PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA UNIVERSITY

FACULTY OF TECHNOLOGIES EL-OUED
DEPARTMENT OF ELECTRICAL ENGINEERING

FINAL STUDY DISSERTATION

In the aim obtaining of MASTER Degree - ACADEMIC Domain:

Option: Telecommunication Sciences and Technology

Specialty: Systems of Telecommunications

THEME

Biometric method for recognition of people

Fingerprint Recognition

Presented by:

MECHARA Mohammed

GHERNOUG Brahim

HEZLA Brahim

SEDIRA Taher

Was Publicly Debated in: June 2022 in front of The Examining Committee Composed from:

President	**Dr. AJGOU Riadh**	**MCA**	**El-Oued University**
Examiner	**Dr. GHENDIR Said**	**MCA**	**El-Oued University**
Supervisor	**Dr. TIDJANI Amina**	**MAB**	**El-Oued University**

Academic year: 2021/2022

ACKNOWLEDGMENT

We would like to express our sincere gratitude to several individuals for supporting us throughout our Graduate study First, we wish to express our sincere gratitude to our supervisor, Tidjani Amina, for her enthusiasm, patience, insightful comments, helpful information, practical advice, and unceasing ideas that have helped us tremendously at all times in our research and writing of this work.

We'd like to say thank you to all our teachers through the previous years who helped us to get to this point with their support and help.

BRAHIM GHERNOUG

To my dear parents "Djamel" and "Mabrouka" I could never thank you enough for being there for me without a doubt. Mom and Dad, you're the reason why I got here to this point, I'd like to say thank you for all the love and support you gave me and I always pray that God keeps you safe and bless you. My words can't describe how much I'm blessed to have you.

To my brothers and sisters who always provided me with the support and advice whenever I needed it, I pray to God to keep you safe and bless you.

To my grandmother's soul, you would be happy and proud of my achievement if you were with us, I always pray for God that he may grant you with his mercy.

To my uncle's soul, you'd be very proud of me God grant you with his great mercy.

To grandmother "Massaouda", my uncle, and all my aunts thank you all for your encouragement, support and for being a part of this achievement.

To my dear friend "Mohammed", it was probably impossible to do this work in such a time without your relentless efforts Thank you.

To all my friends, we are indebted to all of you for your love,
support and encouragement. We could not finish without
saying thank you for everything

MOHAMMED MECHARA

I dedicate this humble work to my dear mother

To all my brothers and sister and their families

To anyone who taught me a letter

To all my friends

BRAHIM HEZLA

To the owner of a fragrant biography and enlightened thought, for he had the first credit in attaining my higher education my beloved father, may God prolong his life.

To who set me on the path of life, and took care of me until I became young, My mother may God prolong and blessed her life

To all my family and friends

God blessed you all

Thanks for everything.

TAHER SEDIRA

To the fountain of giving that planted in my ambition and perseverance

My dear father (may God protect him)

To whom words fail to mention, to the sun that illuminated my path, to whom I will never repay no matter what I say about it.

My mother dear (God rest her soul)

To those who have in the eyes of my childhood memories and my youth and Kanu bond me

my brothers and sisters

To whom the lines were narrowed by mentioning them, my heart expanded them, my friends

To all lovers of science and knowledge

Tables of Content

Chapter II : fingerprint Acquisition

Chapter III :fingerprint Classification with Convolution Nueral Network

List of tables

Table of figures

Acronyms

DNA	Deoxyribose Nucleic Acid
PIN	Personal Identification Number
ID	Identification cards
Dpi	dots per inch
OF	Orientation field
FVC	Fingerprint Verification Competition
DL	Deep learning
NN	Neural networks
CNN	Convolution Neural Network
FP	Fingerprint
STFT	Short-time Fourier transform
AFIS	Automated fingerprint identification system
IAFIS	Integrated Automated Fingerprint Identification System
NBIS	National Bioinformatics Infrastructure
CONV	Convolutional Layer
ReLU	Rectified Linear Unit Layer
POOL	Pooling Layer
FC	Fully Connected Layer
EER	Equal Error Rate
FAR	False Accept Rate
FMR	False match rate
FNMR	False non-match rate
FRR	False Rejection Rate
API	Application Programming Interface
HQWOAP	high-quality without a perturbations
MSAFMP	middle satisfactory and a few moderate perturbations
VFWMP	various fine with moderate perturbation

Genaral introduction

God distinguished human by reason and chose him from among other creatures, so he distinguished between things and learned their names, and he was very observant. Or he saw a person zooming in on his image or voice according to what was previously known, and after what the world and Europe witnessed, especially the industrial revolution, men thought after the invention of the computer to put digital systems to distinguish between individuals.

The environmental characteristics of the human being were called vital traits after he noticed that the human being was not unique in the degrees of the mind only, and in contrast in the vital characteristics such as the color of the eyes, the tone of the voice, facial features, and the character of the fingers. He developed the first systems for distinguishing traits or traits for one finger, and it was a renaissance and a new revolution in identifying many things after tracing the traits of the fingers. The single finger of a person was not the same as the traits of the second finger. With the development of computer systems and their effectiveness, he found several ways to distinguish and extract traits with extreme accuracy and a short period of time Treat the image of the finger in several ways, even after it has been deliberately distorted or decreased. Several filters have been developed, with varying effectiveness, to improve the computer's view of the finger on the basis of the image.

And in light of the great scientific development and the entry of deep learning and machine learning into biometric systems in outputting features and adding images or fingerprints through the neural convolution technique (CNN) and the variation in processing speed and accuracy in the results.

The aim of this work is to classify, identify and name the fingerprints of a certain number of people through neural convolutions (CNN) and to extract the results of accuracy, classification, and evaluation.

In this note, we have studied the subject of biometric methods for identifying people, which is a system that allows us to identify people by physiological and behavioral characteristics. A science that uses the physical and biological characteristics of individuals to identify and identify them. We used deep learning and we used CNN.

Chapter I : We touched on the biometric system, in general and types of types and methods of their use while touching on its most famous systems. At the end of it, we touched on the material and marketing aspects of these systems in recent years.

Chapter II : We relied on explaining the fingerprint system and ways to extract its features, while touching on the types of system, its uses and advantages.

Chapter III : We created a system that works in a deep learning to classify a group of fingers and after extracting its deafness and identifying it and working to develop it for greater efficacy signs.

Key words : digital systems, vital characteristics, accuracy, deep learning, biometric systems, fingerprints, convolution neural Network .

CHAPTER I

Generalities About Biometric

1.1 Introduction:

Biometrics is an automated method for identifying a person using his biological traits or behavioral aspects or characteristics. Sample characteristics are taken from the person asking for authentication to compare the similarity to biometric references previously stored from known persons. But biometric images are affected by several variations due to data acquisition methods or due to aging, lighting, pose, etc., and thus recognition method must be adaptive to the changes in pose, expression, lighting, occlusion, aging, etc.

1.2 Biometric (theory) :

Biometrics is by all accounts well prepared to manage the above issues. It alludes to the utilization of physiological and additionally social attributes to recognize a person. Being subject to the individual himself, thebiometric recognizable proof is more solid than conventional frameworks. Biometric ID depends on what the client "is" for sure he "does". These qualities are naturally connected with the client himself and can't be disassociated from him; moving or duplicating biometric attributes to be utilized rather than somebody is well infeasible. Thus, we can dependably confirm the character asserted by the client.

Biometrics has reformed how ID is performed. It is turning into an issue of any security framework, particularly in access control, government-based and scientific applications. A few biometric characteristics are utilized in people's recognizable proof, these incorporate among others: face, iris, voice, unique finger impression, signature, hand calculation, ear, and so forth the biometrics market is turning out to be progressively boundless, it is relied upon to arrive at 30 billion dollars by 2020. The most prevailing methodology is unique finger impression. This last option establishes the point of convergence of our proposal [1].

1.3 Biometrics in computer Vision:

The biometric measurements are based either on the physiological traits such as the face, ear, fingerprint, and DNA or based on the behavioral traits including gait, voice, and signature. figure 1-1 shows an example of both types of biometrics .Fingerprints, iris, and faces are among the most popular physiological traits used successfully in commercial identification systems with fingerprints capturing over 50% of the market share [2] [3] [4] [5].

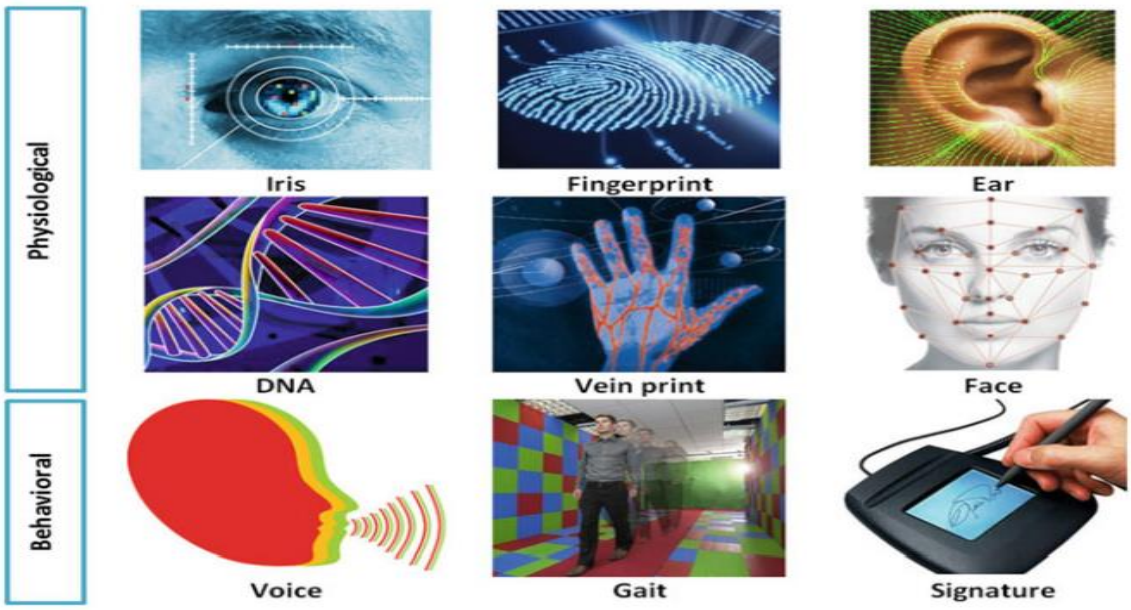

Figure 1 -1 : Various types of biometric modalities

For identification, a one-to-many matching process is conducted for newly acquired biometric data against all people already enrolled in the database to infer the identity of the subject whose matched biometric data exhibits the highest similarity value. Figure 1-2 shows an overview of a biometric system [6]

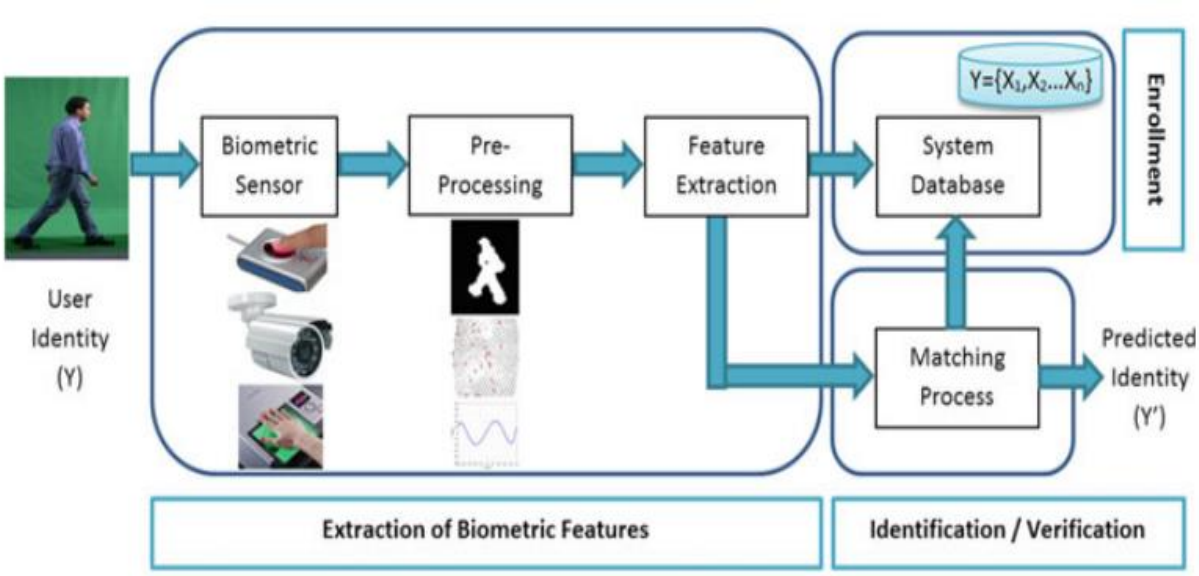

Figure 1 -2 : an overview for a biometric system

1.4 Biometric modalities and system architecture :

Diversely to the old-style recognizable proof frameworks that lay out the character of an individual in light of what he knows (privileged data like passwords) as well as what he has (ownership of items like tokens, smartcards, licenses, …); biometric frameworks depend on what the individual is (organic ascribes) and additionally how he treats (credits). These identifiers are straightforwardly connected with the individual, accordingly can't be neglected, neither replicated nor communicated. Biometric frameworks exploit an assortment of biometric attributes (or modalities) including unique finger impression, face, ear, iris, retina, palmprint, vein, voice, signature, walk, scent, … The most driving biometric modalities are recorded in Figure 1-4 [14].

