People's Democratic Republic of Algeria
Ministry Of Higher Education And Scientific Research
University of Larbi Tebessi –Tebessa
Faculty of Exact Sciences and Sciences of Nature and Life
Department Of Mathematics and Computer Science

A Thesis submitted for the Degree of Master Diploma
Specialty: Computer Science
Option: RSI

Presented By
Bouguerra Mohamed

Fingerprint Recognition and Classification

In Front of the Jury:

Dr. MY. Haouam	President	U. Larbi Tebessi University, Tebessa
Dr. MS. Souahi	Examiner	U. Larbi Tebessi University, Tebessa
Dr. T. Mekhaznia	Supervisor	U. Larbi Tebessi University, Tebessa

Acknowledgment

Before everyone, I want to thank my supervisor Dr. MEKHAZNIA TAHAR for his agreement to be my thesis supervisor and for consistent support, encouragement, patience, and guidance during the work on this project.

I would also thank all members of the jury: DR Haouam Mohamed Yassine and DR Souahi Mohamed Saleh for taking the time to examine my work

I would finally thank my family and all my friends and colleagues of Larbi Tebessi University for their great support.

Dedication

I dedicate my work to my parents Teacher El-haddi Bouguerra and Rachida

Abstract

Biometrics is one of the applications in Image processing that refers to technologies that use physiological or behavioral characteristics of the human body to determine a person's identity.

The use of fingerprinting is today one of the most reliable technologies on the market to identify persons in secure systems, this technology is simple to use and easy to implement as opposed to other biometric modalities.

This thesis deals with the development of a fingerprint recognition system based on minutiae points for identifying individuals. The software platform used for the implementation of the proposed work is MATLAB 2016a and the database used to perform the tests is the FVC 2002 BD1 database. The proposed system gives satisfactory results for individual identifications.

Keywords: fingerprint; minutiae; binirization; thinning; bifurcation; termination; identification; MATLAB

الملخص

يعد القياس البيومتري أحد التطبيقات في معالجة الصور التي تشير إلى التقنيات التي تستخدم الخصائص الفسيولوجية أو السلوكية لجسم الإنسان لتحديد هوية الشخص.

يعد استخدام بصمات الأصابع اليوم أحد أكثر التقنيات موثوقية في السوق للتعرف على الاشخاص داخل الانضمة المؤمنة تعد هذه التكنولوجيا سهلة الاستخدام و التطبيق مقارنتا بالقياسات البيومترية الاخرى.

تتناول هذه الأطروحة تطوير نظام التعرف على بصمات الأصابع بناءً على التفاصيل الدقيقة للبصمة لتحديد هوية الأفراد. البيئة البرمجية المستخدمة لتنفيذ هذا العمل هي MATLAB 2016a و قاعدة البينات المستخدمة لاجراء الاختبارات هي FVC 2002 DB1, يعطي النضام المقترح نتائج مرضية للتعرف على الافراد.

الكلمات المفتاحية : بصمة الاصبع ; تفاصيل ; ثنائية ; الهيكل ; التشعب ; النهاية ; تحديد الهوية ; MATLAB

Résumé

La biométrie est l'une des applications en traitement d'images qui fait référence aux technologies qui utilisent les caractéristiques physiologiques ou comportementales du corps humain pour déterminer l'identité d'une personne.

L'utilisation des empreintes digitales est aujourd'hui l'une des technologies les plus fiables du marché pour authentifier un individu dans les systèmes sécurisés, cette technologie est simple à utiliser et facile à mettre en œuvre contrairement aux autres modalités biométriques.

Cette thèse porte sur le développement d'un système de reconnaissance d'empreintes digitales basé sur des points de minutie pour l'identification d'individus. La plate-forme logicielle utilisée pour la mise en œuvre des travaux proposés est MATLAB 2016a et la base de données utilisée pour effectuer les tests est la base de données FVC 2002 BD1. Le système proposé donne des résultats satisfaisants pour les identifications individuelles.

Mots clés: empreinte digitale ; minutie ; binarisation ; squelettisation ; bifurcation ; terminaison ; identification ; MATLAB

Table of Contents

List of Figures

List of Tables

List of Acronyms

FRS: Fingerprint Recognition System

CN: Crossing Number

DNA: Deoxyribonucleic Acid

FVC: Fingerprint Verification Competition

CV: Computer Vision

General Introduction

General Introduction

The explosion of information technology and communication networks in recent decades has raised people's need to identify themselves dramatically.

In another way, security is a basic human demand that is becoming more important, accurate identification of persons has become a serious problem for a variety of applications (border control, access to public places, transport). All these problems have thus led to the increased development of biometric identification techniques.

Biometrics is the process of automatically identifying (or verifying) an individual based on physiological or behavioral characteristics (e.g., fingerprints, hand geometry, iris, retina, face, hand vein, facial thermograms, signature, voiceprint). Biometric indicators have an advantage over traditional security approaches in that they are difficult to steal or share.

Among all the biometric indicators, fingerprints are commonly utilized for person identification as opposed to other biometric techniques for a variety of reasons, including ease of capture, high distinctiveness, and persistence over time. Additionally, fingerprint sensors are smaller and less expensive than other biometric sensors.

Fingerprint recognition systems use one of these three techniques for the matching of fingerprints: correlation-based matching, pattern-based matching, and minutiae-based matching. The last technique is the most used because it’s based on the extraction of local features of the fingerprint such as terminations and bifurcations, two fingerprint images are identical if their minutiae points are the same.

However, because recognizing fingerprints in low-quality images is still a difficult operation, the fingerprint image must be preprocessed before it can be matched. It is difficult to extract fingerprint characteristics from a grayscale fingerprint image directly. As a result, we developed a fingerprint recognition system that uses a minutiae-based matching algorithm. The suggested algorithm has three stages. Preprocessing the supplied fingerprint image is the first stage. In the second stage, the enhanced and binarized fingerprint image is converted to a thinned image, and minutiae are retrieved using the Crossing Number Concept. The third stage compares the input fingerprint image (after preprocessing and minutiae extraction) to the fingerprint images enrolled in the database and determines whether the input fingerprint is matched or not.

The objective of this work is to implement a fingerprint recognition system for individuals based on fingerprint minutiae points.

The content of the thesis is organized into four chapters as follows:

In the first chapter, we have introduced some definitions and general information about image processing and biometrics as image processing methodology, biometric types, and biometric system architecture.

In the second chapter, we have introduced the fingerprint recognition system in detail, we illustrate fingerprint characteristics, classes, system architecture, and matching techniques.

The third chapter covers our proposed method the algorithms and techniques we used to implement the fingerprint recognition system.

The fourth chapter includes the different tests and results using the FVC 2002 BD1 database that we achieved on our system.

The works ended with a conclusion and general avenues and recommendations for future similar works.

Chapter 1
Imagery and Biometry

I. Chapter 1 Imagery and Biometry

I.1.Introduction

In the age that we live in, data scientists, students, and researchers have been coming up with advanced ways and technics to extract information from any piece of data. Images have not been left out in this process. They have proven to be very useful in regard of the human vision ability that can quickly assimilate large amounts of information within a very short time. Computer's scientists, data scientists, and researchers still trying to bring this interpretation ability and data extraction for a better understanding to computers.

Image processing is defined as a method of converting an image into digital form and performing operations on it in order to obtain a better image or extract relevant information from it. It is a type of signal dispensation in which the input is an image and the output is an image or characteristics associated with that image [1].

In fact, digital image processing has an impact on practically every technical activity. As optics, imaging sensors, as computational technology advanced, image processing become more commonly used in many different areas. Some areas of applications of digital image processing include image enhancement for better human perception, image compression and transmission, as well as image representation for automatic machine perception [2].

Along of various biometrics techniques, in the past few decades, human beings have been addicted to various technologies such as captured photos, scanned signatures, bar code systems, verification IDs and so on. Also, Biometrics is an image processing application that refers to technologies that use physiological or behavioral aspects of the human body to authenticate users. The biometric authentication system is based on two modes: Enrolment and recognition. In the enrolment mode, biometric data from the sensor is collected and saved in a database, together with the person's identity, for recognition purposes. In the recognition mode, the biometric data is re-acquired from the sensor and compared to the stored data to determine the user's identity.

Biometric recognition is based on uniqueness and permanence. The term "uniqueness" refers to the lack of feature similarity between two different biometrics data sets. Even if they are identical twins, no two persons have the same fingerprint feature. Permanence refers to the fact that the characteristics of biometrics do not change through time or with age.

Biometrics can have physiological or behavioral traits, the physiological traits are found in the physical part of the body such as (fingerprint, palm print, iris, face, DNA, hand geometry, retina... etc). The behavioral traits depend on an action taken by a person such as (Voice recognition, keystroke-scan, and signature-scan).

I.2.Imagery Overview

I.2.1.Definition

An image is represented by its dimensions (height and width) based on the number of pixels. For example, if the dimensions of an image are 500 x 400 (width x height), the total number of pixels in the image is 200 thousand. A pixel is a point on the image that takes on a specific shade, opacity or color. It is usually represented in one of the following modes:

1) **Binary Image (Black and White):** The binary image as its name suggests, contains only two-pixel elements i.e. 0 and 1, where 0 denotes black and 1 denotes to white. This image is also known as Monochrome.

Figure 1: A binary image

2) **Grayscale:** A pixel is an integer with a value between 0 to 255 (0 is completely black and 255 is completely white).

Figure 2: Grayscale image

3) **Red, Green and Blue (RGB):** A pixel is made up of 3 integers between 0 to 255 (the integers represent the intensity of red, green, and blue).

Figure 3: RGB image

4) **Red, Green, Blue and Alpha (RGBA):** It is an extension of RGB with an added alpha field, which represents the opacity of the image.

Figure 4: RGBA image

I.2.2.Mathematical Representation

Images are represented in rows and columns According to the following syntax in which images are represented:

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & f(0,2) & \dots & f(0,N-1) \\ f(1,0) & f(1,1) & f(1,2) & \dots & f(1,N-1) \\ \vdots & \vdots & \vdots & & \vdots \\ f(M-1,0) & f(M-1,1) & f(M-1,2) & \dots & f(M-1,N-1) \end{bmatrix}$$

Table 1: Image matrix representation

Where M, N and F denote respectively number of rows, number of columns and function that represents the pixels in the matrix.

