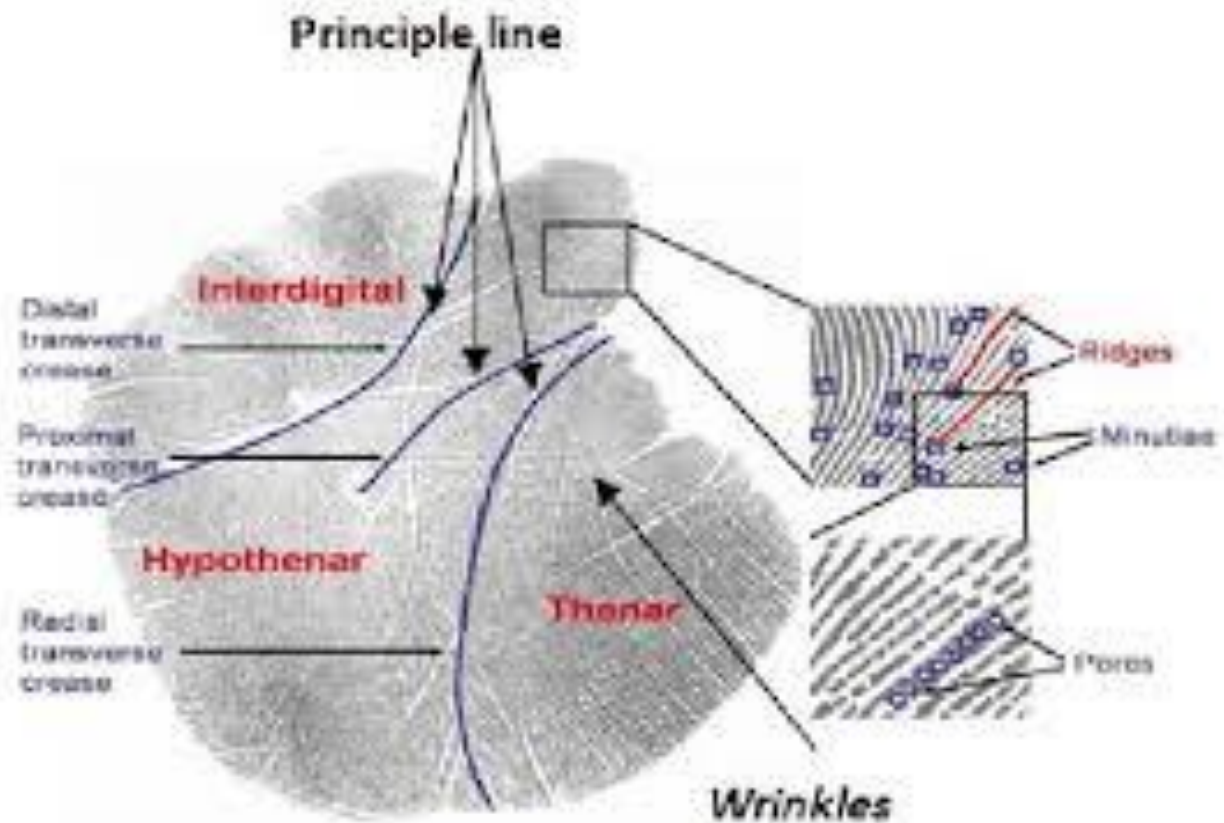


Figure 4.1 Palm print features

4.2.4 System of palm print recognition:

Palm Print Acquisition which consists of capturing the images by widely used CCD based palm print scanners, video cameras, Digital cameras and Digital Scanner.

Preprocessing is used to correct distortions, align different palm prints, and to crop the region of interest for feature extraction. Research on preprocessing commonly focuses on five steps.

Binarizing the palm images, Boundary tracking, and identification of key points, establishing a coordination system and, extracting the central part [20].

Extraction of characteristics, and pairing (matching) which compares two vectors of characteristics. The last step can be a classification which determines the identity of the individual (the classification in itself includes a set of pairings).

4.2.5 Data base of palm print:

The images of palm print that we used in our experiments come from the PolyU Database. The images in this database were collected from 50 individuals using a palm leaf image capture device designed by university researchers

Hong Kong Polytechnic Images were taken in two different time periods separated by a time interval of about two months.