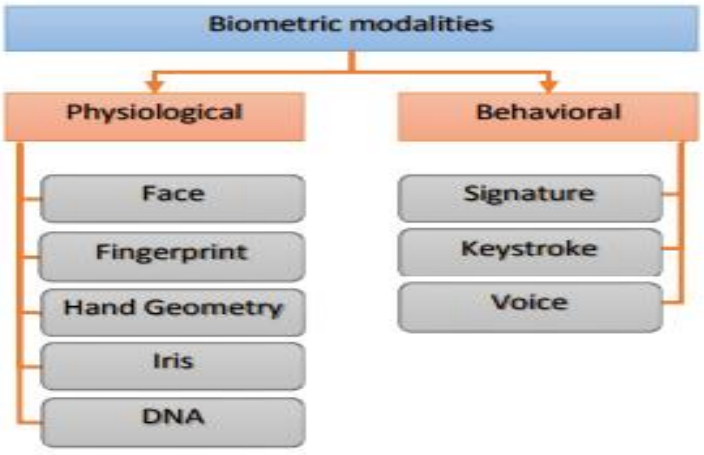

Figure 1 -3 : principal biometric modalities

1.5 Physiological

1.5.1 Fingerprint recognition:

The finger impression is the most established and the most involved biometrics quality in distinguishing proof issues on account of its wide client's agreeableness, exactness, security as well concerning its generally cheap expense. Unique finger impression abuse is going past ID and security spaces to incorporate a few explicit applications like orientation ID) and individual predecessor assurance. Robotized finger impression distinguishing proof framework is primarily a minutiae-based interaction that goes through a few stages beginning by obtaining, picture improvement, division, highlights extraction up to coordinate. Figure 1-5 shows an overview of Fingerprint [15].

Figure 1 -4 : Fingerprint image with marked ridge and valley

1.5.2 Face Recognition:

Face acknowledgment falls into the comprehensively characterized area of biometrics, which is worried about the check and acknowledgment of an individual's character by method for remarkable appearance or conduct qualities. Computerized unique mark acknowledgment, speaker and discourse acknowledgment, and iris and retina acknowledgment are largely instances of «dynamic» biometric undertakings. The unpretentious idea of face acknowledgment makes it more appropriate for a wide scope of reconnaissance and security applications. Specifically, a robotized face acknowledgment framework is fit for catching face pictures from a good way utilizing a camcorder, and the face acknowledgment calculations can handle the information caught: identify, track lastly perceive individuals looked for, like fear based oppressors or medication dealers. Figure 1-6 shows an facial recognition [16].

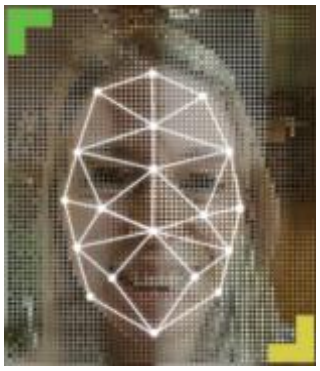

Figure 1 -5 : Facial Recognition

1.5.3 Hand Geometry :

The actual size of a hand math-based the framework is enormous, and it can't be implanted in specific gadgets like PCs. There are confirmation frameworks accessible that

depend on estimations of a couple of fingers rather than the whole hand. These gadgets are more modest than those utilized for hand calculation, yet much bigger than those utilized for acquiring specific different characteristics.. Figure 1-7 shows an hand geometry [17].

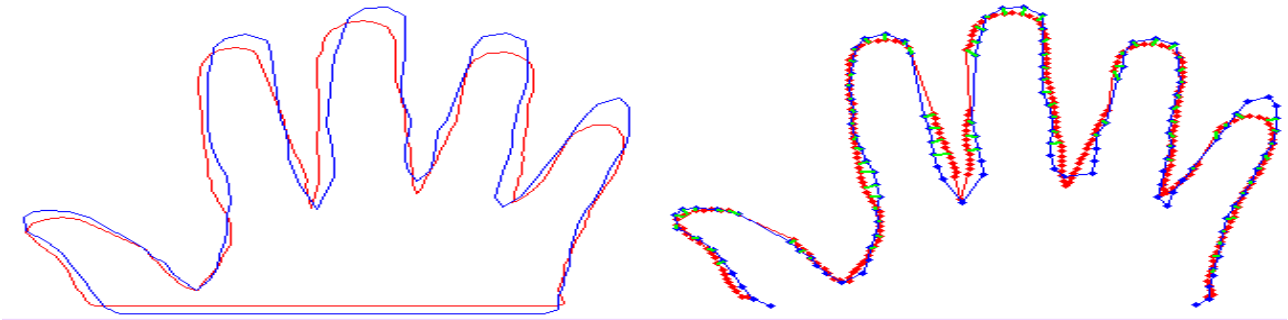

Figure 1 -6: Hand geometry

1.5.4 Iris Recognition:

The human iris is a slender round stomach, which lies between the cornea and the focal point of the natural eye. The iris can control how much light enters through the student, and this is finished by the sphincter and the dilator muscles, which change the size of the student. [18] [19].

The iris comprises a few layers, the most reduced in the epithelium layer, which contains thick pigmentation cells. The thickness of stromal pigmentation decides the shade of the iris. An external zone is called the sclera zone, and the inward one is the pupillary zone. Arrangement of the iris starts during the third month of undeveloped life [20] [21].

The main trademark that is reliant upon hereditary qualities is the pigmentation of the iris, which decides its tone. Light enters inside the eye to arrive at the retina through the understudy. The size of the iris fluctuates to change how much light enters the student. The shade of the iris can change as the sum of color in the iris increments during adolescence. The moment subtleties of the iris surface are accepted to be arbitrary, interesting, and entirely stable all through the lifetime of an individual. [22] [23].

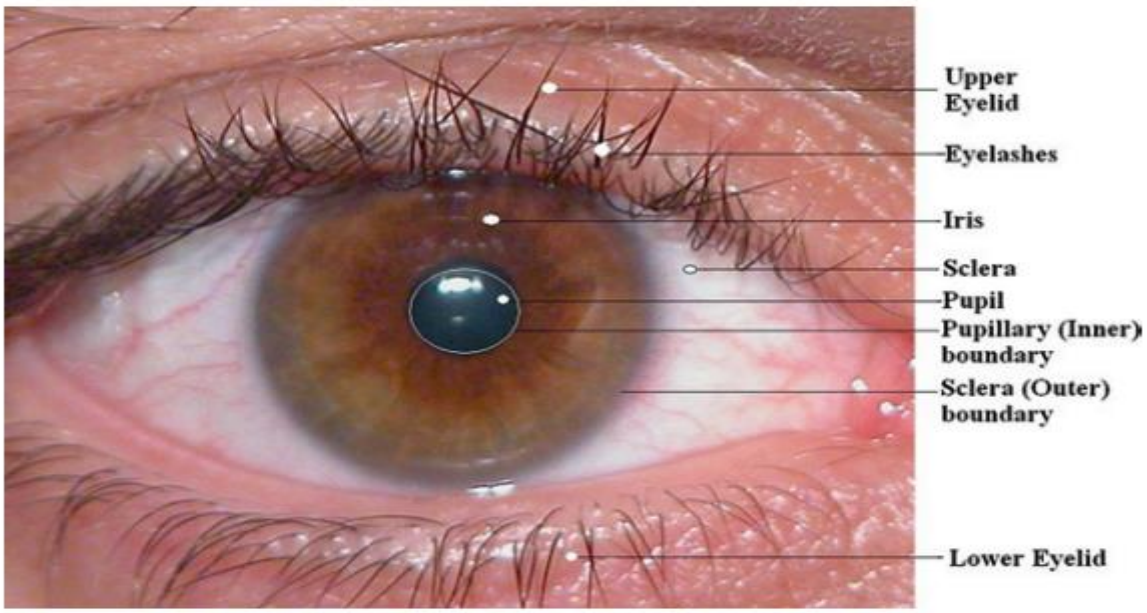

Figure 1 -7: Human eye and its parts

1.5.5 DNA:

The DNA is an acronym for deoxyribonucleic acid which is present in thenucleus of every cell in thehuman body and therefore a highly stable biometric identifier that represents physiological characteristics. The DNA structure of every human is unique, except for identical twins, and is composed of genes that determine physical characteristics [24].

1.6 Behavioral :

1.6.1 Signature :

How an individual signs her name is known to be a trait of that individual. With the multiplication of PDAs and Tablet PCs, an internet-based mark might arise as the biometric of the decision in these gadgets. Marks of certain individuals shift considerably: even progressive impressions of their mark are essentially unique. [24].

Figure 1 -8: Hand signature

1.6.2 Keystroke :

This biometric license is «consistent confirmation» of a singular's character over a meeting after the individual logs in utilizing a more grounded biometric like unique finger impression or iris. [25].

1.6.3 Voice :

A text-free voice acknowledgment framework perceives the speaker-autonomous of what she talks. A text-free framework is more challenging to plan than a text-subordinate framework however offers more assurance against misrepresentation. A weakness of voice-based acknowledgment is that discourse highlights are delicate to a few factors, for example, foundation commotion. Speaker acknowledgment is most fitting in phone-based applications however the voice signal is regularly debated in quality by the correspondence channel. [26].

1.7 Biometric system architecture:

A run of the mill biometric framework is comprised of four head modules Figure 1.10

1.7.1 Biometric sensor:

In fact, this data is a result of transforming a real continuous phenomenon (such as a face) to a digital discreet form (face image) resulting in a loss of data.

1.7.2 Enrollment:

Generally, the enrollment step allows the biometrics recognition system to learn the identities of the authentic persons in the working environment.

1.7.3 Storage system:

A compromised template can help to reconstruct the original biometric characteristics, which constitutes a real threat.

1.7.4 Matching module:

Generally, the comparison result is a degree of similarity ranging between 0 (total mismatch) and 1 (perfect match) that allows the system to take a suitable decision about the identity of the user.

In verification mode, the comparison is made only against one template in the system by conducting 1 to 1 comparison. In the identification mode, the comparison is achieved against all records in the database by conducting 1 to many comparisons. So, the system tries to answer the question «who is the user? » [27].