The right side of this equation illustrated in Table 1 is digital image by definition. Every element of this matrix is called an image element, picture element, or pixel.

I.2.3.Image Processing

1) Definition

Image processing refers to the process of converting an image to a digital format and then executing operations on it to extract useful information such as the image's characteristics and features. All images are normally treated as 2D templates by the image processing system, which then applies specified signal processing procedures.

Image processing requires a set of operations that are performed within each pixel of an image. Pixel by pixel, the image processor executes the first set of actions on the image. Once that's completed, it'll move on to the next operation, and so on. These operations can compute the output value at any pixel in the image.

There are five main types of image processing:

- **Visualization -** Look for objects that aren't apparent in the image.
- **Recognition -** Identify or recognize the objects in the image.
- **Sharpening and Restoration -** From the original image, create an enhanced image.
- **Pattern Recognition -** Determine the different patterns that surround the objects in the image.
- **Retrieval -** Browse and find images similar to the original image from a big library of digital images.

2) Processing Methodology

- **Image Acquisition**

The initial stage in image processing is image acquisition. In image processing, this stage is also known as preprocessing. It entails getting the image from a source, which is usually hardware.

- **Image Enhancement**

The technique of bringing out and highlighting particular areas of interest in an image that has been concealed is known as image enhancement. This can include adjusting the brightness, contrast, and other settings.

- **Image Restoration**

The technique of improving the appearance of an image is known as image restoration. Image restoration, unlike image augmentation, is done using mathematical or probabilistic models.

- **Color Image Processing**

In the digital domain, color image processing encompasses a variety of color modeling techniques. Because of the widespread usage of digital images on the internet, this step has acquired popularity.

- **Wavelets and Multiresolution Processing**

Wavelets are a type of visual representation that comes in a variety of resolutions. For data compression and pyramidal representation, the images are separated into wavelets or smaller sections.

- **Compression**

Compression is a technique for reducing the amount of storage or bandwidth needed to save or transmit an image. This is especially true when the image will be used on the Internet.

- **Morphological Processing**

Morphological processing is a collection of techniques used to morph images based on their forms.

- **Segmentation**

One of the most difficult aspects of image processing is segmentation. It entails breaking down an image into its component bits or objects.

- **Representation and Description**

Each region of an image is represented and described in a manner appropriate for further computer processing once it is segmented into regions in the segmentation process. The qualities and regional properties of a picture are dealt with in representation. The task of description is to extract quantitative information that can be used to distinguish one class of objects from another.

- **Recognition**

Based on its description, recognition assigns a label to an object.

3) Examples and Applications

- **Image Correction, Sharpening, and Resolution Correction**

To correct or enhance damaged images we can use, zooming, sharpening, edge detection, and high dynamic range edits. All of these steps contribute to the enhancement of the image. These things are simple to achieve with most editing software and image correcting code and this is widely used in the field of media to produce high-quality images.

- **Medical Technology**

In the medical field, Image Processing is used for various tasks like PET scan, X-Ray Imaging, Medical CT, UV imaging, Cancer Cell Image processing, and much more. The introduction of Image Processing to the medical technology field has greatly improved the diagnostics process.

- **Computer / Machine Vision**

One of the most interesting and useful applications of Image Processing is in Computer Vision. Computer Vision is used to make the computer recognize the environment identify things, and process the whole environment as one component, an important use of Computer Vision is Self-Driving Cars, Drones, etc. CV helps in obstacle detection, path recognition, and understanding the environment.

- **Pattern Recognition**

Artificial intelligence and Machine Learning are used in pattern recognition, which is a branch of Image Processing. Image processing is a technique for identifying patterns and characteristics in images. Pattern recognition is utilized in a variety of applications, including handwriting analysis, image identification, and computer-assisted medical diagnosis.

- **Video Processing**

Video is basically a fast movement of images. Various image processing techniques are used in video processing. Noise reduction, image stabilization, frame rate conversion, detail improvement, and other video processing techniques are only a few examples.

I.3.Biometric System

I.3.1.Definition

Biometrics is the measurement and analysis of someone’s unique physical and behavioral characteristics. This technology is used for identification (figuring out who someone is) and authentication (someone is who they say they are).

I.3.2.Biometric Evolution

The word "biometrics" comes from the Greek terms "bio" (life) and "metric"(to measure). Interestingly, the term “biometrics” was not used to describe these technologies until the 1980s. The first reference found for the term “biometrics” was in a 1981 article in The New York Times [3, 4].

Fingerprint recognition represents the oldest method of biometric identification, with its history going back as far as at least 6000 B.C [3].

The ancient Assyrians, Babylonians, Japanese, and Chinese used fingerprints to sign legal documents for the first time. Fingerprints were utilized on clay tablets for economic transactions

in ancient Babylon. According to explorer Joao de Barros, a sort of fingerprinting was utilized in China. Chinese merchants were stamping children's palm prints and footprints on paper with ink to differentiate them from one another, he wrote.

The first modern study of finger-prints was done by Johannes Evan-gelista Purkinje, a Czech physiologist and professor of anatomy at the University of Breslau. In 1823, he proposed a system of fingerprint classification. The English began using palm and fingerprints in India in July 1858, when Sir William Herschel pressed handprints on the backs of con-tracts. Herschel moved from palm-prints to prints of the right index and middle fingers [3].

1974 was a breakthrough year for automated biometrics as the University of Georgia began using hand geometry in its dormitory food service areas. Both the Stanford Research Institute in the United States and the National Physical Laboratory in the United Kingdom had begun working on signature recognition systems [3].

In the mid-1980s, the State of California began collecting fingerprints as a requirement for all driver's license applications [3].

The first biometric industry organization, the International Biometrics Association (IBA), was founded in 1986–1987[3].

The International Biometric Industry Association (IBIA) was created in Washington, DC, in 1998 as a non-profit sector trade association to promote the biometric industry's collective international interests. The National Biometric Security Project (NBSP) was founded in 2001 to respond to the events of September 11, 2001, and the need for accelerated development and deployment of biometrics technologies [3].

After the start of the 20th century, a lot of biometric techniques used by human beings in their daily life for example the United Arab Emirates has used an iris recognition biometric screening system for over two years to screen all arriving visa holders at their points of entry to detect previously deported persons.

Retinal scan devices are typically utilized in contexts demanding very high levels of security and accountability, such as high-level government, military, and correctional applications.

I.3.3.Characteristics

Physical and Behavioral characteristics of human trait should meet some requirements in order to be used as biometrics methods. These requirements are either theoretical or practical. There are basically seven theoretical requirements which are:

- **Universality:** Each person should possess a biometric trait. For instance, nearly everyone will have at least one finger for fingerprint biometric and a face for face recognition.
- **Uniqueness:** Each person should be sufficiently unique in terms of their biometric traits. This is how well the particular biometric distinguishes people.
- **Permanence:** Over time, the biometric feature should remain constant. A good biometric system should track something that changes slowly over time (if at all). DNA and

fingerprints, for example, are among the best and rarely change, while handwriting and voice may vary with time.

- **Collectability:** Ease of data capturing, measuring and processing. How easily the biometric can be measured can be significantly important in some applications.
- **Performance:** recognition accuracy, speed (throughput), resource requirements and robustness to operational and environmental factors.
- **Acceptability:** The willingness of users to accept the biometric identifier in their everyday life.
- **Circumvention**: The simplicity with which a fraudulent approach can be used to get around the biometric system. In summary, a realistic biometric system should have adequate recognition accuracy and speed with appropriate resource requirements, be safe for users, be accepted by the desired population, and be sufficiently strong against various fraudulent approaches.

I.3.4.Biometric System Architecture

1) Overview

Biometrics are computerized methods of identifying a person based on physiological and observable qualities. The use of biometric systems has impacted the way we identify and authenticate ourselves around the world. By utilizing this technology, not only has the identification of people changed, but also the time it takes to identify and verify people has been significantly reduced. Face, fingerprints, handwriting, palmprints, hand geometry, gait, iris, retinal, and voice are the various characteristics that are measured in biometric techniques.

2) Description

- **Enrollment**

The user's biometric information is recorded in a database during the enrolment process. It's a one-time action. In this phase, the appropriate information is typically measured quite precisely.

- **Recognition**

This is the second phase of the biometric system. This happens when the detection phase starts depending on the first phase of the user's authentication. This phase must be rapid, accurate, and capable of quickly identifying the authentication issue.

3) Components

Biometric system architecture has the following main components

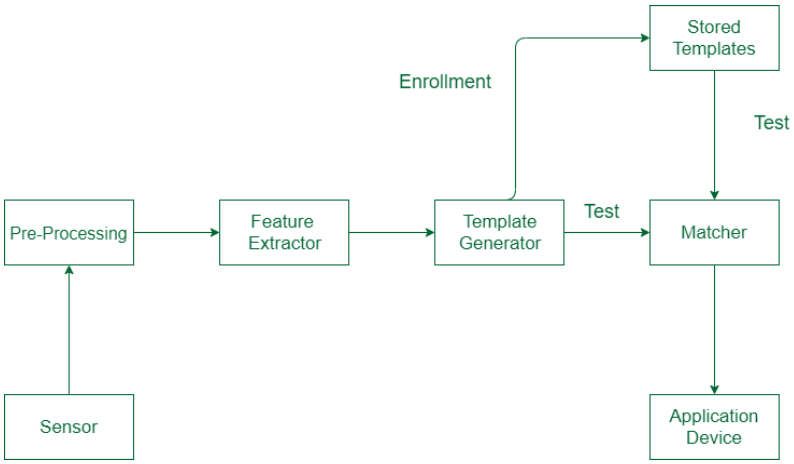

Figure 5: general architecture of biometric system

- **Sensor**

The sensor is the first component of a biometric system, and it captures all of the necessary biometric data. It serves as a link between the system and the outside world. Typically, it is an image acquisition system, but whether it needs to be replaced or not depends on the features or characteristics required.

- **Pre-Processing**

All of the pre-processing happens in the second block. Its goal is to increase the input quality by eliminating sensor artifacts, background noise, and other difficulties. In some way, it normalizes the data.