During each period, each individual was required to take at least 12 palmistry photos.

In addition, in the second period, was the light source and lens of the CCD camera Adjusted to make the first and second period pictures give an impression Captured by two different palmar systems. Pictures were also taken in different lighting conditions for testing durability of the recognition system. Image size 128 x 128 resolution 75 dpi.

4.2.6 Separation of databases:

A total of 600 palm print images was collected from 50 persons (twelve handprints each). The size of fingerprint image will be 128*128 pixels and is in JPG format.

The work of implemented system is divided into two main phases. First is the enrollment phase, and second the test phase.

- a) **Enrollment phase:** The first and the third, the fifth and the seventh images of each person are used for the learning phase.
- b) **Tests phase:** The 8 remaining images of each individual were used for the realization of the different tests.

❖ Experimental Setup

- Lenovo
- Processor: Intel (R) Pentium(R) CPU laptop computer
- RAM: 2Go RAM and 2.13 GHz processor.
- OS: Microsoft Windows 7
- Matlab R2016a Development Tools

We have implemented our face recognition system in the Matlab R2016 programming environment which offers great simplicity manipulation of images.

Why use Matlab in fingerprint recognition?

Matlab is a high-level language that allows the execution of tasks requiring a great computing power and whose implementation will be very simple and fast. This language has very interesting advantages for image applications such as:

- It is easy to access and view our data on Matlab.
- Easy handling of matrices which is a strong and important point in the case of our application.
- A large choice of libraries that support all the tools mathematics.
- Useful for image processing and analysis.
- There are many algorithms for the extraction of characteristics and machine learning.
- It offers a set of reference graphical algorithms and tools for the processing, analysis, visualization and development of algorithms image processing.