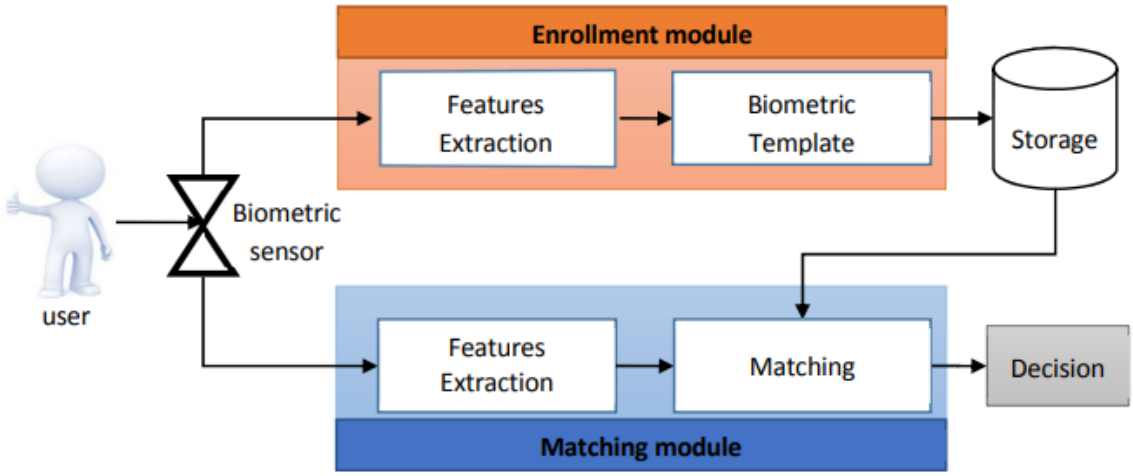

Figure 1 -9: Biometric system Architecture

A biometric system is essentially a pattern recognition system that makes a personal identification by determining the authenticity of the specific physiological or behavioral characteristic possessed by the user. A unimodal biometric system is usually more cost-efficient than a multimodal biometric system. First of all, identification using multiple biometrics is essentially a sensor fusion problem, which utilizes information from multiple sensors to increase fault-tolerance capability, reduce uncertainty, reduce noise, and overcome incompleteness of individual sensors. By using multiple biometric characteristics, the system will apply to a larger target population. System accuracy indicates how reliable and confident a biometric system is in differentiating between a genuine individual and an impostor [29].

1.8 Biometric mode (Verification and identification):

- **Authentication mode (verification):**

When a biometric system operates in authentication mode the user asserts his identity and the system checks whether this assertion is valid or not. The biometric system asks the user for their identity and tries to answer the Question is this person X?. In a verification application the user announces his identity via a password, an identification number, a user name, or any combination of the three. The system also solicits biometric information from the user, and compares the characteristic data obtained from the entered information, with the registered data corresponding to the claimed identity, this is a one-to-one (1:1) comparison). The system will or will not find a match between the two. Verification is commonly used in access control and payment authentication applications. [9] [10] Authentication by biometrics is stronger than that

using conventional means of identification such as cards, keys or passwords because it constitutes a strong and permanent link between a physical person and his identity.

- **Identification mode:**

It makes it possible to establish the identity of a person from a database, the biometric system asks and tries to answer the question, “who is person X? is a one-to-many (1: N) comparison.[11]

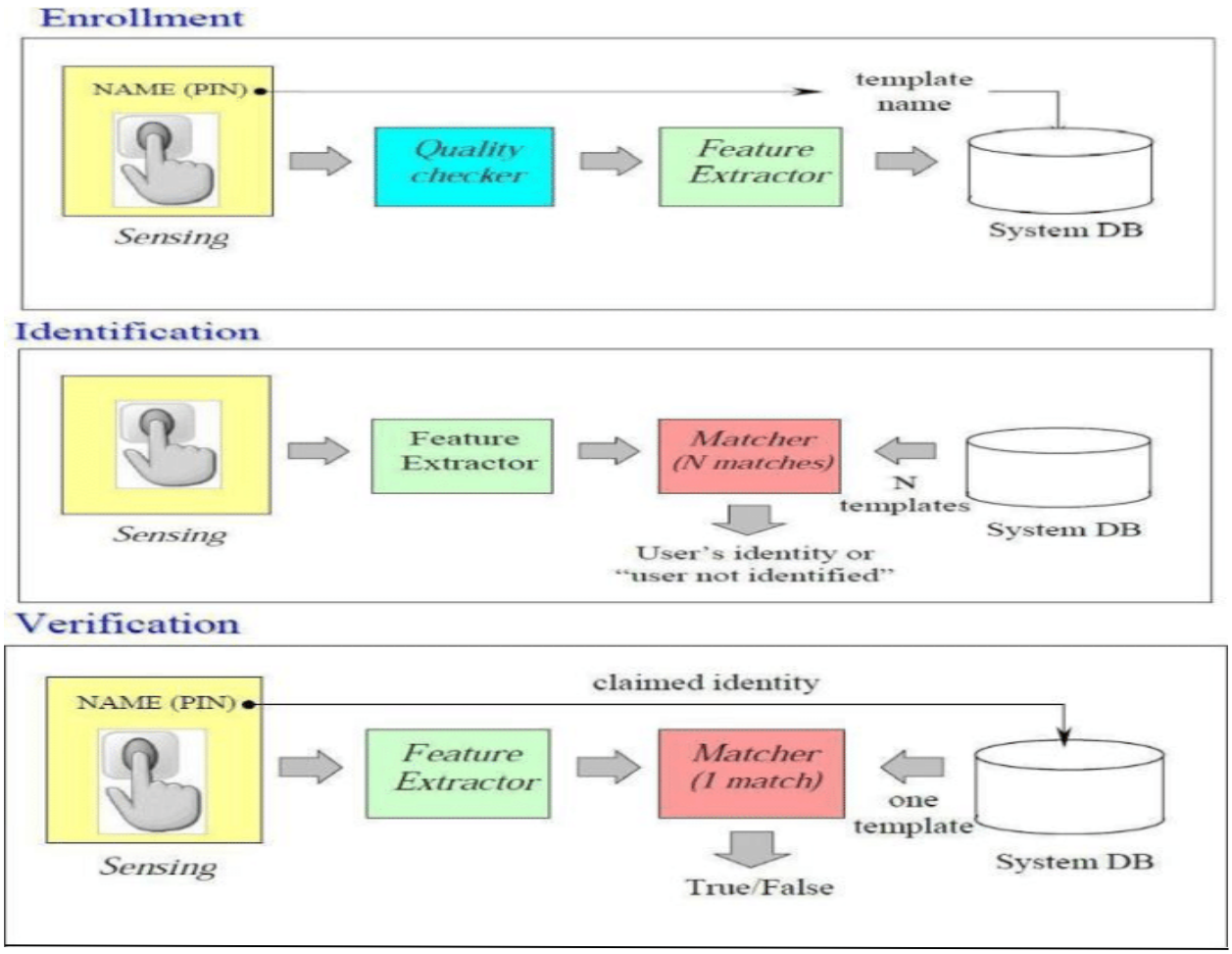

Figure 1 -10 : Process enollement identification and virification

1.9 Biometrics revolution:

1.9.1 Application :

As biometric technology matures, there will be an increased interaction among the market, technology, and applications. The emerging interaction is expected to be influenced by the added value of the technology, the sensitivities of the population, and the credibility of the service provider. It is too early to predict where, how, and which biometric technology would evolve and be mated with which applications. Applications like automating identification for more convenient travel, for transactions via e-commerce, etc. seem to be ready for commercialization, but perhaps, biometric technology could open up a whole new genre of futuristic hi-tech applications that were not foreseen before. Interesting scenarios might materialize as a number of civilian applications of identification are integrated based on single or multiple biometric technologies [30].

1.9.2 Biometrics market:

Ongoing investigations affirm that the market of biometrics would develop from 8,7 billion dollars in 2013 to almost 27,5 billion dollars by 2019 enlisting a yearly development of 19,8% somewhere in the range of 2014 and 2019. This speed increase is supported by the expansion of the electronic administrations that require distinguishing proof, alongside the ascent of misrepresentation acts and wholesale fraud that should be battled [31]. (Relativistic circle of biometrics modalities the market as shown in Figure 1-11 .

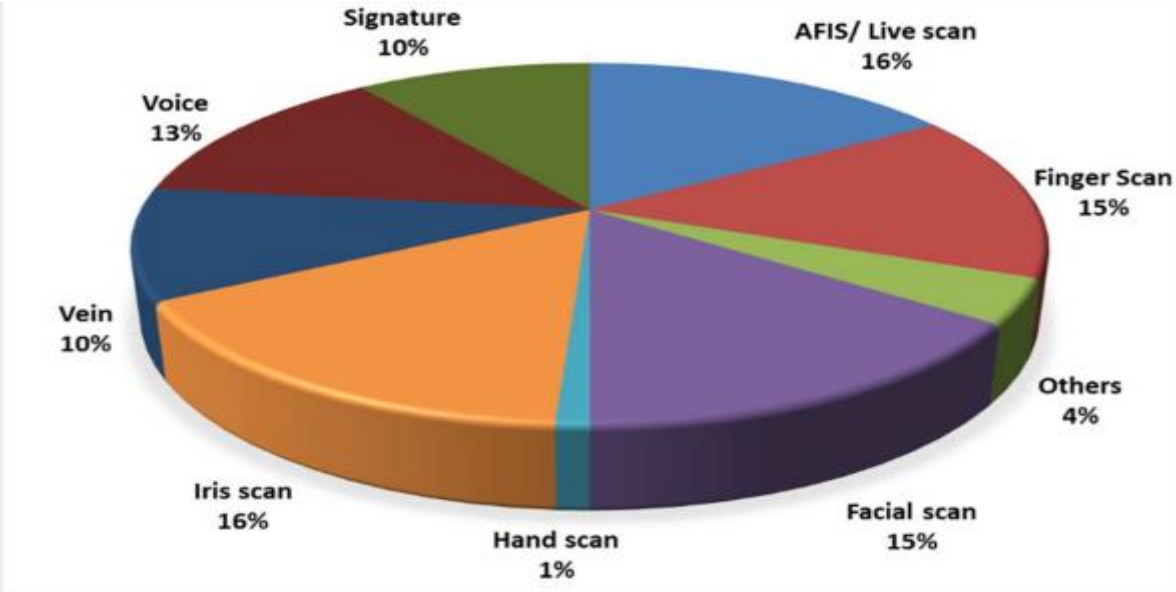

Figure 1-4: Relative circle of biometrics modalities the market

1.10 Performance evaluation :

Two classes of users are intended to be identified by the recognition system. Users who are enrolled in the system constitute the "genuine" class. They already have biometric templates stored in the database. The second class, "imposter" class, is constituted of all other users that are not genuine. The task of the system is to recognize a genuine user as being genuine and imposter as being imposter. Unfortunately, that is not always the case. In practice, several factors are havingan impact on the acquisition of the biometric characteristics in such a manner that two samples originating from the same user's biometric subject are generally not similar. These include:

2. Imperfections related to the sensor: that directly influence the quality of sensed data such as noise and resolution.
3. Acquiring environment conditions: any change in the environment conditions, such as illumination, distances or technologies, with respect to the initial acquiring conditions can lead to dissimilarities between acquired samples.
4. Interaction of the users with the sensor: the manner that the user interacts with the sensor can change from one acquisition to another. This is the case, for example, of applying more or less pressure on the fingerprint reader that affects the skin elasticity.
5. The variability observed in the biometric features set of an individual is referred to as intra-class

variation, it tends to be small; and the variability between features sets originating from two different individuals is known as inter-class variation which tends to be large. Figure 1-12 illustrates

these two types of variations in fingerprint modality. In case of large intra-class variation, the system fails to identify “genuine” persons and considers them as “imposters”, but in case of small

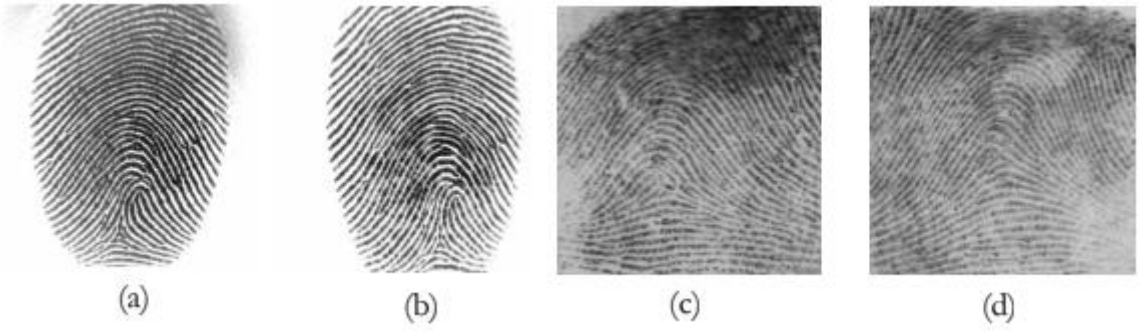

Figure 1-12 . Intra-class and inter-class variations among fingerprints. (a) and (b) two fingerprints from the same finger with low intra-class variation, (c) and (d) two fingerprints from different users with high inter-class variation

1.11 Conclusion :

Biometrics aims to imitate the mental pattern recognition process in the manner that it identifies persons. These characteristics have to fulfill some requirements in particular universality, performance and applicability. It starts by extracting some discriminant attributes from the sensed data which will be compacted to construct a template that will be stored in a database. The template is a highly representative structure that efficiently summarizes the individual biometric characteristics.