- **Feature Extractor**

This is the biometric system's third and most essential stage. Features must be extracted in order to be identified at a later stage. A feature extractor's purpose is to characterize an object so that measurements may be used to recognize it.

- **Template Generator**

The template generator generates the templates that are used for authentication with the help of the extracted features. A template is a numeric vector or an image with discrete tracts. The source groups' characteristics are combined to create a template. Templates are saved in the database for comparison purposes and as input for the match.

- **Matcher**

A matcher is used to complete the matching step. The procured template is provided to a matcher, who compares it to the stored templates using various algorithms like Hamming distance. The results will be generated after the inputs have been matched.

- **Application Device**

It's a device that makes use of biometric system results. Some examples of application devices include the iris recognition system and the facial recognition system.

4) Operation Modes

A biometric system may be either an Identification system or a Verification system.

- **Verification**

In the verification process, the person's fingerprint is verified from the database by using matching algorithms. Also it is known as (1:1) Matching. It is the comparison of a claimant fingerprint against enroll fingerprint.

- **Identification**

In the case of the identification process, the fingerprint acquired from one person is compared with all the fingerprints stored in the database. Also it is known as (1: N) matching. It is used in the criminal investigation process.

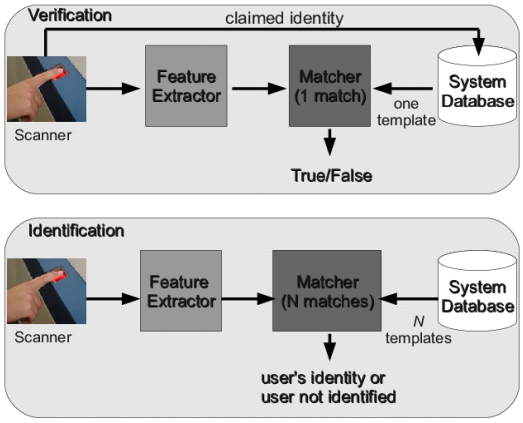

Figure 6: operation modes of biometric system

I.3.5.Unimodal and Multimodal Biometric Systems

Biometric identification systems which use a single biometric trait of the individual for identification and verification are called unimodal systems.

Biometric identification systems which use or are capable of using a combination of two or more biometric modalities to identify an individual are called multimodal biometric systems. The most important reason behind using multimodal biometric systems is to improve the recognition rate.

I.3.6.Biometric Types

There are two types of biometric measurements, namely, physiological and behavioral.

1) Physiological Identifiers

Physiological identifiers are based on the physical features of a human body and are of the following types:

- **DNA**

DNA (Deoxyribonucleic Acid) sampling is now somewhat intrusive, requiring a sample of tissue, blood, or other bodily fluid. This method of capture needs to be improved further. So far, DNA analysis hasn't been automated enough to be classified as biometric technology. The analysis of human DNA is now possible within 10 minutes. It may become more significant as technology progresses and DNA may be matched automatically in real-time. Because DNA is so well-established in crime detection, it will continue to be used in law enforcement for the foreseeable future.

- **Ear Recognition**

Ear pictures are a biometric measurement since a person's ear, anatomy does not change dramatically over time. Ears also satisfy the four essential biometric characteristics of uniqueness, permanence, collectability, and universality.

- **Iris Scanning**

The iris begins to form in the third month of pregnancy, and by the eighth month, the structures that make up its pattern are nearly complete. Its complex pattern can contain many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarets [5]. Because the iris can be seen from many meters away, iris scanning is less intrusive than retinal scanning. Iris responses to variations in light can be used as a secondary verification that the iris on display is from a living person. Another advantage is that identical twins' irises are distinct.

- **Retina**

Retina recognition uses a person's unique retinal patterns to identify them. The person must line up a series of markers that can be seen through the eyepiece. The retina is identified by the distinctiveness of the blood vessel patterns.

- **Face**

Facial recognition is the most natural means of biometric identification. The approaches to face recognition are based on the shape of facial attributes, such as eyes, eyebrows, nose, lips, chin and the relationships of these attributes. As this technique involves many facial elements; these systems have difficulty in matching face images [6].

- **Fingerprint**

A fingerprint is a ridged and furrowed pattern found on the tip of each finger. Fingerprints were used for personal identification for many centuries and the matching accuracy was very high [7]. Patterns were extracted by imprinting a fingertip on paper with ink. Compact sensors can now capture digital images of these patterns. The initial image is acquired with a live scan of the finger by direct contact with a reader device, which can also check for verifying attributes like temperature and pulse. Because the scanning device is touched by the user's finger, the surface might become oily and foggy over time, reducing the sensitivity and reliability of optical scanners. This is a traditional way of authentication that provides accuracy for currently available Fingerprint Recognition Systems.

- **Finger Geometry**

Finger geometry recognition automatically distinguishes people based on the distinctive geometric characteristics of their fingers. Finger geometry biometric systems use parameters such as finger length, fingerbreadth, finger area, and finger thickness to accomplish personal authentication.

- **Hand Geometry**

Hand geometry systems evaluate specific hand dimensions such as finger length and width. The hand is measured using a variety of methods. Mechanical or optical principles are most typically used in these procedures. Today, the latter is far more common. A person's hand geometry is utilized to identify and recognize them.

- **Vein Recognition**

Vein recognition, also known as vascular biometrics, detects parts of a person's circulatory system that are unique to them. Images of veins in the palms, eyes, and fingers are collected using optical biometric scanning technologies.

2) Behavioral Identifiers

- **Keystroke Recognition**

The keyboard is the portion of the computer that allows us to communicate with it. People utilize the keyboard in a variety of ways. Some people type quickly, while others type slowly. Typing speed is also affected by a person's mood and the time of day. Biometric keystroke recognition is a technique for identifying persons based on how they type. It's essential to consider that this technology is concerned with "how" rather than "what" is written.

- **Voice Biometrics**

Physical factors involved in making a sound, such as vocal tracts, mouth, nasal cavities, and lips, determine the characteristics of an individual's voice. These characteristics of human speech

are constant for an individual, but the behavioral part varies with age because of medical conditions and emotional state. Voice recognition techniques are generally categorized according to two approaches: 1) Automatic Speaker Verification (ASV) and 2) Automatic Speaker Identification (ASI). In a two-factor scenario, speaker verification uses speech as the authenticating property. Speaker identification makes use of a person's voice to try to figure out who they are.

- **Signature**

It is well recognized that the manner a person signs his or her name is unique to that person. The distinctive variances in human hand geometry are expressed in signatures in a simple, concrete way. Subject cooperation and the use of a writing instrument are required for collecting samples for this biometric. Signatures are a type of behavioral biometric that varies over time and is impacted by a subject's physical and emotional state. A signature recognition system may detect the pressure and velocity of the stylus point as it moves across the sensor pad, in addition to the general shape of the signed name.

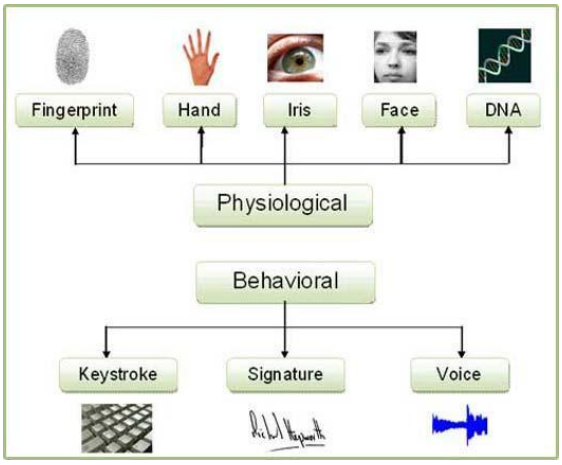

Figure 7: different biometric modalities

I.3.7.Biometric Characteristics

- **Improves System Security**

Passwords, pins, and security codes are hard to remember for some people. The biometric system eliminates the need to remember passwords. It offers different modes like retina recognition, fingerprint, or face scanner.

Additionally, the system can be used to protect sensitive data, because fingerprints can’t be forged, while passwords and pins can be stolen.

- **Maximizes Convenience**

Because it delivers authentic sign-in and sign-out data, the biometric system is a straightforward way to track each employee in an organization.

- **No Identity Theft**

Face patterns, fingerprints, iris scanning, and other biometrics are nearly hard to recreate with today's technology.

- **User Experience is Convenient and Fast**

While the internal biometric authentication processes are sophisticated, they are extremely simple and rapid for users. It's faster to put your finger on a scanner and unlock an account in a matter of seconds than it is to type out a long password with several special characters. Furthermore, most users make the error of forgetting their passwords. How likely is it that you will forget your biometrics? Never!

- **Guarantees Physical Location**

Ensures the presence of the subject at the time of authentication.

- **High-Throughput**

High throughput even during false identification or some fraud.

- **Non-transferable**

Biometric authentication necessitates the presence of the user's input at the time of permission. A physical biometric cannot be transferred or shared digitally; most biometric authentication solutions must be used with a physical application.

- **Data breaches**

Businesses and governments that collect and store users' personal data are under constant threat from hackers. Because biometric data is irreplaceable, businesses must treat it with greater caution and security - something that is both costly and technically challenging. If a password or pin has been compromised, it is always possible to change it. Physiological and behavioral biometrics, on the other hand, aren't the same.

- **No Remote Access**

In a crisis, like a security breach, HR (Human Resources) professionals cannot access the system 'remotely' to try and eliminate sensitive data, which is a major disadvantage for the system.

- **Expensive on the Pocket**

While the system is reliable and convenient, it comes at a high price. Because the biometric system is still in its infancy, the setup, integration, and hardware can be pricey, particularly for small firms.

- **False Positives and Inaccuracy**

To confirm a user's identity, the majority of conventional biometric authentication methods rely on partial information. For example, during the enrolling step, a mobile biometric device will

scan a whole fingerprint and convert it to data. Future biometric fingerprint authentication, on the other hand, will only use parts of the prints to verify identity, making it quicker and faster. In 2018, a research team from New York University created an Artificial Intelligence platform that was able to fraudulently crack fingerprint authentication at a success rate of 20% by matching similarities of partial prints to the full biometric data [8].