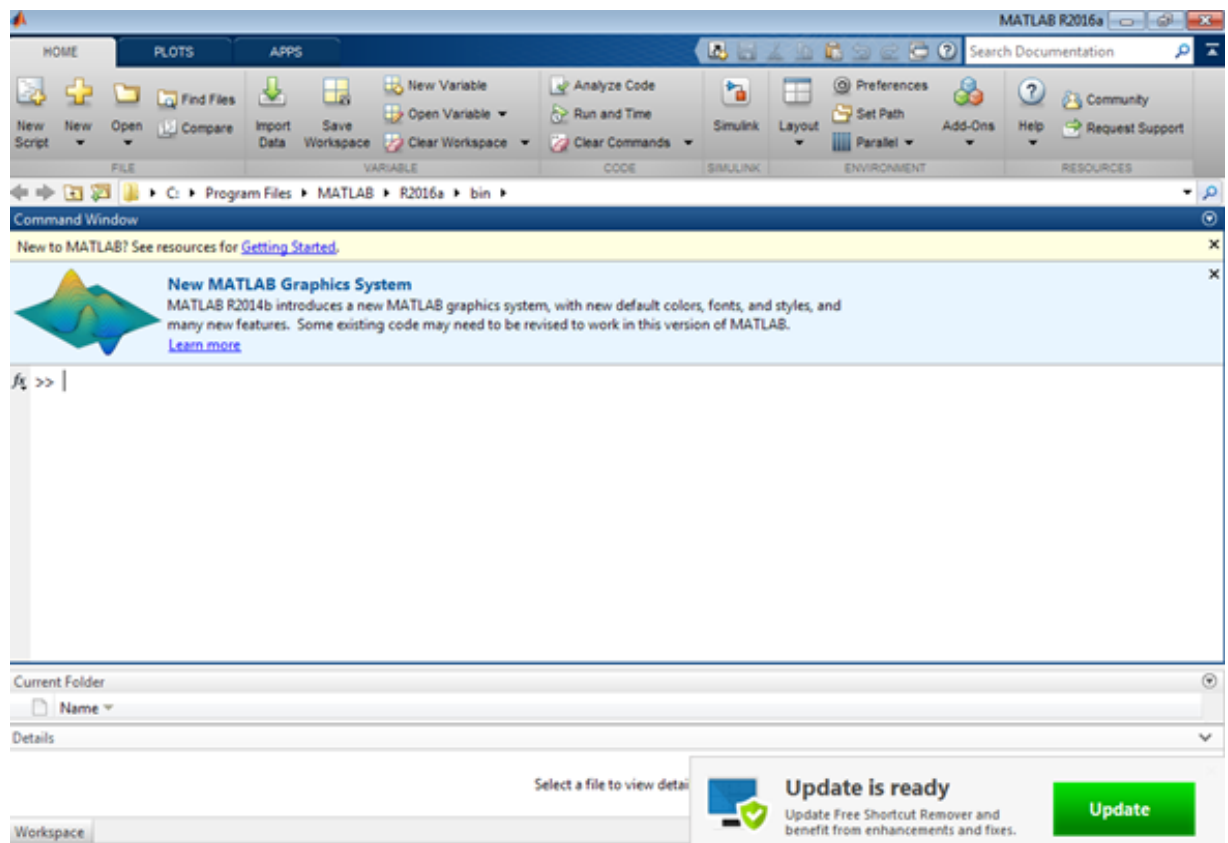


Figure 4.2 MATLAB interface

4.3 General view of blurred form:

In this biometric system, our method is presented in order to extract a fuzzy model of Palm print image. The image after processing and scanning is a matrix of dimensions $128 * 128$, its value is pixel gray levels.

The blurred model of the image is characterized by a system of two (02) inputs and one (01) output. Each input (linguistic variable) and composed of five (5) linguistic values modeled by their membership functions correspond.

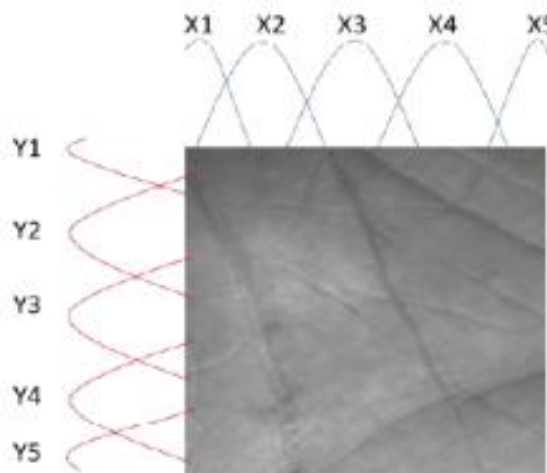


Figure 4.3 Fuzzy logic image

The inference engine of our fuzzy model is made up of 25 covering linguistic rules all the possible combinations of inputs ie (5 * 5 rules).

The output of this model is gray level this output is characterized by 25 functions membership according to the number of fuzzy rules (C1, C2, C3, C25).

I is the gray level

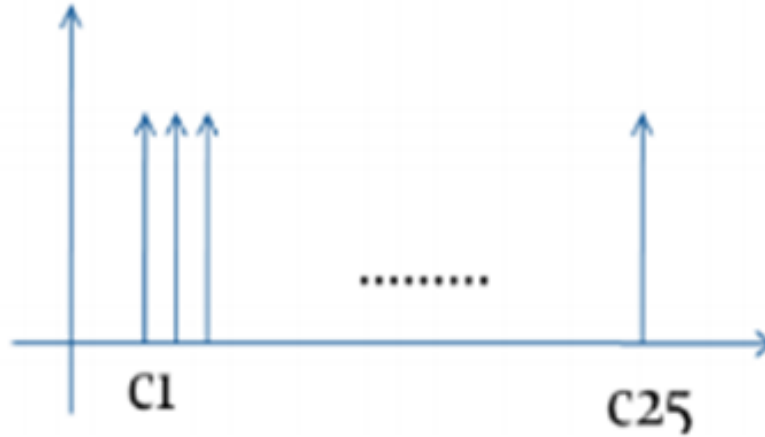
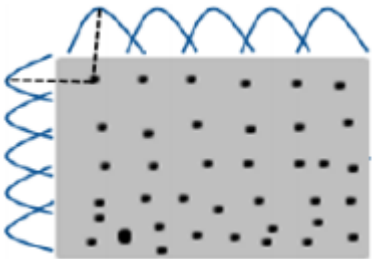
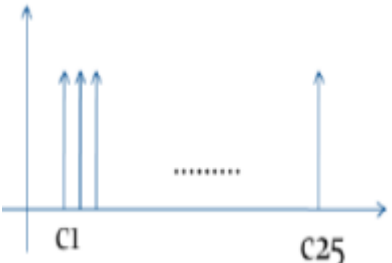