The second step, matching step, recalls the already stored template to be compared with newly extracted attributes. Upon the comparison results, the system makes a decision whether the individual is truly the enrolled identity that he is claiming or not with a certain degree of confidence ranging between 0 and 1.

the information of the fingerprint as biometric characteristics and the automatic reputation manner based totally on this modality will be mentioned in the subsequent chapter

Chapter II

Fingerprint Recognition

2.1 INTRODUCTION

Fingerprints are the most widely used biometric feature for person identification and verification in the field of biometric identification. Fingerprints possess two main types of features that are used for automatic fingerprint identification and verification: (i) Ridge and furrow structure that forms a special pattern in the central region of the fingerprint and (ii) Minutiae details associated with the local ridge and furrow structure. In a traditional biometric recognition system, the biometric template is usually stored on a central server during enrollment. The candidate biometric template captured by the biometric device is sent to the server where the processing and matching steps are performed. This paper presents an approach to speed up the matching process by classifying the fingerprint pattern into different groups at the time of enrollment, and improves fingerprint matching while matching the input template with stored template. To solve the problem, we take several aspects into consideration like classification of fingerprint, singular points. The algorithm result indicates that this approach manages to speed up the matching effectively, and therefore prove to be suitable for large database like forensic divisions.

2.2 FINGERPRINT SYSTEM DEFINITION

Fingerprint is one of the most mature biometric traits and considered legitimate proof of evidence in courts of law all over worldwide. Fingerprints are, therefore, used in forensic divisions worldwide for criminal investigations. More recently, an increasing number of civilian and commercial applications are either using or actively considering using fingerprint-based identification because of a better understanding of fingerprints as well as demonstrated matching performance than any other existing biometric technology. Modern fingerprint matching techniques were initiated in the late 16th century [1]. Henry Fauld, in 1880, first scientifically suggested the individuality and uniqueness of fingerprints. At the same time, Herschel asserted that he had practiced fingerprint identification for about 20 years [2]. This discovery established the foundation of modern fingerprint identification. In the late 19th century, Sir Francis Galton conducted an extensive study of fingerprints [2]. He introduced the minutiae features for single fingerprint classification in 1888. The discovery of uniqueness of fingerprints caused an immediate decline in the prevalent use of anthropometric methods of identification and led to the adoption of fingerprints as a more efficient method of identification.

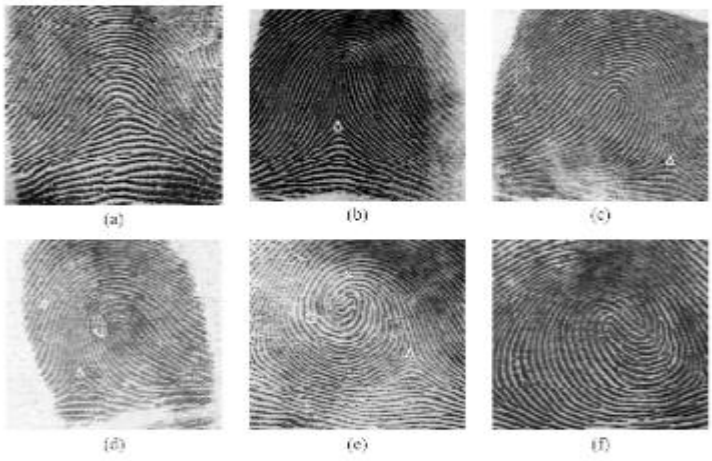

Figure 2-1 : Fingerprints classification involving six categories: (a) arch, (b) tented arch, (c) right loop, (d) left loop, (e) whorl, and (f) twin loop. Critical points in a fingerprint, called core and delta, are marked as squares and triangles. Note that an arch does not have a delta or a core

2.3 Steps of fingerprint system

The enrollment, verification, and identification processes involved in user recognition make use of the following system modules:

2.3.1 Capture:

a digital representation of biometric characteristic needs to be sensed and captured. A biometric sensor, such as a fingerprint scanner, is one of the central pieces of a biometric capture module. The captured digital representation of the biometric characteristic is often known as a sample; for example, in the case of a fingerprint system, the raw digital fingerprint image captured by the fingerprint scanner is the sample. The data capture module may also contain other components (e.g., a keyboard and screen) to capture other (non-biometric) data

2.3.2 Feature extraction : in order to facilitate matching or comparison, the raw digital representation (sample) is usually further processed by a feature extractor to generate a compact but expressive representation, called a feature set.

2.3.3 Template creation : the template creation module organizes one or more feature sets into an enrollment template that will be saved in some persistent storage. The enrollment template is sometimes also referred to as a reference.

2.3.4 Pre-selection and matching : the pre-selection (or filtering) stage is primarily used in an identification system when the number of enrolled templates is large. Its role is to reduce the effective size of the template database so that the input needs to be matched to a relatively small number of templates. The matching (or comparison) stage (also know as a matcher) takes a feature set and an enrollment template as inputs and computes the similarity between them in terms of a matching score, also known as similarity score. The matching score is compared to a system threshold to make the final decision, if the match score is higher than the threshold, the person is recognized, otherwise not.

2.3.5 Data storage: is devoted to storing templates and other demographic information about the user. Depending on the application, the template may be stored in internal or external storage devices or be recorded on a smart card issued to the individual. Using these five modules, three main processes can be performed, namely, enrollment, verification, and identification. A verification system uses the enrollment and verification processes while an identification system uses the enrollment and identification proce processes are:

2.3.6 Enrollment : user enrollment is a process that is responsible for registering individuals in the biometric system storage. During the enrollment process, the biometric characteristic of a subject is first captured by a biometric scanner to produce a sample. A quality check is often performed to ensure that the acquired sample can be reliably processed by successive stages. A feature extraction module is then used to produce a feature set. The template creation module uses the feature set to produce an enrollment template. Some systems collect multiple samples of a user and then either select the best image (or feature set) or fuse multiple images (or feature sets) to create a compos

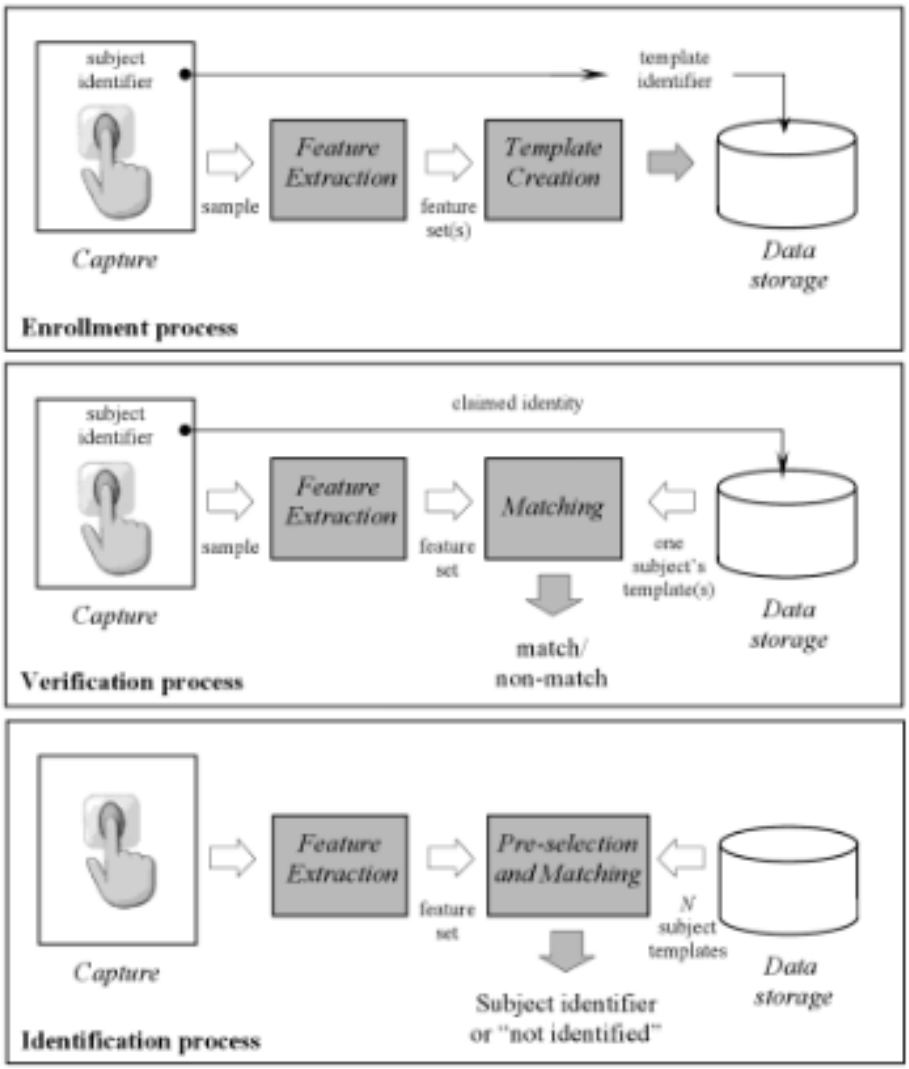

Figure 2-2. Enrollment, verification, and identification processes. These processes use the following modules: capture, feature extraction, template creation, matching, pre-selection, and data storage. In the identification process pre-selection and matching are often combined.

2 .4 Fingerprint Feature Extraction

The human fingerprint is comprised of various types of ridge patterns, traditionally classifid according to the decades-old Henry system: left loop, right loop, arch, whorl, and tented arch.

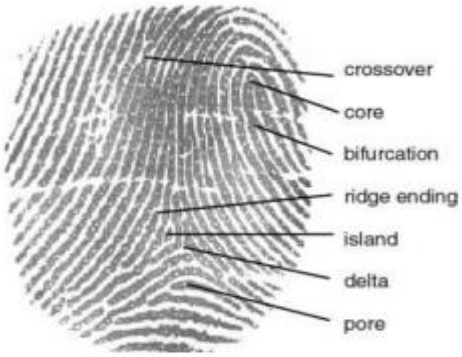

Figure 2-3: Minutiae- points on a fingerprint

Loops make up nearly 2/3 of all fingerprints, whorls are nearly 1/3, and perhaps 5-10% are arches [3]. These classifications are relevant in many large-scale forensic applications, but are rarely used in biometric authentication. Many types of minutiae exist, including dots (very small ridges), islands (ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges), ponds or lakes (empty spaces between two temporarily divergent ridges), spurs (a notch protruding from a ridge), bridges (small ridges joining two longer adjacent ridges), and crossovers (two ridges which cross each other) [4].

2.5 Fingerprint-Matching Process

Fingerprint matching techniques can be placed into two categories: minutiae-based and correlation based. But the commonly used technique with minimum FAR and FRR is Minutiae-based techniques. In this process we, first find minutiae points and then map their relative placement on the finger. However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method does not take into account the global pattern of ridges and furrows [5]. Fingerprint Verification System is a system that determines the correspondence of an input fingerprint with a template fingerprint stored in data base. A typical block diagram of biometric matching systems .

2.6 Automatic Fingerprint Verification system

In a verification fingerprint system, the template fingerprint image is obtained in the enrollment phase. After that verification process takes place by a inputting the sample of the user's fingerprint at sensor. Such input fingerprint must be processed, in the preprocessing step. The preprocessing includes image enhancement, gray level adjust, ridge thinning, etc. After the fingerprint image has been preprocessed, the feature extraction block extracts the relevant information that will be used for matching with the template fingerprint [6]. Finally a verification decision is made with the results or percentages of similarity obtained from the matching step. Section 2 describes the work in this field and the problems associated with this field. Section 3 describes the proposed work and the efficiency of proposed work based on experimental calculations.