I.3.8.Biometric System Performance

Due to different positioning on the acquiring sensor, to environmental changes, to deformations and noise, it is impossible that two samples of the same biometric characteristic, acquired in different sessions, exactly coincide [9]; As a result, the matching is done by an algorithm that computes a similarity score and compares it to a threshold of acceptance: in case the similarity is greater than the threshold the system claims that the two samples coincide. Unlike password matching, the result of a biometric system can occasionally be wrong: the main system errors are usually measured in terms of:

1. **FRR (False Rejection Rate)** the frequency of rejections relative to people who should be correctly verified. When an authorized user is rejected he/she must represent his/her biometric characteristic to the system. Note that a false rejection does not always indicate a system error; for example, in a fingerprint-based system, wrong finger positioning on the sensor or dirtiness can result in false rejections.
2. **FAR (False Acceptance Rate)** the frequency of fraudulent accesses due to impostors claiming a false identity.

In general, FAR and FRR are inversely proportional to the acceptance threshold t, which is utilized to determine the required security level. Because FRR(t) is an increasing function and FAR(t) is a decreasing function, increasing the threshold setting to make access more difficult for impostors may make it more difficult for authorized users to acquire access.

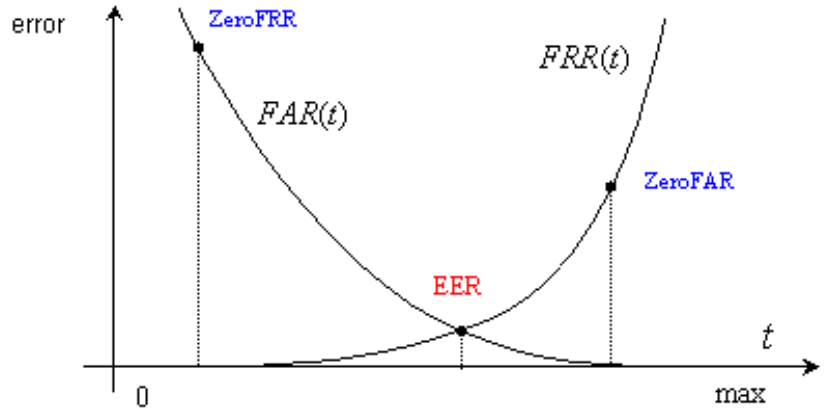

Figure 8: False acceptance rate (FAR) and false rejection rate (FRR) as functions of the threshold t [9]

Other performance indexes are commonly used to evaluate biometric systems:

- **EER (Equal Error Rate):** denotes the system error when FRR=FAR
- **Zero FAR:** denotes FRR when FAR=0
- **Zero FRR:** denotes FAR when FRR=0

I.3.9.Applications of Biometrics

Biometric systems can be used in a large number of applications. For security reasons, biometrics can help make transactions, and everyday life both safer and more practical. The following domains use biometric solutions to meet their respective needs:

- **Justice and Law Enforcement**

Biometric technology and law enforcement have a long history together, and this mutually beneficial connection has resulted in several major breakthroughs in identity management. Biometrics used by the police force nowadays is multimodal. Fingerprint, face, and voice recognition all play a crucial part in enhancing public safety and tracking down the persons we're looking for.

- **Border Control and Airport**

A key area of application for biometric technology is at the border. Biometric technology helps to automate the process of border crossing.

- **Healthcare**

In the field of healthcare, biometrics introduces an enhanced model. Medical records are among the most valuable personal documents; doctors need to be able to access them quickly, and they need to be accurate. A lack of security and good accounting can make the difference between timely and accurate diagnosis and health fraud.

- **Security**

As connectivity continues to spread around the world, it is clear that old security methods are simply, not strong enough to protect what is most important. Fortunately, biometric technology is more accessible than ever, ready to bring protection and simplicity to anything that needs to be secured, from a car door to a phone's PIN.

- **Finance**

Financial identification, verification, and authentication in commerce are among the most widely used applications of biometric technology, and they help to make banking, purchasing, and account management safer, more convenient, and responsible.

- **Mobile**

Biometric solutions for mobile devices exist at the crossroads of connectivity and identity. They use one or more biometric terms for authentication or identification, and they make use of smartphones, tablets, and other forms of handhelds, as well as wearable technologies and the Internet of Things, to provide a wide range of deployment options.

I.4.Conclusion

In this chapter, we have presented basic general information about image processing its definition, processing methodology and the applications of this field in different areas, we also highlighted in detail the biometric system step by step its definition and history we make a good description of the biometric system architecture, different modalities of biometrics and the seven main characteristics for biometric traits, we also illustrated how we can evaluate the performance of the biometric system and the main advantages and disadvantages of biometrics and finally the applications of biometric systems in our daily life.

Chapter 2
Fingerprint Recognition System

II.Chapter 2 Fingerprint Recognition System

II.1.Introduction

Nowadays, in the world of advanced digital technology, there is an increasing need for security measures that lead to the development of many biometric-based personal authentication systems. Biometrics is an emerging technique that allows us to verify the identity of an individual by using one or more of his or her personal characteristics. Its advantage is to increase the level of security by using as an identifier data that cannot be lost, stolen, or tampered with, unlike passwords or personal identification number (PIN) codes.

Among all biometrics, the fingerprint is the most commonly utilized biometric on personal identification systems. Additionally, fingerprint-based authentication is now considered one of the most secure and reliable biometric recognition techniques. The reason why fingerprint recognition is the most popular and attractive among biometric-based security systems is due to the unchanged ability and uniqueness of an individual’s fingerprints throughout their life [10].

A fingerprint is a one-of-a-kind pattern of ridges and valleys on the surface of an individual's finger. A valley is an area between two neighboring ridges, whereas a ridge is a single curved segment. Local ridge discontinuities, known as minutiae points, are divided into two types: ridge ends and bifurcations. Fingerprint classification is a method of grouping fingerprints consistently and reliably so that different impressions of the same finger are assigned to the same category.

Fingerprint recognition is an automated way of recognizing or confirming an individual's identity by comparing two fingerprints. Fingerprint recognition is used in numerous applications that include civilian and commercial applications like military, law enforcement, medicine, education, payment using ATM [11], civil service, forensics [12] driving license registration, cellular phone access, computer log-in [11].

II.2.Literature Review

Fingerprint has been used since the eighth century AD history, during China's Tang dynasty in clay to describe, served as a kind of signature in business contracts and law enforcement cases [13]. Since thousands of years ago in clay, fingerprints have been used to identify individuals. In the past, fingerprints were used to identify a person in law enforcement. Following that, fingerprints were employed in criminal investigations and forensics, it continues until now. A fingerprint is an impression made by a person’s fingertip on a surface [14]. Fingerprint is a significant biometric among other biometrics traits. The FBI and US government departments in the 1970s developed were releasing biometric recognition database [15]. For almost a century, fingerprints have been utilized for human identification in digitization applications and in forensic applications.

Karthik Nandakumar and Anil K. Jain [16] proposed a correlation-based fingerprint matcher that utilized local correlation of regions around the minutiae to estimate the degree of similarity between two fingerprint images. From the template and query fingerprint images, minutiae points

and associated ridge points were retrieved. To align the query with the template, this method used Procrustes analysis to produce a decent approximation of related ridge curves. A bank of Gabor filters in various orientations was used to enhance the two images. The quality of the minutiae match was determined using normalized cross correlation. A database consisting of fingerprint impressions of 160 users were used to evaluate this method the results show that the proposed method enhances the degree of match between two fingerprint images but it is computationally intensive.

Loris Nanni and Alessandra Lumini [17] presented a novel hybrid fingerprint matcher system based on local binary patterns. The two fingerprints were pre-aligned using the retrieved minutiae sets. To get more precise information about the local orientation and scales of the ridge lines, the images were split into numerous overlapping blocks, each of which was convolved with a bank of Gabor filters at various scales and orientations. The Local Binary Pattern (LBP) features computed as the difference between the gray value of a central pixel and the average gray value over its circular neighborhood was extracted from the convolved image. The similarity between the two LBP histograms was evaluated by their Euclidean distance the results show that the method is robust to noise and skin distortions but it is computationally expensive.

Ravi.J, K.B. Raja et [18] presented Fingerprint matching using FRMSM. Image binarization, ridge thinning, and noise removal are all used to pre-process the original fingerprint. The minutia points are matched utilizing the Minutia Score Matching technique, and for performance analysis, they considered large fingerprint database images having different patterns such as fingerprint left loop, right loop, whorl and arch. The proposed method FRMSM gives better FMR values compared to the existing method.

II.3.Fingerprint Characteristics

Fingerprint is the reproduction of the exterior appearance of the fingertip epidermis (outer skin). Ridges and valleys form the most noticeable structural characteristic of a fingerprint. A fingerprint consists of a pattern of interleaved ridges and valleys. Ridges, also called ridge lines, are dark lines and valleys are bright lines. The pattern of ridges and valleys has different characteristics for different fingerprints, the ridge structure of every fingerprint is permanent and unchanging. The ridge details are usually analyzed in a hierarchical order at three different levels which exhibit different types of features.

II.3.1.Level 1

The global ridge flow pattern (Level 1) is mainly a pattern of ridges that run smoothly in parallel, but there are regions that assume distinctive shapes characterized by frequent ridge endings and high curvature. These regions are called singular regions and can be classified into three categories, loops (core), deltas, and whorls (core). An example of the singular regions can be seen in Figure 10. The fingerprint orientation image and frequency image are also features that can be detected at the global level.