Figure 4.4 Shades of grey

The general view of our model is as follows:

fuzzification	Inference	defuzzification
 <p data-bbox="360 1608 536 1641">fuzzification</p>	<p data-bbox="699 1216 1054 1283">SI x is x1 and y is y1 so I is c1</p> <p data-bbox="699 1317 1054 1384">SI x is x1 and y is y2 so I is c2</p> <p data-bbox="699 1417 1054 1485">SI x is x2 and y is y1 so I is c6</p> <p data-bbox="699 1518 1054 1585">SI x is x2 and y is y2 so I is c7</p> <p data-bbox="699 1619 1054 1686">SI x is x5 and y is y5 so I is c25</p>	 <p data-bbox="1209 1619 1417 1653">defuzzification</p>

Experimental Result and Analysis:

Table 4.1 Results of uni_modal systems for the Threshold challenges

Thresholds	FRR (%)	FAR (%)	EER (%)	GAR (%)
0	0	0.010	0.3801	100
0.1	0	0.03	0.14	100
0.11	0	0.0204	0.05102	100
0.2	0	0.142	0.071	100
0.3	0	1.02	0.51	100
0.4	0	5.867	2.9335	100
0.5	0	19.69	9.845	100
0.6	0	45.33	22.665	100
0.7	0	73.49	36.745	100
0.8	0	90.19	45.095	100
0.9	0	96.37	48.185	100
1	0	100	50	100

The evaluation of fuzzy logic feature extraction technique on palm print modal was calculated and score matrix was generated. From the score matrix genuine and impostor score was extracted and the evaluation parameter above.

The following table shows the results of the uni-modal system for us value of Thresholds.

After the evaluation the results obtained from palm print gave **the FAR of (0.0204)** and **FRR of (0)** with the lowest **EER of (0.0510)** with the highest **GAR (100)** at the threshold values (**T0**) of **(0.11)**.