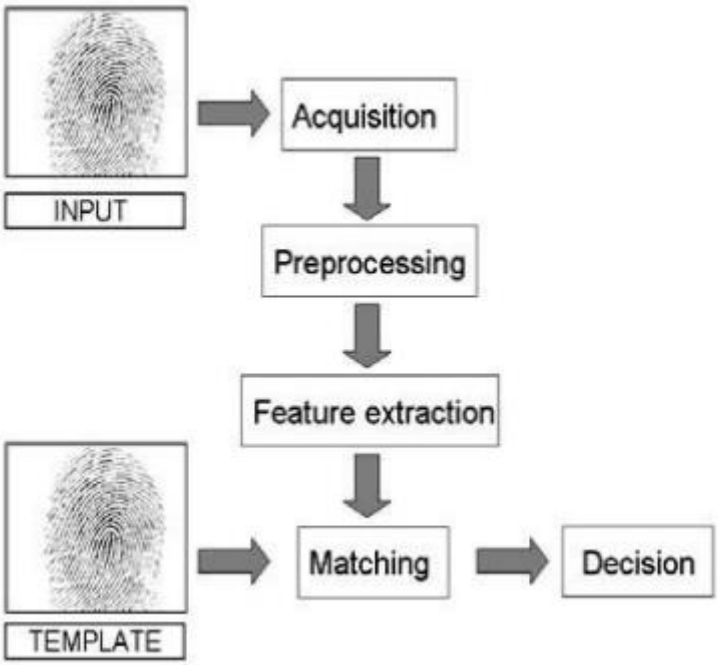

Figure 2-4: Block diagram of a typical Automatic Fingerprint Verification system

2.7 Automated fingerprint identification system (AFIS)

The manual system established for searching and verifying fingerprints was requiring more and more human resources as well as an extended time to answer one request. As a result, the first automated fingerprint identification system prototype was installed in 1972 that was fully operational in 1983. Since then, many improvements have been brought to the system at both the hardware and the software levels [11].

2.7.1Definition:

An automated fingerprint identification system is a computerized technology that allows the collection, processing, and storing of an individual's fingerprint features to decide his identity. The system comprises hardware and software subsystems [2].

2.7.2 Recognition process:

The goal of an AFIS is to establish the identity of an individual based on his fingerprint. The recognition process starts by acquiring the fingerprint of the individual's finger, using an electronic reader, as a bitmap image where darker areas depict the ridges and brighter ones indicate valleys. These features are compacted in a summarized form into the so-called 'descriptor' or 'template'. The comparison result is a similarity score, ranging between 0 and 1, that quantifies to what extent the input fingerprint represents the claimed identity found by the system..

2.7.3 Image acquisition:

1- Offline acquisition: The fingerprint is acquired not directly from the individual's finger, instead, it is digitized from a medium on which the fingerprint is recorded. This is the case of an inked fingerprint that is initially rolled on paper using ink. The paper is then acquired using an ordinary paper scanner to produce the digitized image. In crime

scenes, the fingerprint is found left on some objects, due to the sweat and grease characteristics of the finger (Figure 2-6 (e) and (f) show inked and latent fingerprints) [2].

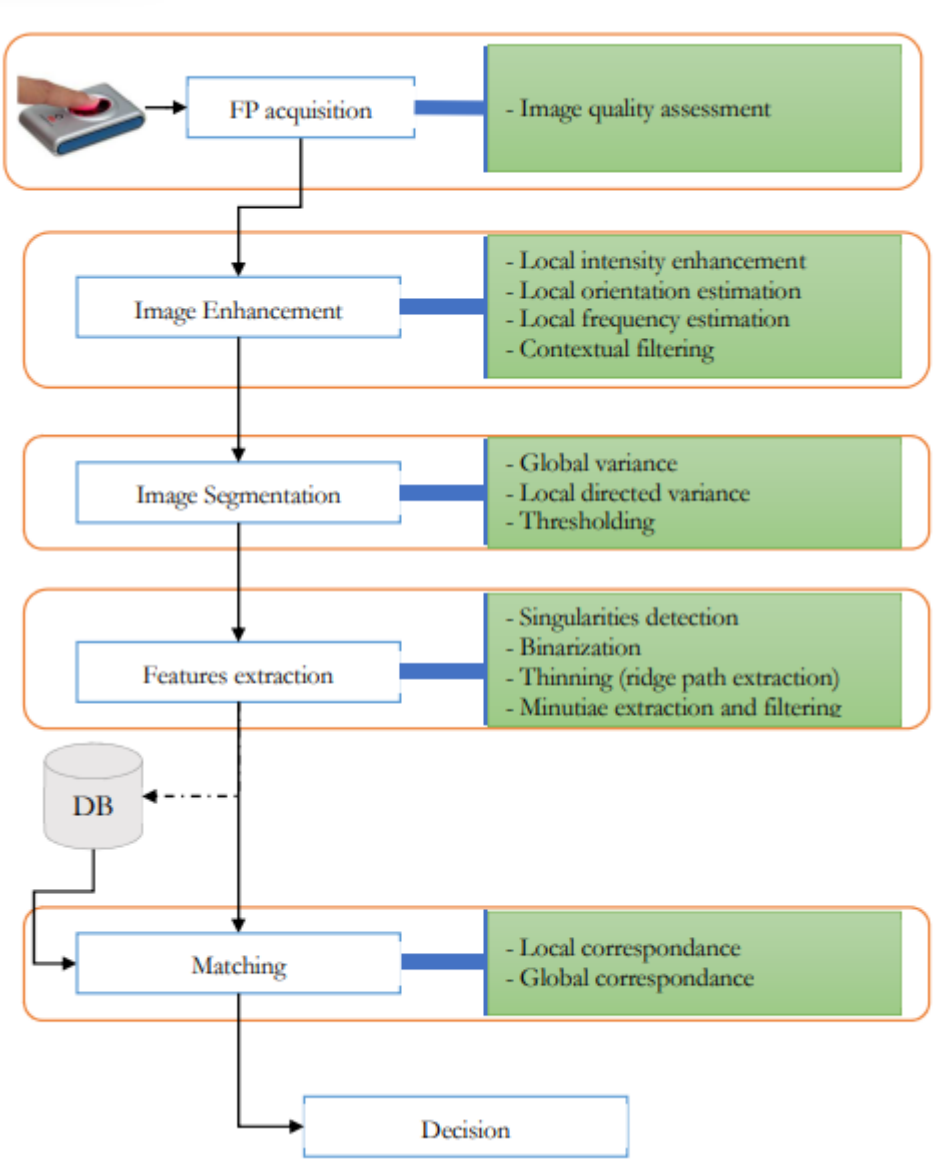

Figure 2- 5: General process of features based fingerprint recognition

2- Online acquisition: The fingerprint is acquired directly from the subject's finger. This is achieved using an electronic fingerprint device. Nowadays, there are several live-scan fingerprint technologies available that can be either optical readers, solid-state readers, or ultrasound readers. Some fingerprint images are acquired from different readers (Figure 2-6) [2].

2.7.4 Image quality assessment:

The performance of the recognition system depends on the quality of the sensed image. When acquiring an image, several factors are hurting the quality of the image. These imperfections can be related to:

1. Reader's technology: Resolution is the most important characteristic of the reader. Most AFISs work on image resolution of 500dpi. A higher resolution, 1000 dpi, is needed in some applications. As shown in (Figure 2-6) [2].

2. State of the skin: the surface of the fingertip may be suffering from the character of the issue's occupation (managing acids, farmers, construction, etc.) as well as through growing old (older human beings tend to have bad ridge structure than younger) [2].
3. Environmental conditions: A dry fingertip results in a low-quality fingerprint image with an interrupted ridge structure, whereas a wet fingertip results in a saturated fingerprint with thicker linked ridges [12].
4. Interoperability of the user: High-pressure results in high skin distortions whereas small contact of the skin with the glass surface results in a partial fingerprint [2].

These types of elements may additionally lead the subsequent steps to address faulty capabilities such as false ridge structures that later carry out spurious trivialities.

It is said that more or less 10% of fingerprints manipulated can be categorized as 'poor' images. Generally, a fingerprint image vicinity can be divided into four areas [13].

1. Background region: that corresponds to the floor of the scanner that isn't always blanketed by using the finger. this region doesn't include any ridge shape.
2. Clear region: ridges in such areas are well defined and pretty distinguishable. each ridge is well separated using two valleys and vice versa.
3. Recoverable region: ridges are noised with smudges, creases, and small links but their common structure continues to be visible.
4. Unrecoverable region: the ridge shape is rather suffering from noises and it isn't seen. ridges are related collectively constituting smudged areas.

(Figure .27) shows two fingerprint images with labeled quality regions. these areas can be robotically categorized in keeping with the neighborhood assessment, orientation, and frequency consistencies. these elements joined with others, can define a first-rate index associated with a fingerprint image [11].

Another task of the enhancement algorithms is to mark the unrecoverable regions as being of low quality that must be taken into consideration in the subsequent steps. Once these algorithms are adapted to the nature of the imperfections listed above, optimal matching performances are soon obtained.

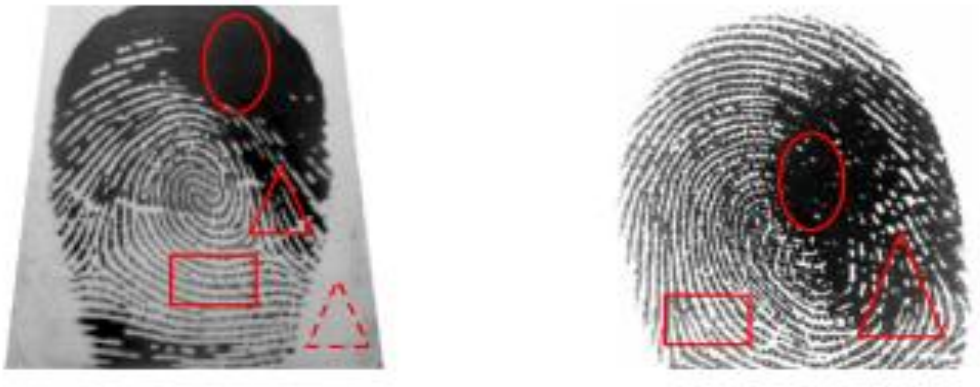

Figure 2-6: Fingerprint images with marked quality regions

2.7.5 Fingerprint image enhancement algorithms:

They range from the simplest pixel-wise operations to complicated contextual filtering. Pixel-wise enhancement schemes are generally inherited from the fundamental image processing concepts, such as normalization, histogram equalization, mean and variance normalization, and Wiener filtering. These operations affect only the pixel itself and don't alter

the ridge structure. In general, contextual filters are dealing with context formed by local pixel orientation and frequency [14].

1) Fingerprint segmentation:

As with all image processing applications, segmentation is a mandatory problem that must be rigorously resolved. Fingerprint segmentation refers to the process of decomposing a fingerprint image into two disjoint regions: foreground and background. The foreground consists of the useful ridge structure that constitutes the region of interest whereas the background represents the region of the reader screen that was not covered by the finger during the acquisition, extended with the unrecoverable regions in which the ridge structure is ill-defined. accept any further thinning process.

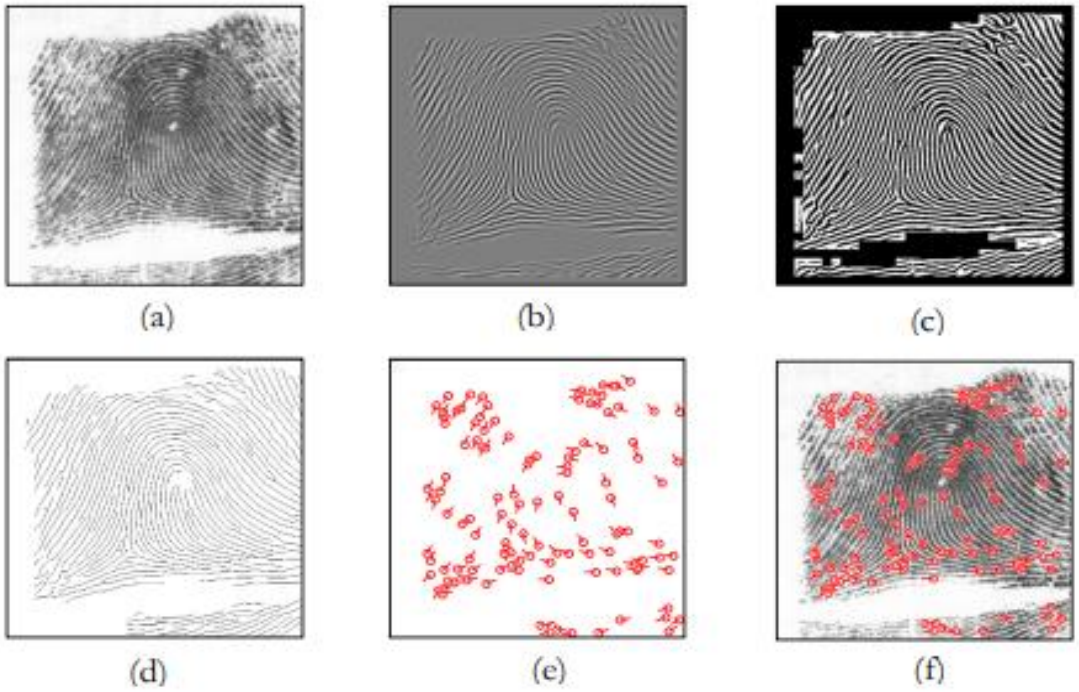

Figure 2- 7 : Results of processing a fingerprint image

2.7.6 Minutiae extraction and filtering:

As soon as the thinned photograph is calculated, the trivia extraction method is confined to a simple experiment of the thinned image to affirm the crossing quantity related to every ridge pixel (black pixel). the crossing quantity related to a pixel P(i,j), stated CN(P), is defined as being the range of black neighbor pixels. an ending minutia is described as a pixel having CN = 1, while a bifurcation minutia is described to have a CN of 3. a fingerprint photograph with its related minutiae is shown in Figure 2-10(e and f).