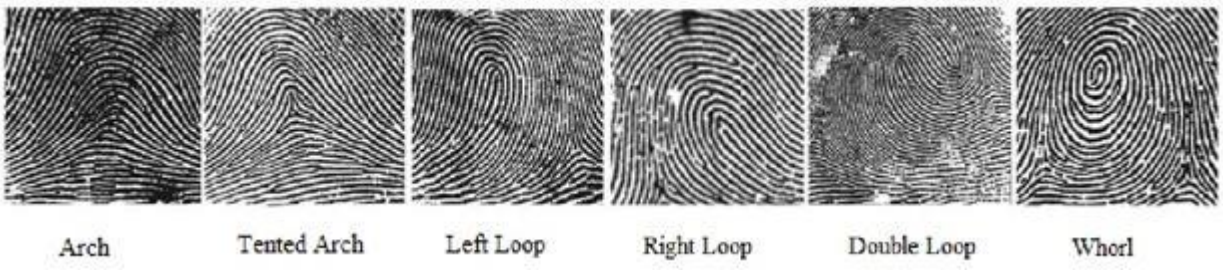

Figure 9: level 1 features

II.3.2.Level 2

Local ridge characteristics called minutiae can be found at the local level (Level 2). Minutia means small details, ridge endings and bifurcations are the two most prominent minutiae. A ridge ending is where a ridge suddenly comes to an end and a bifurcation is where a ridge divides into two ridges.

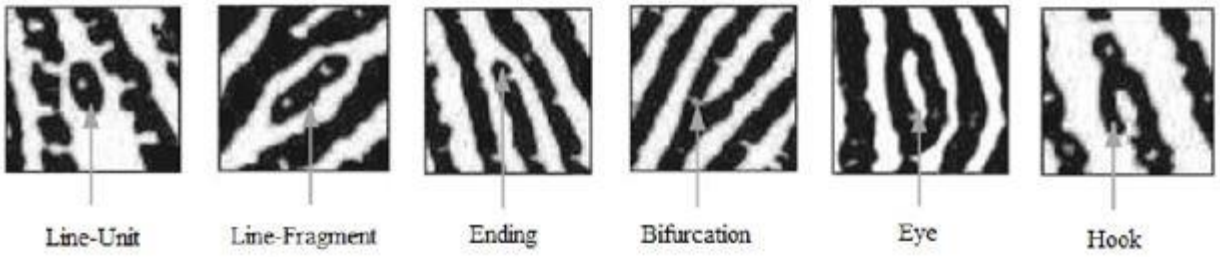

Figure 10: level 2 features

II.3.3.Level 3

The intra-ridge details detected at the very-fine level (Level 3) include width, shape, curvature, and edge contours of ridges but also incipient ridges, pores, creases, breaks, and scars. Sweat pores located at the ridges are considered the most important detail at the very-fine level. However, high-resolution fingerprint images of high quality are necessary for the extraction of details at this level.

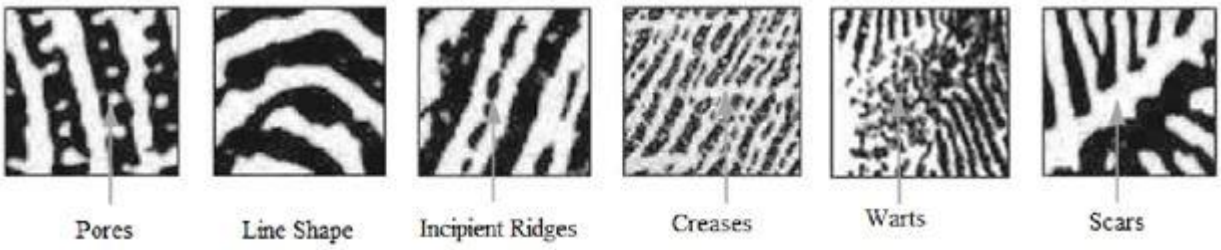

Figure 11: level 3 features

II.4.Fingerprint Classification

The first rigorous scientific study on fingerprint classification was made by Sir Francis Galton in the late 1880s [19]. Classification was introduced as a means of indexing fingerprints to speed up the search in a database. Ten years late, Edward Henry refined Galton's work and introduced the concept of fingerprint ''core'' and ''delta'' points for fingerprint classification [20]. Figure 13 shows the five most classes of the Galton–Henry classification scheme where the core and delta points and the class names are shown. Henry's classification scheme constitutes the basis for most modern classification schemes

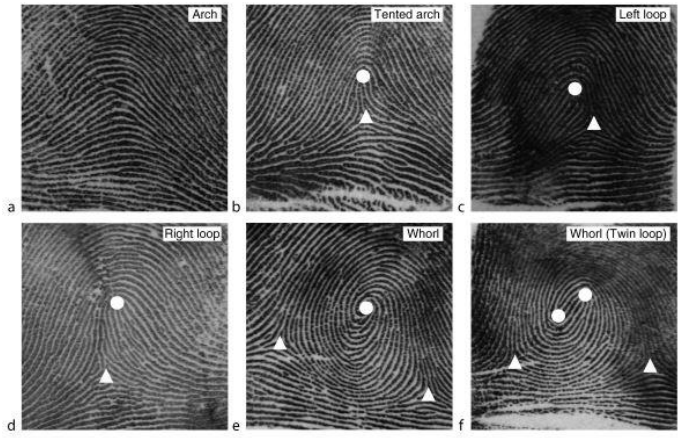

Figure 12: Under the Galton–Henry classification approach, six sample fingerprints from the five most widely used fingerprint classes (arch, tented arch, left loop, right loop, and whorl) are displayed, with two whorl fingerprints (a plain whorl and a twin loop whorl).

II.4.1.Fingerprint Classes

- **Arch:** ridges enter from one side, rise to form a small bump, and then go down to the opposite side. No loops or delta points are present Figure 13.a.
- **Tented Arch:** similar to the arch except that at least one ridge has high curvature, thus one core and one delta points Figure 13.b.
- **Left Loop:** one or more ridges enter from one side, curve back, and go out the same side they entered. Core and delta are present Figure 13.c.
- **Right Loop:** same as the left loop, but different direction Figure 13.d.
- **Whorl:** contains at least one ridge that makes a complete 360-degree path around the center of the fingerprint Figure 13.e.

II.5.Applications

- **Mobile Authentication:** Users verify their identity via fingerprint scan to access a mobile device or application.
- **Civil Identity Systems:** Governments use fingerprint recognition to verify civilian identities for voting, benefits disbursements, and border security.

- **Large-scale Automated Fingerprint Imaging Systems (AFIS):** are generally used by law enforcement.
- **Physical Access Control:** Employers and businesses use fingerprints for time and attendance and to manage facilities access.
- **Onboarding:** Organizations use fingerprint recognition for the identification of prospective customers and employees to prevent fraud.
- **Identity management:** Organizations use fingerprint recognition to prevent duplicate or false identities.

II.6.Fingerprint Acquisition

II.6.1.Optical Scanners

The early fingerprint scanners were optical scanners. These scanners use CCD or CMOS image sensors to capture the fingerprint's optical picture, as the name implies. These are comparable to camera sensors, however unlike a typical camera, they are built to take high-contrast images. The sensor consists of an array of LEDs that the CCD/CMOS sensors capture light up the finger's areas and the reflected light waves. The sensor is packed with a high density of diodes to get a detailed image of the fingerprint. The acquired image is a two-dimensional representation of the scanned fingerprint. The most recent models have dimensions as small as 1mm and can even scan damp fingers. As the costs are gradually falling, optical-capacitive hybrid scanners capable of detecting live finger are trending.

Figure 13: Optical scanner

II.6.2.Capacitive Scanners

To read a fingerprint, capacitive scanners employ completely different technology. It detects capacitance between finger ridges and valleys for capacitor plates using an array of hundreds of tiny capacitors. The distance between the ridge and the capacitor plate is narrow everywhere there is a ridge, resulting in slightly less capacitance. With an air gap in between, the distance between the valley and the capacitor plate is bigger. As a result, the capacitance increases. With the use of analog-to-digital converters, the capacitance from each capacitor in the array is

transmitted to the operational amplifier and recorded. This produces a digital scan of the fingerprint according to the capacitive touch sensing.

Figure 14: Capacitive scanner

II.6.3.Ultrasonic Scanners

Ultrasonic scanners are the most advanced fingerprint scanners on the market, capable of making 3D scans of fingerprints. At the moment, only a few high-end smartphones incorporate this technology. There are several ultrasonic transmitters and receivers in an ultrasonic scanner. The transmitters send out ultrasonic pulses, which are reflected in the fingerprint's ridges, valleys, and pores. The reflected pulses are detected by an array of receivers. The receivers are essentially sensors that use the strength of reflected ultrasonic pulses at various places to calculate mechanical stress. This creates a 3D map of the fingerprint scan, which must be more detailed than any capacitive scanner's 2D scan.

Figure 15: Ultrasonic scanner

II.7.Fingerprint Matching Techniques

There are various approaches of fingerprint matching which are classified basically into three families

II.7.1.Correlation-Based Matching

In this approach, two fingerprints are placed on top of each other and the correlation among the corresponding pixels is matched for various alignments (different displacement and rotations). The principal disadvantage of correlation-based matching is its computational complexity. Moreover, it requires an accurate position of the recording point and is affected by non-linear distortion.

II.7.2.Minutiae-Based Matching

This approach is the most common and used method, minutiae are extracted from two fingerprint images and stored as point sets in the 2- dimensional plane. Minutiae-based matching mainly consists of gaining alignment between template and input minutiae sets which leads to the greatest number of minutiae pairs [21].

II.7.3.Pattern-Based (Image-Based) Matching

This approach compares the basic fingerprint patterns (whorl, arch, and loop) between a candidate's fingerprint and the pre-stored template, which needs the fingerprint images to be aligned in the same direction. The employed algorithm detects a central point in the image for this reason. The template in the pattern-based matching algorithm contains the size, type, and orientation of the patterns in the alignment fingerprint image. The template image is compared graphically with the candidate to define the similarity degree.

II.8.Fingerprint Recognition System

II.8.1.Definition

Fingerprint Recognition System (FRS) is a biometric system that recognizes a person based on his or her fingerprint. This system is utilized for the purposes of identification and verification. The user whose impression is to be identified or verified; his/her fingerprint is enrolled onto the fingerprint scanner by putting a fingertip on the scanner and the scanner produces a digital representation of the same and then it is compared with the Database templates and thus the user is identified or verified.

II.8.2.Architecture

FRS consists of two stages: enrollment and authentication. In the enrollment stage, the fingerprint image is captured by the device and after preprocessing; its features are extracted and

stored in the database as a template. In the authentication stage, the initial same stages are applied and the features extracted are matched with the template and the score is found to have personal authentication.