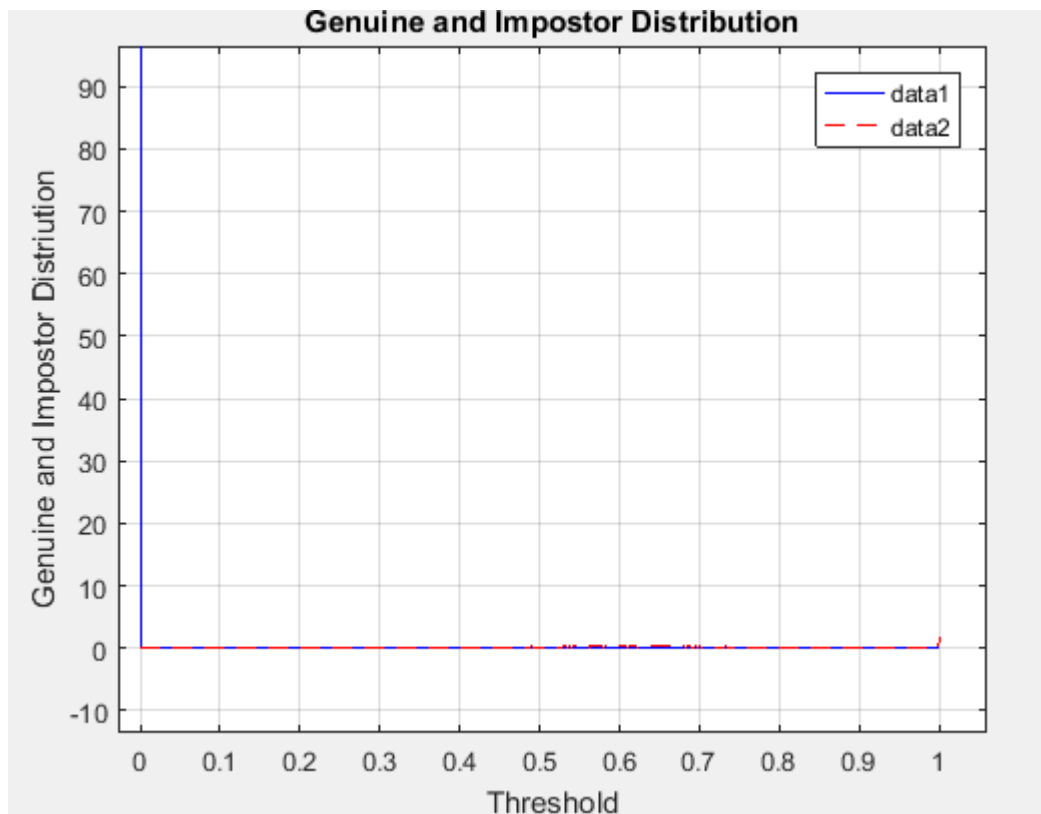


Figure 4.5 Relation genuine and impostor of threshold.