The vicinity of the underlying pixel defines the 2nd coordinates of the minutia. the minutia path θ is defined because of the angle that the ridge related to the minutia makes with the horizontal axis. it can be sincerely deduced from the ridge OF price at that pixel, or calculated

2.8 Performance evaluation:

Most of them are used in principal fingerprint competitions such as FVC competitions based on which fingerprint verification algorithms are ranked. As for fingerprint benchmarks, many public fingerprint databases can be used to assess the performance of a fingerprint identification system.

2.9 Conclusion

Fingerprint recognition was first automated in the early 1970s. Because of its acceptability, maturity, and low cost, the fingerprint is and will continue to be the most widely utilized method of individual identification. The ridge path's local characteristics are referred to as Level 2. The most crucial qualities based on which individuals can be identified are special discontinuities in the ridge path called minutiae.

The second local trait that ensures individuality is the ridge path itself. A fingerprint identification system is primarily a detail-oriented procedure that includes processes such as acquisition, enhancement, segmentation, feature extraction, and matching.

Chapter III

Fingerprint Classification with CNN

3.1 Introduction:

Fingerprint recognition is a common real-world task in applications such as lawenforcement, forensics, and biometric identification. In the current chapter we will touch
Through our previous theoretical work, Through our previous theoretical work, we touched on the types of feature extractions for fingerprints. In the current chapter we will address how to acquire the data package and process it in modern ways and extract its features. And we'll work on how to learn deep from matching and recognize fingerprints. we touched on the types of feature extractions for fingerprints.

3.2 Data processing:

3.2.1 Data Base Selection:

Ultimately, FVC2000 (DB1_B) (the dataset from www.kaggle.com)was chosen because the image quality is acceptable, there are class labels for each fingerprint, there are 80 samples, it is freely available, and many existing approaches also use it. Modern fingerprint scanning devices vary greatly inquality, and though image quality may not be perfect, ink smudging is no longer a problem.

Many of the existing approaches to fingerprint classification use the orientation field or singular points as features for classification. However, instead of using orientation angles to generate an orientation field, the angles themselves are normalized and stored as images, referred to in this work as «orientation angle images», where represents the width or height of the image divided by the local window size N . This distinction is necessary because the CNN operates on normalized pixel representations of orientation angles instead of a set of vectorized orientations, such as those used other methods.

3.3 Performance of system :

For you to look at and compare the performance of biometric technologies, there are some key measures identified under which are generally used to check such structures .

- False Meduim Rate (FMR): The FAR is also known as «Type I error». As almost all biometric systems aim to attain correct identity authentication, this number should be as low as possible .
- False No Medium Rate (FNMR): The FRR is also known as «Type II error». In order to minimize inconveniences or embarrassment to the genuine user, this number should also be low as possible.
- Equal Error Rate (EER): FAR and FRR are related. A stringent requirement for FAR (as low as possible) will inadvertently increase the FRR. The point where the FRR is equal to FAR is given by this measure. Lowering the rate of EER will increase the performance of the system as it indicates a good balance in the sensitivity of the system. shown in figure 3-1 .

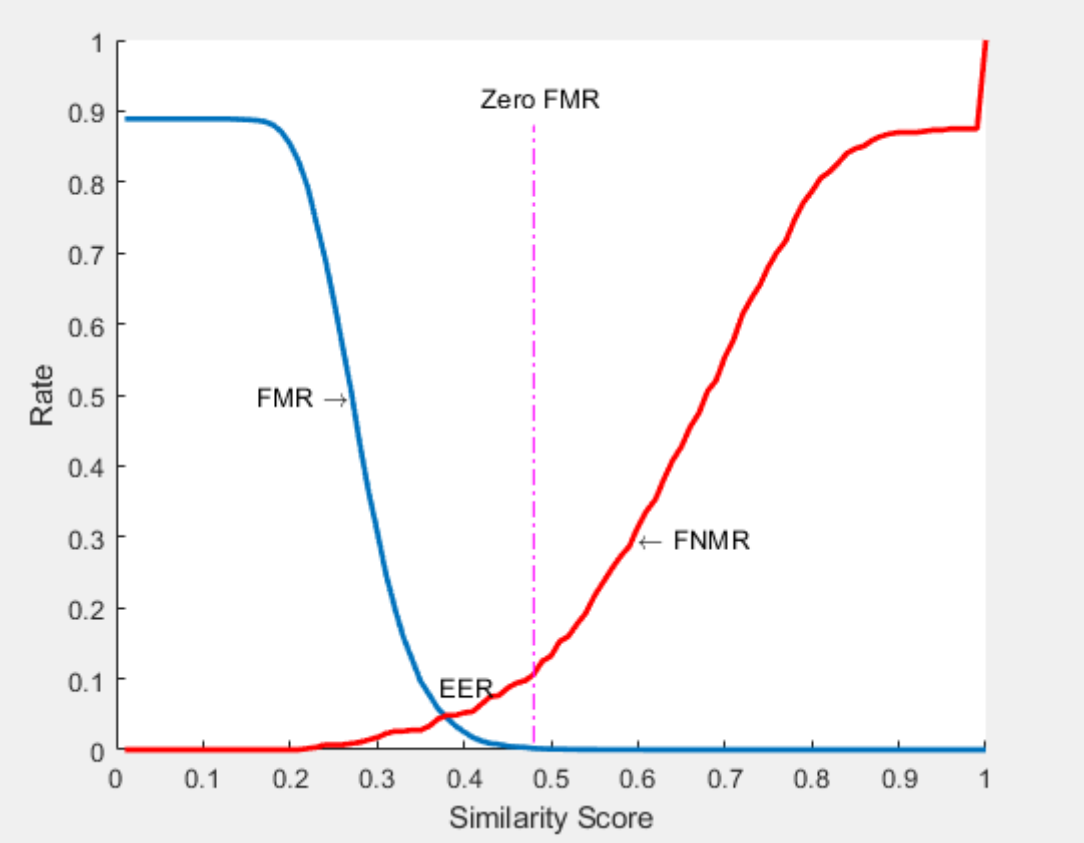

Figure 3- 1 : Perfermance of the system

3.4 Data augmentation and Normalization:

To facilitate network training, the mean fee of every pixel over the whole populace became calculated and subtracted from that pixel (characteristic-wise centering) and every pixel turned into divided by using the same old deviation of the corresponding pixels over the entire population (characteristic-wise normalization).

Facts augmentation became used to generate additional photographs from the present set of schooling samples. facts augmentation is an effective method that makes the nice viable use of every training sample by using acting minute adjustments to the photograph, effectively growing new schooling photographs. the augmentation parameters used in this case include random rotations in the variety [-15 degrees, 15 degrees], vertical and horizontal translations expressed as a fraction of the width and height of the picture within the variety [-0.2, 0.2], shearing expressed in radians within the variety [-0.2, 0.2], and zooming (expansion or discount) in the range of [0.8, 1.2]. the photo was now not flipped vertically or horizontally this could by chance confuse the model as to which elegance the photograph belongs. 80 augmented snapshots were created for each education sample in actual time throughout schooling.

3.5 CNN model architechture (Convolutional neural networks):

The secret to the success of any neural architecture lies in tailoring the structure of the network with a semantic,understanding of the domain at hand. Convolutional neural networks are heavily based on this principle, because they use sparse connections with a high-level of parameter-sharing in a domain sensitive way. In general, the success of the convolutional neural network has important lessons for other data domains.

A significant level of domain-aware regularization is also available in recurrent neural networks, which share the parameters from different temporal periods. Even though artificial neural networks are only caricatures of the true complexity of the biological brain, one should not underestimate the intuition that one can obtain by studying the basic principles of neuroscience [1].

Convolutional Neural Networks (CNN) have proven to be very effective at image classification tasks including classic problems such as FVC2000 (DB1_B) handwritten digit recognition, as providing country-of-the artwork solutions to real global troubles such as facial popularity, pose estimation [16], motion synthesis, colorization of gray-scale images, and lots of others. the primary cnn structure upon which this work is modeled. dialogue of the operational of CNN will be limited in this work as they're well described in many different guides , shown in figure 3-2 .

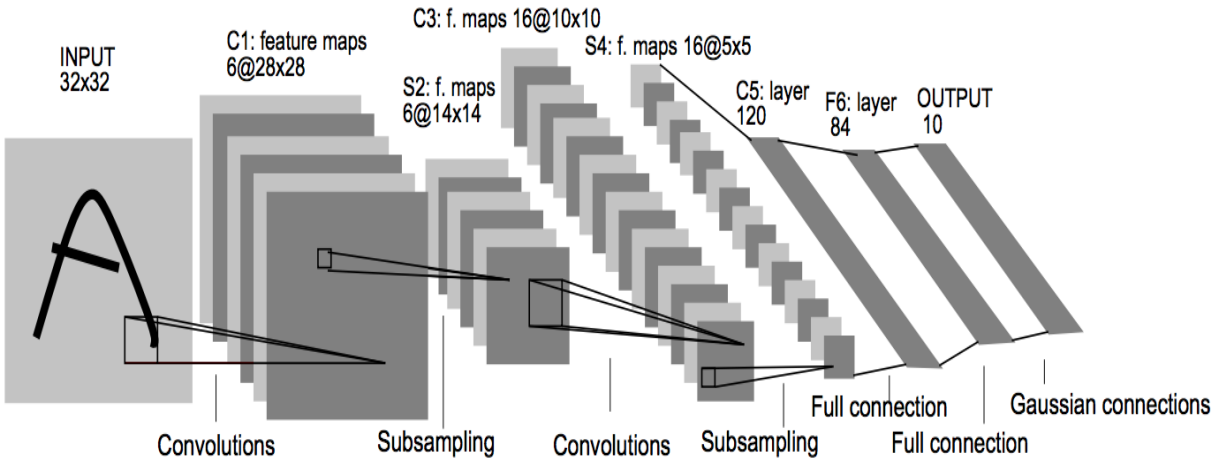

Figure 3- 2 : Architecture of Lenet-5

In case of classification fingerprints we show this stracture in figure 3-3

Figure 3-3 : Stracture of fingerprints classification with CNN model

As we see below, one of the major ways of feature extraction which is orientation field figure 3-4.