FRS runs either as an identification or verification system depending on the use case.

Verification: The fingerprint of a person is checked against a database using matching algorithms throughout the verification process. (1:1) Matching is another name for it. It is the comparison of a claimant's fingerprint with that of an enrollee.

Identification: The fingerprint obtained from one person is compared to all of the fingerprints stored in the database throughout the identification process. It's also referred to as (1:N) matching. It is employed in the criminal investigation procedure.

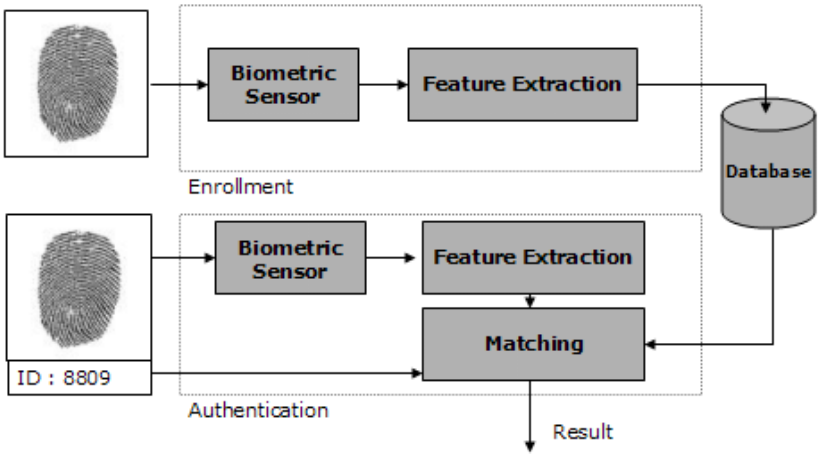

Figure 16: general architecture of fingerprint recognition system

II.9.Recognition Process

II.9.1.Image Acquisition

The Image Acquisition stage involves obtaining images in a variety of ways. Fingerprint images can be captured in two ways: online and offline. The optical fingerprint reader is used to capture the image of a fingerprint in online fingerprint identification. Offline fingerprint identification is accomplished by applying ink to the finger's surface, then placing a sheet of white paper over the fingerprint, and then scanning the paper to generate a digital image.

II.9.2.Image Pre-processing

The pre-processing stage is the process of removing unwanted data in the fingerprint image such as noise, reflection .etc. The fingerprint image pre-processing is used to increase the clarity of ridge structure. There are many steps for doing this process

1) Image Enhancement

In this stage fingerprint image is enhanced using Contextual filtering methods such as Gabor Filtering. Finger impressions must be enhanced since the ridges may be sliced or damaged, and adjacent ridges may seem united due to excessive finger pressure on the sensor.

2) Binarization

The majority of minutiae extraction methods work with binary images with only two levels of interest: black pixels representing ridges and white pixels representing valleys. The process of converting a greyscale image to a binary image is known as binarization. This increases the contrast between the ridges and valleys in a fingerprint image, making minutiae extraction easier.

II.9.3.Feature Extraction

The feature extraction process of the fingerprint image is applied on the output of pre-processing stage. The process of feature extraction divided into two steps

1) Thinning

In this stage thinning operation is performed on binary image to create a skeletonised version of the binary image. Thinning is a morphological procedure in which the foreground pixels in a binary image are gradually eroded until they are one pixel wide.

2) Minutiae Marking

The Crossing Number (CN) concept is the most often used way of minutiae extraction. The skeleton image is used in this method, and the ridge flow pattern is eight-connected. The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3×3 window. The CN value, which is half the sum of the differences between pairs of adjacent pixels in the eight-neighborhood, is next computed.

II.9.4.Post Processing (Remove False Minutiae)

Noisy or spurious minutiae may appear or generated by the subsystem. Spurious minutiae or noisy is the problem for matching minutiae. For any spurious or noisy that rises up with ridgeline on object will be removed or corrected from the fingerprint surface.

II.9.5.Matching

The process of comparing the acquired feature to the database template is known as the matching stage. In other words, the matching stage calculates the degree of similarity between an input test image (for the user to establish his or her identity) and a database training image (the template which created at the time of enrolment).

It is not difficult to match high-quality fingerprints with tiny intra-class differences, and any reasonable algorithm can accomplish it. The real challenge is matching samples (sometimes very poor quality) affected by:

- **High displacement and/or rotation**

Finger displacement and rotation often cause part of the fingerprint area to fall outside the sensor's "field of view," resulting in a smaller overlap between the template and the input fingerprints. This problem is particularly serious for small-area sensors. In a fingerprint image scanned at 500 dpi, a finger displacement of merely 2 mm (invisible to the user) leads in a translation of around 40 pixels.

- **Non-linear distortion**

The act of sensing translates a finger's three-dimensional shape onto the sensor's two-dimensional surface. This results in a non-linear distortion in successive acquisitions of the same finger due to skin plasticity.

- **Different pressure and skin condition**

If the ridges of the part of the finger being scanned were in uniform contact with the sensor surface, the ridge structure of the finger would be accurately captured. However, finger pressure, dryness of the 60 D. Maltoni skin, skin disease, sweat, dirt, grease, and humidity in the air all confound the situation, resulting in a non-uniform contact.

- **Feature extraction errors**

The feature extraction algorithms are imperfect and often introduce measurement errors. For example, the minutiae extraction procedure in low-quality fingerprint images may introduce a high number of spurious minutiae and may not be able to detect all of the actual minutiae.

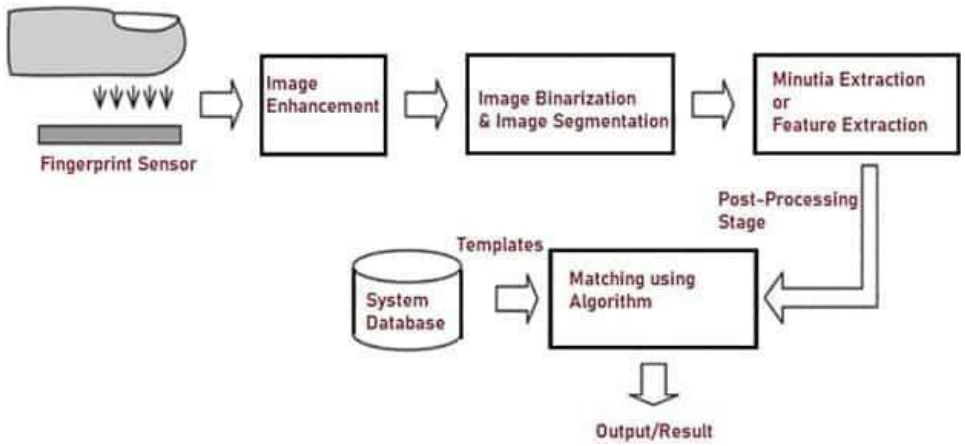

Figure 17: main process of fingerprint recognition system

II.10.Conclusion

This chapter introduced the basic techniques for fingerprints recognition a preview was made on the fingerprint features and classification, we show the principle architecture of FRS, and different techniques for fingerprint matching that exist in the literature, the applications and uses of that system and we highlighted on the previous studies of fingerprint recognition systems and their performance we have noticed that many academics, scholars, students, and development institutions are working hard to develop new or improve existing algorithms and approaches to improve the accuracy and speed of fingerprint recognition.

Chapter 3
Proposed Fingerprint Recognition System

III.Chapter 3 Proposed Fingerprint Recognition System

III.1.Introduction

Fingerprint recognition is a branch of biometrics most widespread, both in the field of public and private security, fingerprint recognition systems are used in several applications for example: securing access to a computer. In the field of anti-criminal, police forces use fingerprints as a means for the identification of a person for more than 100 years.

The principle of fingerprint recognition consists of comparing one fingerprint provided to the system to one or more other fingerprints also called “Template” or signatures, the biometric system returns a positive result in case the fingerprint provided at the input corresponds to one of the Templates, and a negative result in the opposite case

In this chapter we would like to present an overview of the different modules of our algorithm that we used to implement the fingerprint recognition system, starting with preprocessing module that used to enhance the fingerprint image and increase the clarity of ridges, then the feature extraction module that extracts the minutiae points of the fingerprint and finally the matching module that matches two fingerprints based on their set of minutiae points.

III.2.System Architecture

III.2.1.Load Image

An example of the fingerprint to be identified is given by the following figure. This image is loaded in Matlab using the imread(101_1.tif) command.

Figure 18: 101_1 fingerprint image

III.2.2.Preprocessing

1) Normalization

Normalization is used to standardize the intensity values in fingerprint image by adjusting the range of grey-level values so that it lies within a desired range of values. It normalizes the intensity values of the image so that the ridge regions have zero mean, unit standard deviation.

Figure 19: Normalized Image

2) Ridge Segmentation

Segmentation is the process of separating the foreground regions in the image from the background regions. In the fingerprint image the foreground regions correspond to the fingerprint area containing the ridges and valleys, which is our area of interest and the background corresponds to the regions outside the borders of the fingerprint area, which do not contain any valid fingerprint information. It breaks the image up into blocks of size W x W and evaluates the standard deviation in each region. If the standard deviation is above the threshold it is deemed part of the fingerprint.

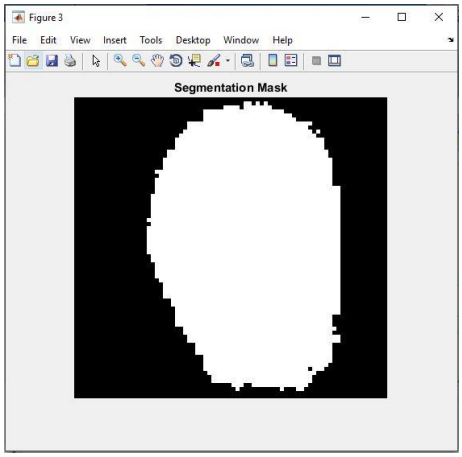

Figure 20: Segmentation Mask

3) Ridge Orientation

Estimates local orientation of ridges, an image is divided into a set of WxW non-overlapping blocks and a single local ridge orientation is defined for each block.