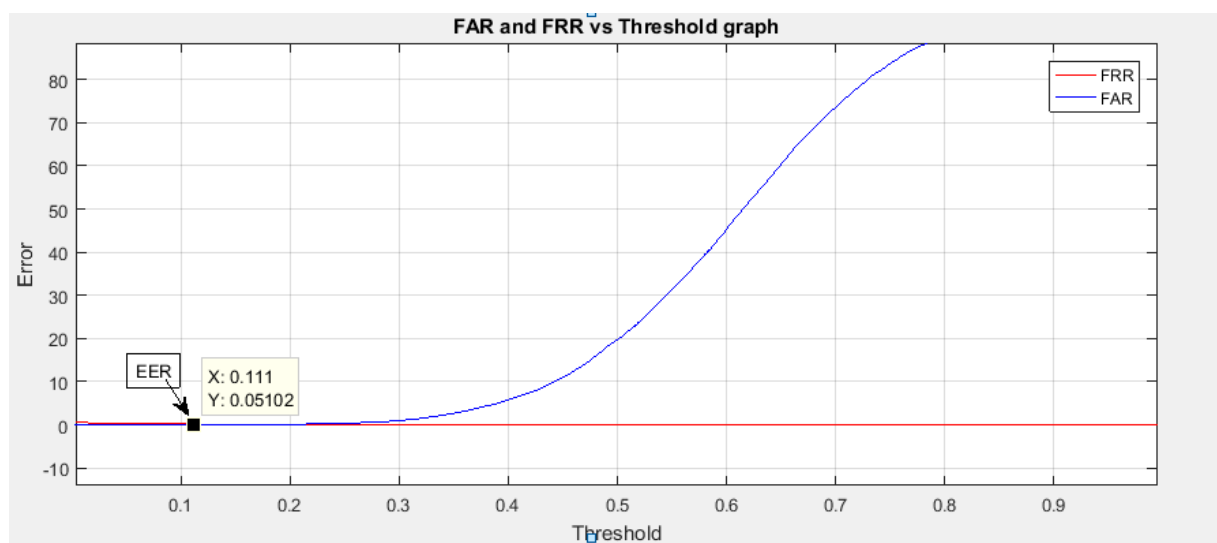


Figure 4.6 Relation FAR and FRR

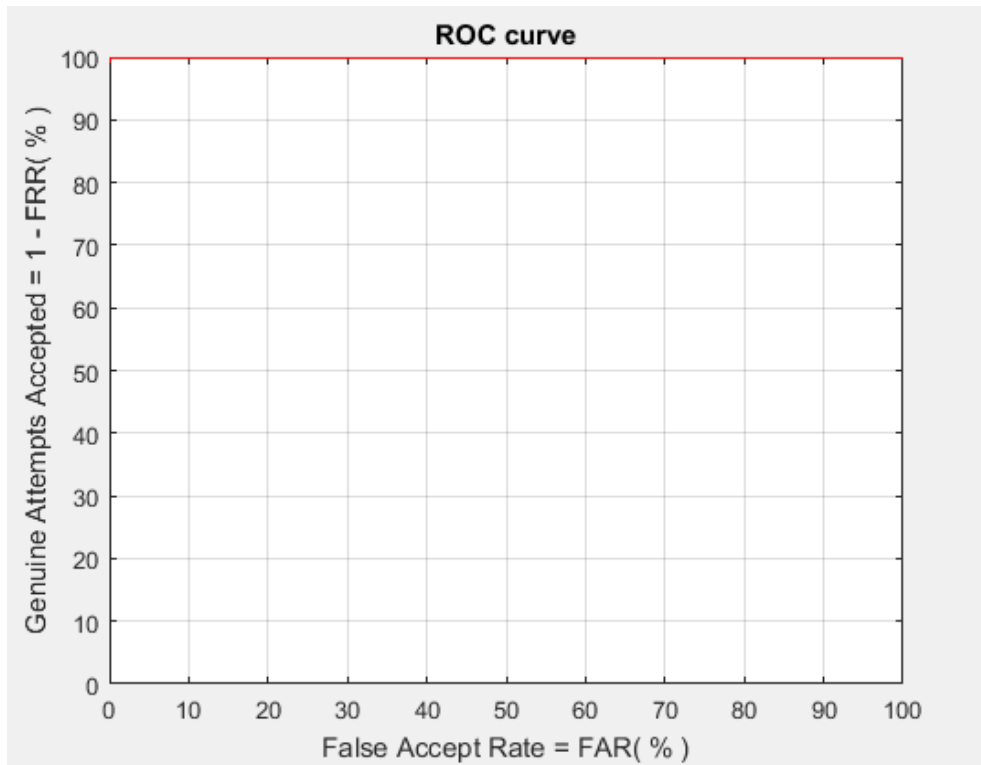


Figure 4.7 ROC Curve.

Figure (3) debit the ROC curve of performance of the system by plotting GAR against the FAR at different T.