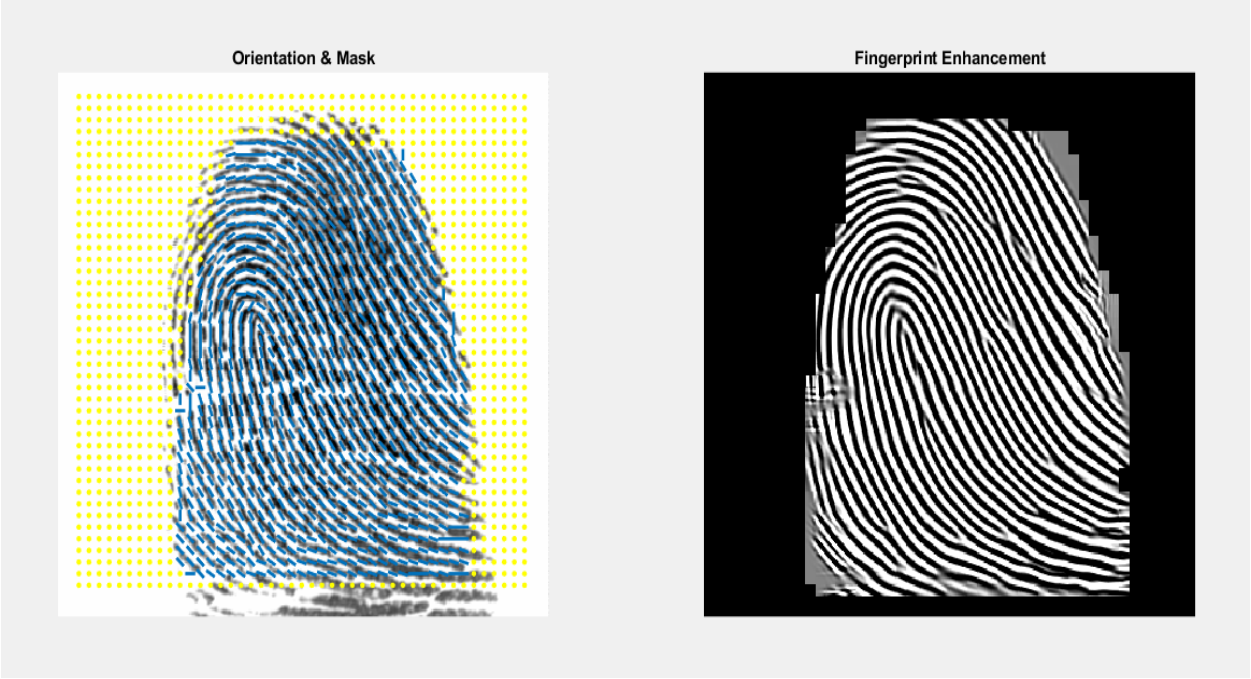

Figure 3- 4 : Fingerprint orientation field and masking

Several software programs are available that provide a framework for implementing neural networks. the paintings provided here uses keras, that is a python library that gives smooth to use abstractions to effective deep studying libraries inclusive of theano and tensorflow (used right here). the cnn used in this paintings uses the construction . The types of layers used are described as follows:

- Convolutional Layer: each convolutional layer includes a financial institution of filters (weights) which can be convolved with the output of the previous layer, or the input photo if it's miles the first layer, to produce some reaction.
- Max-Pooling Layer: the max-pooling layer performs sub-sampling on the outputs generated with the aid of the previous convolutional layer(s) by way of choosing the most price in an mxm window. in this work, all max-pooling layers are 3x3 with a stride of three, as a consequence decreasing the scale of the output by way of 4 .
- Fully Connected Layer: the absolutely linked layer connects a hard and fast of neurons to each of the neurons of the preceding layer. the model proven above has 3x3 feature maps inside the remaining max-pooling layer that ultimately shape neurons linked to the 64 neurons within the proceeding absolutely linked layer for a total of 49713 weights (sixty four bias 32 weights).

The Keras provides several types of additional «layers» that simplify certain aspects of implementation. , the flatten layer simply vectorizes and connects all of the neurons from the outputs of the previous layer to all of the neurons in the fully connectedlayer.

All the convolutional layers and the primary absolutely linked layer use the rectified linear activation feature (relu):

$$f(x) = \begin{cases} 0 \; if \; x \leq 0 \\ x \; if \; x > 0 \end{cases} \qquad 3.1$$

Relu activation has been proven to reduce the want to carry out unsupervised pre-schooling in deep neural networks. and is the maximum widely used activation feature used in modern-day deep architectures. The softmax function , given as :

$$P(y = j) = \frac{e^{xj}}{\sum_k e^{Zk}} \ , for\ j = 1, \dots k \qquad 3.2$$

Scales the cnn outputs such that they're all inside the variety [0,1] and sum to at least one, allowing them to be interpreted as a specific possibility distribution over k instructions. for that reason, the best fee may be taken because the version's prediction that a given information pattern is a member of that magnificence. Categorical cross-entropy, given as:

$$H(P, Q) = -\sum Pi \log(qi) - (1 - pi).\log(1 - qi) \qquad 3.3$$

is used, where p_i is the true distribution of the data and q_i is the distribution predicted by the model.

We explain all of this detailed in table 3-1 , It is what we get from analyzing result of work system . Figure 3-5 of Analys Network .

ANALYSIS RESULT

	Name	Type	Activations	Learnable Prope...
1	input 219×227×1 images with 'zerocenter' nor...	Image Input	219(S) × 227(S) × 1(C) × 1(B)	-
2	conv_1 8 3×3×1 convolutions with stride [1 1] an...	Convolution	219(S) × 227(S) × 8(C) × 1(B)	Weigh… 3 × 3 × 1 … Bias 1 × 1 × 8
3	batchnorm_1 Batch normalization with 8 channels	Batch Normalization	219(S) × 227(S) × 8(C) × 1(B)	Offset 1 × 1 × 8 Scale 1 × 1 × 8
4	relu_1 ReLU	ReLU	219(S) × 227(S) × 8(C) × 1(B)	-
5	maxpool_1 2×2 max pooling with stride [2 2] and pa...	Max Pooling	109(S) × 113(S) × 8(C) × 1(B)	-
6	conv_2 16 3×3×8 convolutions with stride [1 1] a...	Convolution	109(S) × 113(S) × 16(C) × 1(B)	Weig… 3 × 3 × 8 … Bias 1 × 1 × 16
7	batchnorm_2 Batch normalization with 16 channels	Batch Normalization	109(S) × 113(S) × 16(C) × 1(B)	Offset 1 × 1 × 16 Scale 1 × 1 × 16
8	relu_2 ReLU	ReLU	109(S) × 113(S) × 16(C) × 1(B)	-
9	maxpool_2 2×2 max pooling with stride [2 2] and pa...	Max Pooling	54(S) × 56(S) × 16(C) × 1(B)	-
10	conv_3 32 3×3×16 convolutions with stride [1 1] ...	Convolution	54(S) × 56(S) × 32(C) × 1(B)	Weig… 3 × 3 × 16… Bias 1 × 1 × 32
11	batchnorm_3 Batch normalization with 32 channels	Batch Normalization	54(S) × 56(S) × 32(C) × 1(B)	Offset 1 × 1 × 32 Scale 1 × 1 × 32
12	relu_3 ReLU	ReLU	54(S) × 56(S) × 32(C) × 1(B)	-
13	maxpool_3 2×2 max pooling with stride [2 2] and pa...	Max Pooling	27(S) × 28(S) × 32(C) × 1(B)	-
14	conv_4 64 3×3×32 convolutions with stride [1 1] ...	Convolution	27(S) × 28(S) × 64(C) × 1(B)	Weig… 3 × 3 × 32… Bias 1 × 1 × 64

15	batchnorm_4 Batch normalization with 64 channels	Batch Normalization	27(S) × 28(S) × 64(C) × 1(B)	Offset 1 × 1 × 64 Scale 1 × 1 × 64
16	relu_4 ReLU	ReLU	27(S) × 28(S) × 64(C) × 1(B)	-
17	fc_1 64 fully connected layer	Fully Connected	1(S) × 1(S) × 64(C) × 1(B)	Weights 64 × 48384 Bias 64 × 1
18	relu_5 ReLU	ReLU	1(S) × 1(S) × 64(C) × 1(B)	-
19	fc_2 32 fully connected layer	Fully Connected	1(S) × 1(S) × 32(C) × 1(B)	Weights 32 × 64 Bias 32 × 1
20	relu_6 ReLU	ReLU	1(S) × 1(S) × 32(C) × 1(B)	-
21	fc_3 16 fully connected layer	Fully Connected	1(S) × 1(S) × 16(C) × 1(B)	Weights 16 × 32 Bias 16 × 1
22	relu_7 ReLU	ReLU	1(S) × 1(S) × 16(C) × 1(B)	-
23	fc_4 8 fully connected layer	Fully Connected	1(S) × 1(S) × 8(C) × 1(B)	Weights 8 × 16 Bias 8 × 1
24	fc_5 4 fully connected layer	Fully Connected	1(S) × 1(S) × 4(C) × 1(B)	Weights 4 × 8 Bias 4 × 1
25	softmax softmax	Softmax	1(S) × 1(S) × 4(C) × 1(B)	-
26	classoutput crossentropyex with 'finger_1' and 3 oth...	Classification Output	1(S) × 1(S) × 4(C) × 1(B)	-

Figure 3-5 : Analyzing Architecture of this work

3.6 Exprimenal Results:

The model described above was tested using one configurations in which either , fingerprints from FVC 2000 (DB1_B)was used for training and testing For 1000 iterations , First, our work is by reading a random collection of images as shown in the Figure 3-5 , in the training of system We see Figure 3-6 .

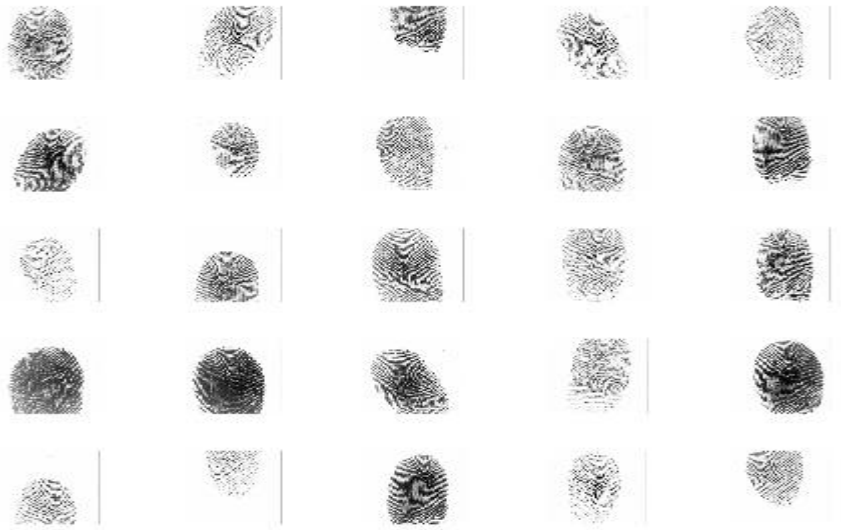

Figure 3-6: A random sample for fingerprints

Tabel 3- 3 : The classification Accuracy

Epoch	Iteration	Time Elapsed (hh:mm:ss)	Mini-batch Accuracy	Mini-batch Loss	Base Learning Rate
1	1	00:00:16	29.17%	1.6194	1.0000e-04
50	50	00:01:43	58.33%	1.0054	1.0000e-04
100	100	00:02:57	66.67%	0.8228	1.0000e-04
150	150	00:03:47	62.50%	0.8378	1.0000e-04
200	200	00:05:07	75.00%	0.6453	1.0000e-04
250	250	00:06:17	87.50%	0.4816	1.0000e-04
300	300	00:07:22	79.17%	0.4364	1.0000e-04
350	350	00:08:35	87.50%	0.3986	1.0000e-04
400	400	00:09:46	91.67%	0.3649	1.0000e-04
450	450	00:10:59	83.33%	0.3481	1.0000e-04
500	500	00:12:13	87.50%	0.2722	1.0000e-04
550	550	00:13:22	91.67%	0.2670	1.0000e-04
600	600	00:14:23	91.67%	0.2518	1.0000e-04
650	650	00:15:24	95.83%	0.1263	1.0000e-04
700	700	00:16:26	95.83%	0.2336	1.0000e-04
750	750	00:17:29	91.67%	0.1944	1.0000e-04
800	800	00:18:33	95.83%	0.1692	1.0000e-04
850	850	00:19:53	100.00%	0.1096	1.0000e-04
900	900	00:21:14	91.67%	0.1571	1.0000e-04
950	950	00:22:31	95.83%	0.1524	1.0000e-04
1000	1000	00:23:54	91.67%	0.2163	1.0000e-04

We also note the classification accuracy for training iterations . as shown in figure 3-7