4) Ridge Frequency

Estimate the fingerprint ridge frequency across a fingerprint image. This is done by considering blocks WxW of the image and determining a ridge count within each block.

5) Apply Gabor Filter

Enhances the fingerprint image via Gabor filters based on ridge orientation and ridge frequency.

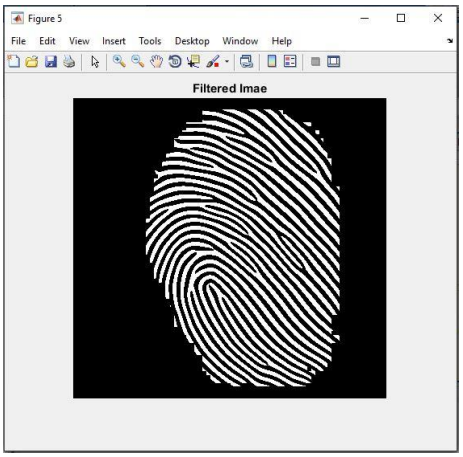

Figure 21: Filtred Image

6) Binarization

Most minutiae extraction algorithms operate on binary images where there are only two levels of interest: the black pixels that represent ridges, and the white pixels that represent valleys. Binarization is the process that converts a grey level image into a binary image. This improves the contrast between the ridges and valleys in a fingerprint image, and consequently facilitates the extraction of minutiae. In this stage grayscale fingerprint image is converted into a binary image using a global threshold [22].

The Binarization process involves examining the grey-level value of each pixel in the enhanced image and if the value is greater than the global threshold, then the pixel value is set to a binary value one; otherwise, it is set to zero. The outcome is a binary image containing two levels of information, the foreground ridges and the background valleys.

Let I (x, y) represent the intensity value of the enhanced grayscale image at pixel position (x, y). Let Tp be the threshold value. In the case of fingerprint images Tp represents the differentiating intensity between the background pixels and ridge pixels. BW(x, y) represent the binary image obtained by the equation

$$BW(x,y) = \begin{cases} 1 & if\ I(x,y) \geq T_p \\ 0 & Otherwise \end{cases}$$

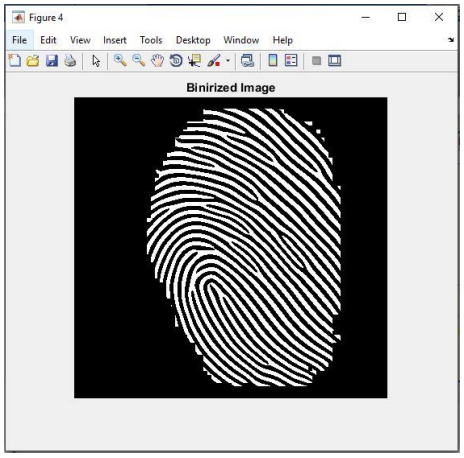

Figure 22: Binarised Image

III.2.3.Feature Extraction

1) Thinning

In this stage thinning operation is performed on binary image to create a skeletonised version of the binary image. Thinning is a morphological operation that successively erodes away the foreground pixels in binary image until they are one pixel wide [23]. A standard thinning algorithm is employed, which performs the thinning operation using two subiterations. This algorithm is accessible in MATLAB via the 'thin' operation under the bwmorph function [23]. The skeleton image is then used in the subsequent extraction of minutiae.

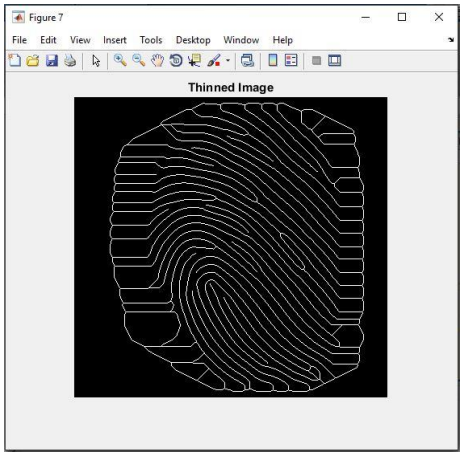

Figure 23: Thinned Image

2) Minutiae Detection

The most commonly employed method of minutiae extraction is the Crossing Number (CN) concept. This method involves the use of the skeleton image where the ridge flow pattern is eight-connected. The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3×3 window. The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighborhood. According to Rutovitz the CN for a ridge pixel P is given by: [24] [25]

$$CN = \frac{1}{2}\sum_{i=1}^{8} |P_i - P_{i-1}|, \quad P_9 = P_1$$

Where Pi is the pixel value in the neighborhood of P. For a pixel P, its eight neighboring pixels are scanned in an anti-clockwise direction as follows:

P4	P3	P2
P5	P	P1
P6	P7	P8

Table 2: 3×3 window for searching minutiae

After the CN for a ridge pixel has been computed, the pixel can then be classified according to the property of its CN value. Using the properties of the CN as shown in Table 2, the ridge pixel can then be classified as a ridge ending, bifurcation or non-minutiae point. For example, a ridge pixel with a CN of one corresponds to a ridge ending, and a CN of three corresponds to a bifurcation.

CN	property
0	Isolated point
1	Ridge ending point
2	Continining ridge point
3	Bifurcation point
4	Crossing point

Table 3: Properties of Crossing Number

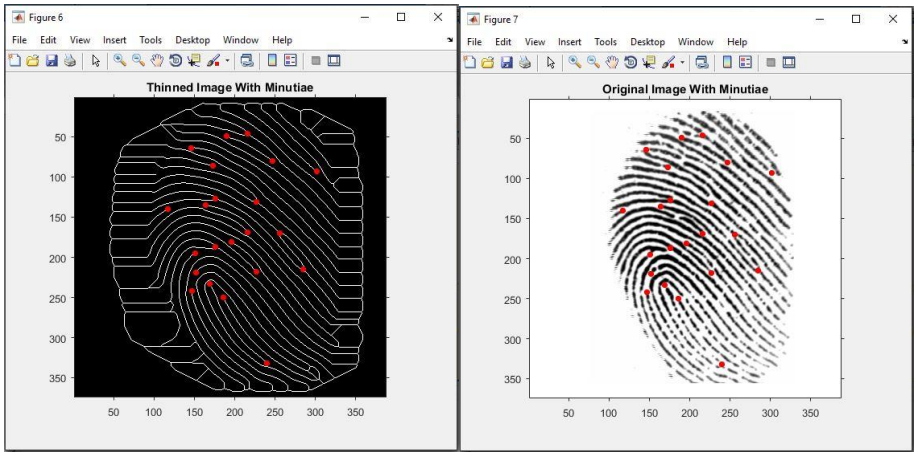

Figure 24: Minutiae Points

III.2.4.Matching

Let T and I be the representation of the template and input fingerprint, respectively. Each minutia is considered as a triplet m = {x, y, θ} that indicates the x, y minutia location coordinates and the minutia angle θ:

T = {m1, m2, m3 ….. mm}, mi= {xi, yi, θi}, i=1,2…m I = {m′1, m′2, m′3 ….. m′n}, m′j= {x′j, y′j, θ′j}, j=1,2…n where m and n denote the number of minutiae in T and I, respectively. A minutia m′j in I and a minutia mi in T are considered “matching”, if the spatial distance (sd) between them is smaller than a given tolerance r0 and the direction difference (dd) between them is smaller than an angular tolerance θ0 [26].

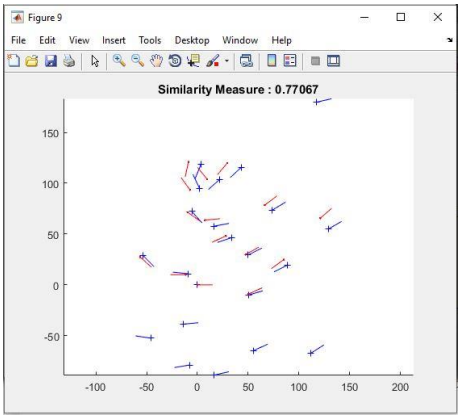

Figure 25: Similarity Measure between 101_1 and 101_2 fingerprint images

III.3.Conclusion

This chapter was an overview of the algorithm implemented in the fingerprint recognition system and its different modules as preprocessing where we used different image processing techniques to enhance the fingerprint image like normalization, binarization and thinning that facilitate the extraction of minutiae points using the crossing number concept then the matching to decide if two fingerprints are matched or not.

Chapter 4
Tests and Results

IV.Chapter 4 Tests and Results

IV.1.Introduction

In the previews chapter, the modules of our fingerprint recognition algorithm have been implemented and discussed, during which several methods of image processing are used to help in the extraction of features.

In this chapter, we will present the experimental results collected during our work. We will describe the different fingerprint databases. These databases are used in the FVC2002 (Fingerprint Verification Competition), and the environment that we worked on. Afterward, the different evaluation criteria used for the validation of the classification results are given. Then, several experiments are conducted to study the effect of the initial parameters on the identification system performances. Finally, the results obtained are presented with a set of different categories of properties. These results allow us to measure the performance of our approach.

IV.2.Work Environment

In order to carry out this project a Lenovo computer with the following characteristics was made available to us

- Processor: intel(R) core(TM) i3-4005U CPU @ 1.70GHz
- Ram: 8 GB
- Hard disk: 500 GB
- Os: windows 10

We used during the development of our work Matlab 2016a, and the Matlab programing language to implement our algorithm.

IV.3.Database FVC 2002

FVC Databases Four international Fingerprint Verification Competitions (FVC) have been organized in 2000, 2002, 2004, and 2006 [27]. For each competition, four databases were acquired using three different sensors and the SFinGe synthetic generator [28]. Each database has 110 fingers (150 in FVC2006) with 8 impressions per finger (12 in FVC2006), resulting in 880 impressions (1,800 in FVC2006). In the four competitions, the SFinGe synthetic generator was tuned to simulate the main perturbations introduced in the acquisition of the three real databases.

In FVC2002, the acquisition conditions were the same for each Database, interleaved acquisition of different fingers to maximize differences in finger placement, no care was taken in assuring a minimum quality of the fingerprints, and the sensors were not periodically cleaned. During some sessions, individuals were asked to exaggerate displacement or rotation and to have their fingers dried or moistened.