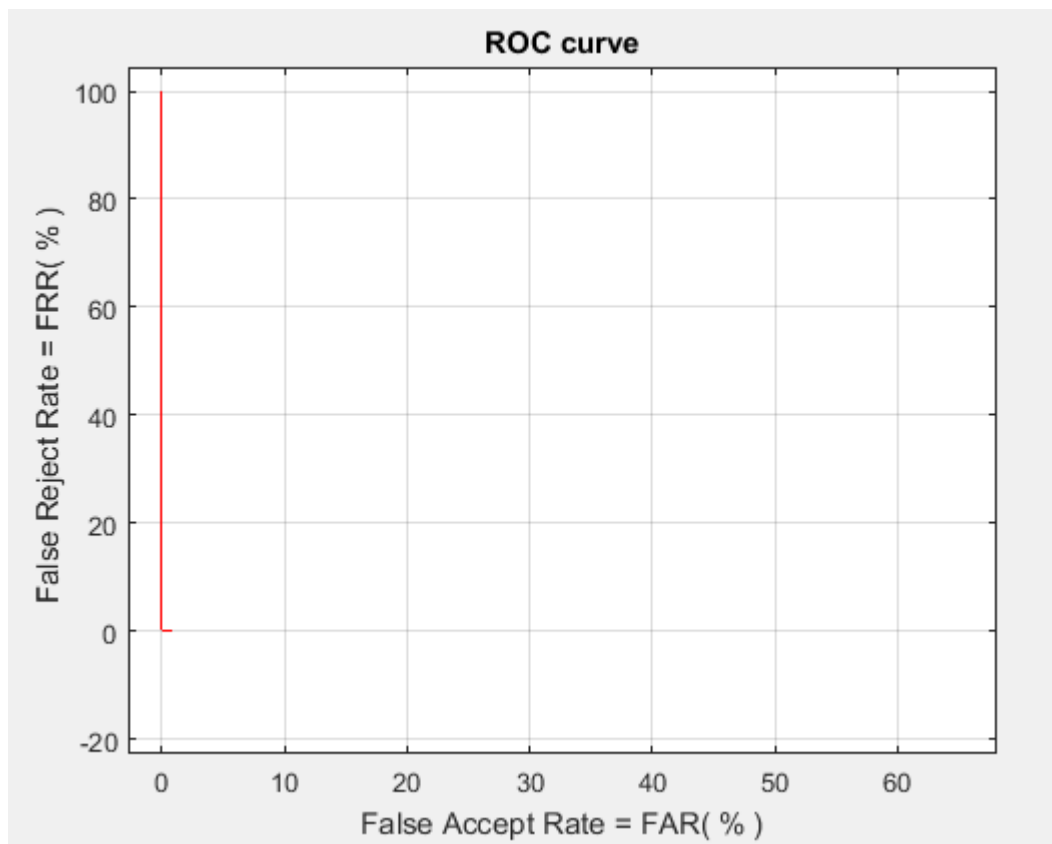


Figure 4.8 ROC Curve relation FAR and FRR.

Figure(4) represent the ROC curve of the plotting relation between FAR and FRR of the system .

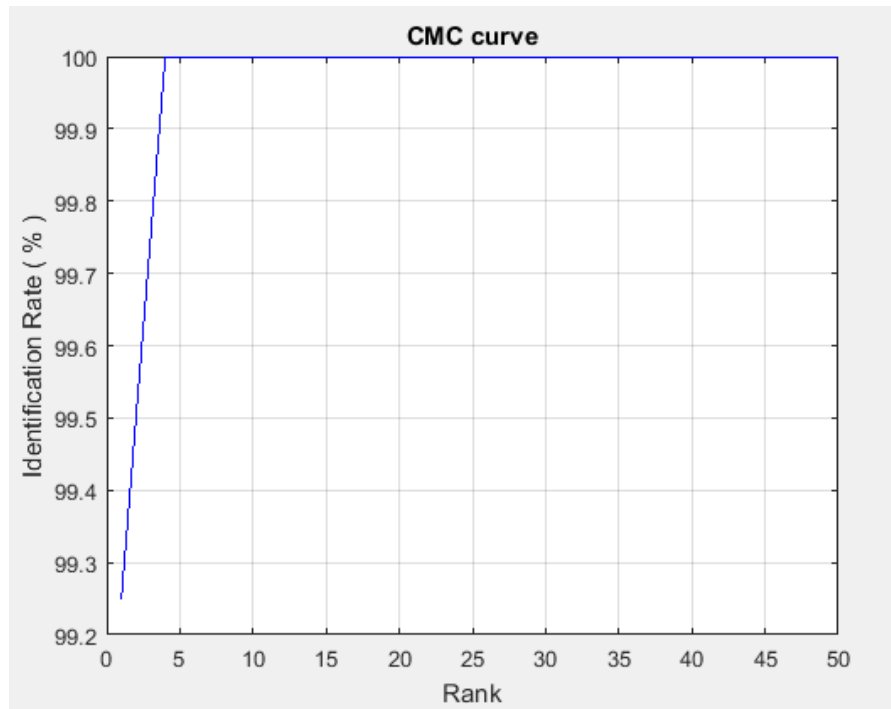


Figure 4.9 CMC Curve

The CMC curve of performance of the system by plotting relation rank values between the identification rate.

4.4 Conclusion:

The results obtained justify the effectiveness of our biometric system based on a fuzzy model related. An image of dimension $128 * 128$ is modeled at the end by a characteristic vector of dimension 25 only. The calculation time is acceptable and the results are good.

We can also say that our model is not frozen but it is adaptable by a correction gain T .

4.5 Recommendation:

Although this research has significance in getting the required information from scanned images, there are some matters that need further study to develop efficient and effective system.

- Pre-processing techniques like noise removal helps to increase the effectiveness and efficiency of the system. Introducing advanced techniques on these areas improve the performance of fingerprint image identification system.
- Using a large local data set and testing this algorithm and others as well.

- Better segmentation techniques may be considered in the future.

General Conclusion

As Bill Spence notes: “Every time you use your key, you indent to your house. Every time you use your credit card, every time you log into a system, you indent.” Ultimately, all passwords, codes, badges, keys ... etc. will be replaced by systems biometric. Biometrics research is therefore an area with very high potential.