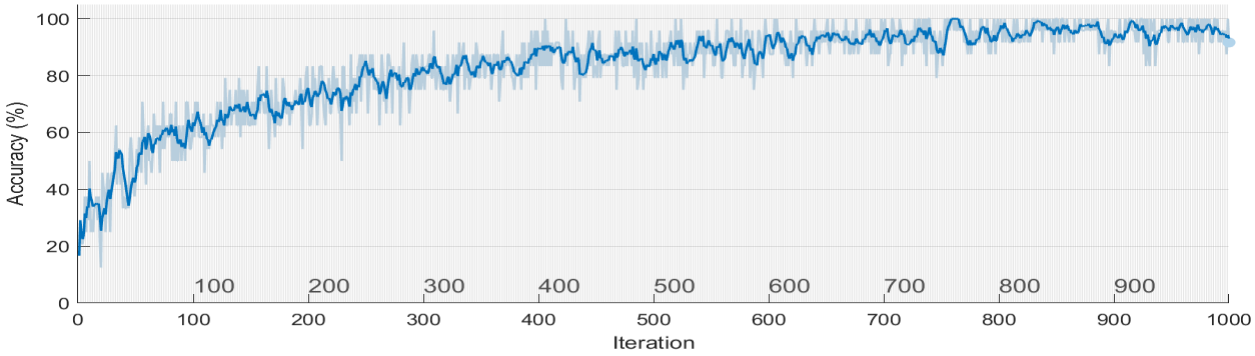

Figure 3-7 : The Classification accuracy for training

We also note the loss for training iterations , as we shown in figure 3-8

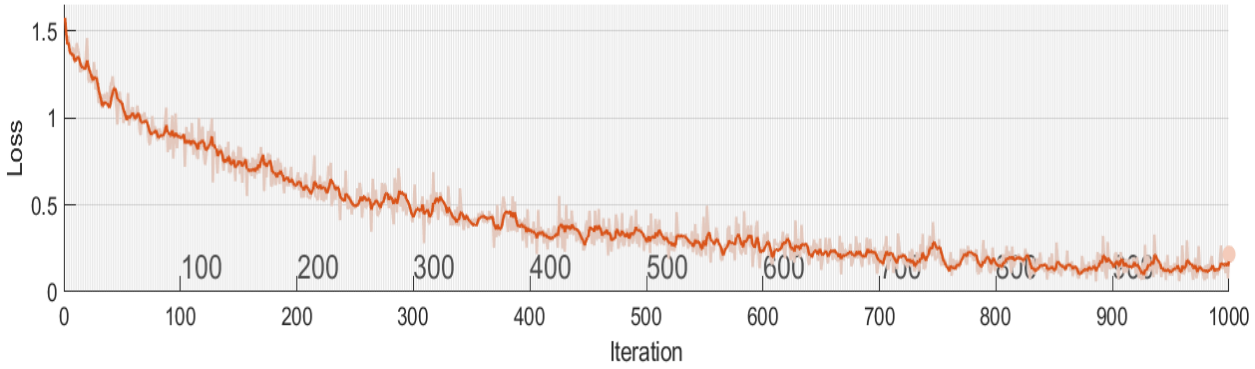

Figure 3- 8: The loss of accuracy for training

As we get, the latter has the results of the classification of his eye random . At the same time, we received a rate of 95,26% the score of system as we shown in figure 3-9

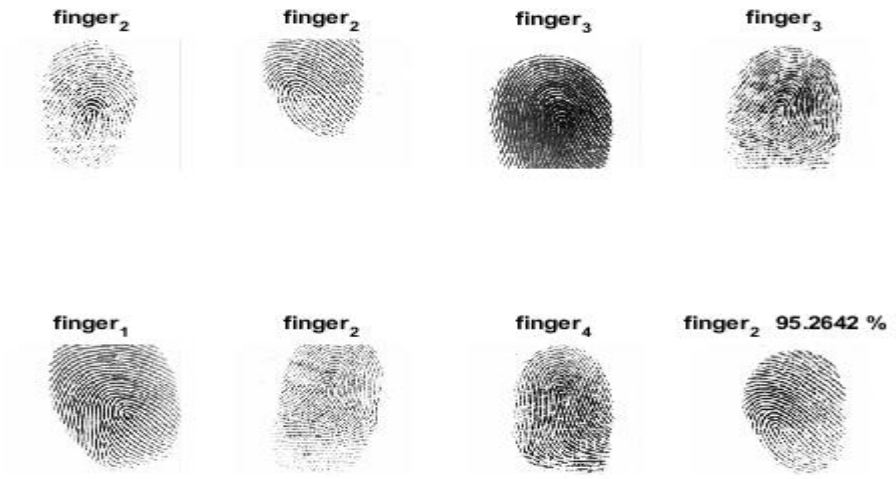

Figure 3-9 : Test of system with score

3.7 Conclution and Future Work :

In this work, a new technique to fingerprint type using convolutional neural networks become created and examined. it has been proven that a incredibly shallow network may be effectively skilled to understand fingerprint lessons with a high degree of accuracy. moreover, with a small amount of preprocessing, the dimensionality of the network inputs can be considerably decreased through a component (in the case of FVC 2000), thus reducing network training time.

In future visions , additional steps may be taken to augment the classification process. we keep in mind the a priori distribution of fingerprints discovered in nature and removed pix from the contemporary dataset to mirror this herbal distribution.Many methods allow for some pattern rejection. additionally, even though the model produces enormously correct effects with 0 rejection, allowing for a small percent of rejected snap shots ought to boom accuracy to 100% on the training datasets.

The use of the SFinge device for use in checking out classification algorithms. every database contains 10,000 fingerprint pics with 288x384 pixels following a natural distribution.even though those prints are synthetically generated, they are extraordinarily just like actual fingerprints. they also incorporate simplest true classlabels, not like the ambiguous labeling of fvc2000, making an allowance for greater self belief in training and trying out on the entire dataset rather than most effective a subset. due to the value of the SFinge software program, checking out on these databases became no longer viable for this work, but future work using this version ought to consist of trying out on those three databases.

General Conclusion

As humans observed scientific developments in all fields, he wanted to enter development after entering computer science in the development of biometrics, all their structural structures and their use in wide ranges to ensure protection, security, and adaptability, and the use of measurement frameworks would improve progress in the modern era and include them in Many fields after medicine, crime-fighting, information security, technology and the multiplicity of its methods.

After we touched on the diversity of the methods used and we took in this work to see the machine for the fingerprint and its various characteristics and types of processors, some of the processors are by discovering the ridges and valleys and extracting the features after the image optimization operations are done to extract its features in a good way and they are the most influential factors on improving the quality of the image captured by the fingerprint Through the sensitive factor, the type, and extent of its development, and that is through the development in this field. This is after entering deep learning and machine learning in recognizing objects. Biometric recognition of a fingerprint has become part of this work by recognizing and classifying fingerprints, and it is through training the machine on multiple situations similar to the real situation. The results of accuracy in learning vary day by day. Research increases and be The accuracy rate is more than the previous one.

In the end, research does not end in every field and every day, and this is what the world witnesses, and this is by reference to the power of God and his miracles in creating man, namely the mind.

Summary

In our work, after we started by identifying biometrics in general, and headed to work on identifying people with the fingerprint system, introducing it and explaining it in-depth, we resorted to our applied work to keep pace with modern scientific development by introducing deep learning into our work and relying on Convolutional Neural Network model. We got results that are in the system's classification success rate to 95.26% .

Keywords : biometrics , fingerprint , convolutional neural network .

ملخص

في عملنا هذا بعد ان كانت بدايته عن القياسات الحيوية بصفه عامة، وتوجها بالعمل على نظام التعرف على الاشخاص بنظام بصمة الأصابع والتعريف به وشرحه شرحا معمقا التجأنا في عملنا التطبيقي لمواكبة التطور العلمي الحديث بإدخال التعلم العميق في عملنا والاعتماد على نموذج شبكة الحلقات الالتفافية وحزنا على نتائج تكون في نسبة نجاح التصنيف في النظام الى 95.26% .

الكلمات المفتاحية : القياسات الحيوية ، بصمة الأصابع ، شبكة الحلقات الإلتفافية

Resumé

Dans notre travail, après avoir commencé par identifier la biométrie en général, et nous sommes dirigés vers l'identification des personnes avec le système d'empreintes digitales, l'introduisant et l'expliquant en profondeur, nous avons eu recours à notre travail appliqué pour suivre le rythme du développement scientifique moderne en introduisant des apprendre dans notre travail et s'appuyer sur le modèle de réseau neuronal convolutif. Nous avons obtenu des résultats qui sont dans le taux de réussite de la classification du système à 95,26 %.

Mots clé : biométric , empreintes digitales , réseau neuronal convolutif .

Bibliography

[1]	F. Belhadj, "*Biometric system for identification and authentication," Hal.archieve*, Alger, 2017.
[2]	K. N. A. K. J. Arun A. Ross, *Handbook of Multibiometrics (International Series on Biometrics*), Springer, 2006.
[3]	K. N. A. K. J. Arun A. Ross, "*50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities*," Pattern Recognition Letters, January, 2016.
[4]	A. K. A. K. Jain, "*Biometric Recognition: An Overview,Second Generation Biometrics: The Ethical*," 2012, p. 49–79.
[5]	S. M. R. A. B. J. T. Nicholas Evans, "*Biometrics Security and Privacy Protection," IEEE Signal Processing Magazine* , vol. 32, no. 5, pp. 17-18, 2015.
[6]	I. Bouchrika, "*A Survey of Using Biometrics for Smart," in Advanced Sciences and Technologies for Security Applications*, Souk Ahras, Algeria, Springer International Publishing, 2018, pp. 6-7.
[7]	W. Prosser, "*Privacy*," California Law Review, vol. 48, no. 3, 1960.
[8]	S. K. a. L. Millett, *Who Goes There?: Authentication Through the Lens of Privacy Committee on Authentication Technologies and Their Privacy Implications*, National Research Council, National Academies Press, 2003.
[9]	W. James, J. Anil, M. Davide and M. Dario, *Biometric systems: technology, design, and performance evaluation*, Springer Science+Business Media, 2005.
[10]	R. Arun A, N. Karthik and J. Anil K, *Handbook of Multibiometrics*, 1 ed., New York: Springer Science+Business Media, 2006, pp. 8-10.
[11]	F. BELHADJ, "*Biometric system for identification and*," HAL Science ouvert, Alger, 2017.
[12]	F. Belhadj, "*Biometric system for identification and authentication*".
[13]	W. James, J. Anil, M. Davide and M. Dario, *Biometric Systems Technology, Design and Performance Evaluation*, p. lbid.97.
[14]	R. Arun A, N. Karthik and J. Anil K, *Handbook of Multibiometrics*, p. lbid. 44.
[15]	L.Masek, "*Recognition of human iris patterns for biometric identification*," Available on: http://www.csse.uwa.edu.au/~pk/stude, Western Australia, 2003.
[16]	J. Daugman, "*How Iris Recognition Works," IEEE International Conference on Image Processing*, vol. 1, p. 33–36, 2002.
[17]	H. K. Lewis, "*Eugene Wolff's Anatomy of the Eye and Orbit, 7th ed.," Survey of Ophthalmology*, 1976.
[18]	"*Iris recognition: An emerging biometrie technology*," Proceedings of the

	IEEE, vol. 85, no. 9, p. 1348–1363, 1997.
[19]	J. Daugman, "*High Confidence Visual Recognition of Persons by a Test of Statistical Independence*," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15, no. 11, p. 1148–1161, 1991.
[20]	J. Daugman, "*Biometric personal identification system based on iris analysis*". USA Patent 5,291,560, 1994.
[21]	" *DNA Fingerprint Identifi cation*," [Online]. Available: http://www.fi ngerprinting.com/dna-fi ngerprint-identifi cation.php . [Accessed 20 Feb 2010].
[22]	R. Arun A, K. Nandakumar and A. K. Jain, *Handbook of Multibiometrics*, pp. lbid 23-24.
[23]	R. Arun A, K. Nandakumar and A. K. Jain, *Handbook of Multibiometrics*, p. lbid.23.
[24]	R. Arun A, K. Nandakumar and A. K. Jain, *Handbook Multibiometrics*, p. lbid 24.
[25]	F. Belhadj, *Biometric system for identification and authentication*, pp. 7-8.
[26]	J. Anil K, B. Ruud and P. Sharath, *Biometrics personal identification in Networked society*, p. lbid.328.
[27]	J. Anil, B. Ruud and B. Sharath, *Biometrics personal identification in networked society*, pp. lbid.36-37.
[28]	S. Nanavati, M. Thieme and R. Nanavati, Biometrics: *Identity Verification in a Networked World*, New York: John Wiley & Sons, Inc, 2002.
[29]	S. Angela , B. Sacha and W. D, "*Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security*," BT Technology Journal, vol. 19, no. 3, p. 122–131, 2001.
[30]	S. G.Davies, "*Touching Big Brother How Biometric Technology Will Fuse Flesh and Machine*," Information Technology & People, vol. 7, no. 4, 1994.
[31]	J. R. Reidenberg, "*Privacy in the Information Economy: A Fortress or Frontier for Individual Rights*," Fordham University School of Law, vol. 44, p. 195, 1992.