Four different databases (DB1, DB2, DB3 and DB4) were collected by using the following sensors/technologies:

- DB1: optical sensor "TouchView II" by Identix [29].
- DB2: optical sensor "FX2000" by Biometrika.
- DB3: capacitive sensor "100 SC" by Precise Biometrics.
- DB4: synthetic fingerprint generation.

Each database encloses 110 fingers wide (w) and 8 impressions per finger deep (d) (880 fingerprints in all); fingers from 101 to 110 (set B) have been made available to the participants to allow parameter tuning before the submission of the algorithms; the benchmark is then constituted by fingers numbered from 1 to 100 (set A).

	Sensor type	Image size	Set A(w*d)	Set A(w*d)	resolution
DB1	Optical Sensor	388x374 (142 Kpixels)	100x8	10x8	500 dpi
DB2	Optical Sensor	296x560 (162 Kpixels)	100x8	10x8	569 dpi
DB3	Capacitive Sensor	300x300 (88 Kpixels)	100x8	10x8	500 dpi
DB4	SFinGe v2.51	288x384 (108 Kpixels)	100x8	10x8	about 500 dpi

The following figure shows a sample image from each database:

Figure 26: sample images from each database

IV.4.Recognition

IV.4.1.Used Functions

- **Load database:** we have 80 enrolled fingerprints of DB1 database in our system database.
- **Load fingerprint image:** fingerprint image of the person to be identified for this test is 103_1 from DB1 database.

```
1
2 -    load('db.mat');
3 -    finger_print=imread('103_1.tif');
4
```

Figure 27: load database and fingerprint image

- **Enhance image:** enhance fingerprint image function

```
42
43 -    [ binim, mask, cimg, cimg2, orient_img, orient_img_m ] = f_enhance(img);
44
```

Figure 28: image enhancement function

- **Extract features:** extract fingerprint features function and return minutiae points.

```
5
6 -    f_minutiae=ext_finger(finger_print,1);
7
```

Figure 29: extract fingerprint features function

- **Matching:** matching fingerprints function
- **Identification:** identification base on threshold of 0.48

```
6
7 -    threeshold=0.48;
8 -    identified=0;
9 -    tic
10 -   for i=1:80
11 -       if(match(f_minutiae,ff{i})>=threeshold)
12 -           identified=1;
13 -           break;
14 -       end
15 -   end
16 -   toc
```

Figure 30: matching and identification function

The person with fingerprint 103_1 from the FVC DB1 database was identified using our system in 24.283952 seconds.

```
>> identification
 >>> enhancement done.
 >>> finding minutiae
Elapsed time is 24.283952 seconds.

>>> person identified
>>
```

Figure 31: fingerprint identification

We have tested our system using the FVC 2002 DB1 database that includes 80 fingerprint patterns for ten persons each with eight impressions, the system evaluation shows that the false matching ratio (FMR) and false non matching ratio (FNMR) are equal to 0.1929 % and 10.59 % respectively base on a threshold of 0.48 which gives us an accuracy of 94.6 %, from that we can say that the minutiae-based matching technique is good for implementing the fingerprint recognition system and our system is performing well in terms of accuracy and security.

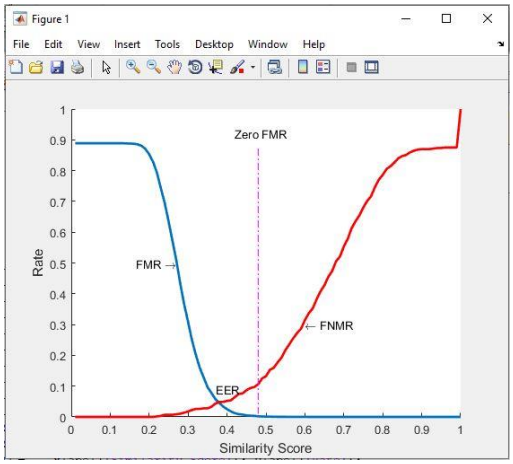

Figure 32: FMR and FNMR

IV.5.Conclusion

In this chapter, we have presented the tests carried out and the results obtained thanks to a biometric authentication system based on fingerprint minutiae. The results obtained show that the recognition rates are very encouraging and reliable. These good performances are related to the algorithms of extraction of features and the use of minutiae as a classifier.

General Conclusion

General Conclusion

Biometrics technologies are automated methods that use physiological or behavioral characteristics of an individual for verifying or recognizing the identity of a living person, it has been a very active field of research in recent years. As part of this work, we were interested in the biometric system based on the fingerprint modality in order to improve the recognition of individuals.

We start by presenting the definitions and types of images, as well as image processing methods and applications. Then, we moved on to biometrics, including their modalities, characteristics, and basic biometric system architecture.

The Fingerprint literature review and its features levels and classes are also discussed; It is followed by the structure of conventional fingerprint recognition system and different fingerprint sensors used in the market.

Then we propose an approach for implementing a fingerprint recognition system for individuals based on minutiae matching. We exhibit its different steps as preprocessing which increases the clarity of the fingerprint followed by feature extraction using the crossing number concept and matching.

The system experiments are carried out using the FVC 2002 DB1 database. The obtained results seem satisfactory regarding the similar literature.

Despite the numerous efforts dispensed to obtain such results, it still various on-going challenges and open issues that need to be considered. It is hence essential to consider more test databases, to proceed a comparative study with similar works and to extend work to other biometric features.

References

References

[1] R Suganya, *Big data in medical image processing*. Boca Raton, Fl: Crc Press, 2018.

[2] E. Du, R. Ives, A. van Nevel, and J.-H. She, "Advanced Image Processing for Defense and Security Applications," *EURASIP Journal on Advances in Signal Processing*, vol. 2010, no. 1, Mar. 2011.

[3] Biometric Technology Application Manual Volume One: Biometric Basics Compiled And Published by: National Biometric Security Project 2008.

[4] James L. Wayman in Biometrics-Now and Then: The Development of Biometrics over the Last 40 Years. New York Times article: "Technology; Recognizing the Real You" Pollack. September 24, 1981.

[5] J. Daugman, "How Iris Recognition Works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, Jan. 2004.

[6] S. Lawrence, C. L. Giles, Ah Chung Tsoi, and A. D. Back, "Face recognition: a convolutional neural-network approach," *IEEE Transactions on Neural Networks*, vol. 8, no. 1, pp. 98–113, 1997.

[7] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, A. K. Jain, "FVC2002: Fingerprint verification competition" in Proc. Int. Conf. Pattern Recognition (ICPR), Quebec City, QC, Canada, August 2002, pp. 744-747.

[8] "Machine Learning Masters the Fingerprint to Fool Biometric Systems | NYU Tandon School of Engineering," *engineering.nyu.edu*. https://engineering.nyu.edu/news/machine-learning-masters-fingerprint-fool-biometric-systems.

[9] "Biometrika - Basics of fingerprint recognition technology and biometric systems," *Biometrika.it*, 2015. http://www.biometrika.it/eng/wp_biointro.html

[10] Maltoni, D.; Maio, D.; Jain, A.K.; Prabhakar, S. Handbook of Fingerprint Recognition; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2009.

[11] S.Padma Priya, "Biometrics and Fingerprint Payment Technology," International Journal of Advanced Research in Computer Science & Technology, vol. 5, no. 1, 2017

[12] S. Li and A. C. Kot, "Fingerprint Combination for Privacy Protection," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, Feb. 2013.

[13] Glaeser, A., Sonderegger, B. and Peter, M.U. (2012) 1913-2013 the Fingerprint: 100 Years in the Service of the Swiss Confederation. Federal Department of Justice and Police, Bern.

[14] Perichappan, K.A.P. and Sasubilli, S. (2017) Accurate Fingerprint Enhancement and Identification Using Minutiae Extraction. Journal of Computer and Communications, 5, 28-38. https://doi.org/10.4236/jcc.2017.514003.

[15] Jain, A.K., Nandakumar, K. and Ross, A.A. (2011) Introduction to Biometrics. Springer, Berlin. https://doi.org/10.1007/978-0-387-77326-1.

[16] Karthik Nandakumar and Anil K. Jain ,(2004), "Local Correlation-based Fingerprint Matching", Conference proceeding of Computer Vision, Graphics and Image Processing, Kolkata, India, pp. 503-508.

[17] Loris Nanni and Alessandra Lumini, (2008), "Local binary patterns for a hybrid fingerprint matcher", Pattern Recognition 41, no.11, Pg. 3461 – 3466.

[18] Ravi.J, K.B. Raja, Venugopal.K.R, "Fingerprint Recognition using Minutia Score Matching", Vol.1(2),2009, pp.35-42

[19] Galton, F.: Finger Prints. McMillan, London (1892).

[20] Henry, E.: Classification and Uses of Finger Prints. Routledge, London (1900).

[21] Shukla, P.; Abhishek, R. Fingerprint Recognition System. Int. J. Eng. Dev. Res. 2014, 2, 3140–3150.

[22] B.N. Lavanya, K. B. Raja and K.R. Venugopal, "Minutiae Extraction in Fingerprint using Gabor Filter Enhancement," International Conference on Advances in Computing, Control and Telecommunication Technologies, IEEE, 2009.

[23] Dr. Salah M. and Dr. Feryal I. Haj Hassan, "Fingerprint Minutiae Extraction," Journal of Computing Press, vol. 2, November 2010.

[24] F. Zhao and X. Tang, "Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction," Pattern Recognition Society, Published by Elsevier Ltd, pp. 1270-1281, 2007.

[25] I. S. Virk and R. Maini, "Fingerprint Image Enhancement and Minutiae Matching in Fingerprint Verification," Journal of Computing Technologies, vol. 1, June 2012.

[26] D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar, "Handbook of Fingerprint Recognition," 2nd ed. Springer, 2003.

[27] FVC-onGoing, On-line evaluation of fingerprint recognition algorithms (2009), https://biolab. csr.unibo.it/fvcongoing.

[28] D. Maltoni, D. Maio, A. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, 2nd edn. (Springer, New York, 2009).

[29] "FVC2002 - Second International Fingerprint Verification Competition," *bias.csr.unibo.it*. http://bias.csr.unibo.it/fvc2002/databases.asp