As fingerprint recognition, verification and identification become very popular nowadays, the main intent of this research is to design fingerprint identification and verification system with scanned images from paper using image processing tools. On the work the effort is to select feature extraction and matching techniques to enhance the performance of the fingerprint identification system. On the present work an attempt is made to feature extraction and matching techniques that are crucial to enhance the performance of the fingerprint image identification system.

The reliability of any automatic fingerprint identification and verification system strongly relies on the precision obtained in the minutia extraction process. A number of factors damage the correct location of minutia. Among them, poor image quality is the one with most influence. The proposed minutiae matching algorithm is capable of finding the correspondences between minutiae without resorting to exhaustive research. However, there is a scope of further improvement in terms of efficiency and accuracy which can be achieved by improving the hardware to capture the image or by improving the image enhancement techniques.

Accurate extraction of these characteristics is an essential part for the correct identification of individuals, forcing us to work in a context of very large diversities. This diversity is also found in the considerable number of algorithms which have been proposed in the detection of characteristics of a biometric image, for example: Harris, FAST, GABOR, Canny, Robert, LBP ... etc.

In this thesis, we are interested in the problem of extraction methods characteristics of biometric images. Our job is to develop a system of fingerprint recognition based on method of extracting different characteristic

- [1] Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). Introduction to biometrics. Springer Science & Business Media.
- [2] Nanavati, S., Thieme, M., & Nanavati, R. Biometrics. Identity Verification in a Networked World. 2002.
- [3] Adesua, O. (2015). ONLINE VOTING SYSTEM WITH BIOMETRIC AUTHENTICATION FOR UI ELECTIONS.
- [4] (<https://en.ppt-online.org/590504>, s.d.)
- [5] <http://www.biometrics.gov>.
- [6] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of fingerprint recognition. Springer Science & Business Media.
- [7] Sahoo, S. K., Choubisa, T., & Prasanna, S. M. (2012). Multimodal biometric person authentication: A review. IETE Technical Review, 29(1), 54-75.
- [8] El-Abed, M., Giot, R., Hemery, B., & Rosenberger, C. (2012). Evaluation of biometric systems: A study of users' acceptance and satisfaction. International Journal of Biometrics, 4(3), 265-290.
- [9] Olaniyi, O. M., Folorunso, T. A., Aliyu, A., & Olugbenga, J. (2016). Design of secure electronic voting system using fingerprint biometrics and crypto-watermarking approach. International Journal of Information Engineering and Electronic Business, 8(5), 9.
- [10] Kumar, D. A., & Begum, T. U. S. (2012, March). Electronic voting machine A review. In International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME-2012) (pp. 41-48). IEEE.
- [11] Gritzalis, D. A. (2012). Secure electronic voting (Vol. 7). Springer Science & Business Media.
- [12] Caarls, S. (2010). E-voting Handbook: Key Steps in the Implementation of E-enabled Elections. Council of Europe.
- [13] Gentles, D., & Sankaranarayanan, S. (2012). Application of biometrics in mobile voting. International journal of Computer network and information security, 4(7), 57.
- [14] Prof. P. B. Dhamdhere, Abhishek Kasar, Nilesh Satpute, Priyanka Lekurwale. "A Secure E-voting System using Biometrics Authentication Methods for Android" 2017
- [15] Kogeda, O. P., & Mpekoa, N. (2013, June). Model for a mobile phone voting system for South Africa. In 2013 Conference.
- [16] Patil, H., Barot, H., Gawhale, K., Mhaisgawali, M. A., & Chaudhari, S. Mobile Based Voting Application.

[17] <https://www.geeksforgeeks.org/fuzzy-logic-introduction/>

[18] Gaikwad, A. T. Evaluation of Fingerprint Identification Based on Local Binary Pattern (LBP).

[19] <https://www.slideshare.net/MazinAlwaaly/pattern-recognition-palm-print-authentication-system>

[20] Krishneswari, K., & Arumugam, S. (2010). A review on palm print verification system. International Journal of Computer Information Systems and Industrial Management Applications (IJCISIM) ISSN, 2150-7988.

