PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
Ministry of Higher Education and Scientific Research

UNIVERSITY ECHAHID HAMMA LAKHDAR - EL OUED
FACULTY OF EXACT SCIENCES
Computer Science department

End of study memory
Presented for the Diploma of

ACADEMIC MASTER

Domain: **Mathematics and Computer Science**
Industry: **Computer Science**
Specialty: **Distributed Systems and Artificial Intelligence**

Theme

Fingerprint Based Authentication System for Exam Hall.

Presented by:
Houssna Hebbaz
Omar Benabdelkader

Sustained on 30-September-2020 from the jury:

Miss. Chourouk Guettas MA (...)	Supervisor Univ. El Oued
Mr. Messaoud Abbas MA (...)	President Univ. El Oued
Mr. Mohib eddine Khebbache MA (...)	Reporter Univ. El Oued

Academic year
2019/2020

ACKNOWLEDGEMENT

To My Parents

Who offered To me

everything …

DEDICATION

We thank Allah the Almighty, who gave us the strength and patience to do this work.

Thanks To

The special beautiful teacher Chourouk Guettas. For all the time, effort, advice, support and encouragement.

My Family Brothers and Sisters each in his own name. My friends in the room, My friends in didacticism, and everyone who encouraged *me.*

K. Houssna

Abstract

Identity identification and authentication has always been difficult, especially with the development of fraud, counterfeiting and theft operations with the progress of technology. In the field of education, validating the identity of the student is monotonous and time consuming for the invigilator and students, especially during exams. The main aim of this project is to create a smart authentication system which ensures that only authorized students are allowed to enter the exam hall without any human intervention using fingerprint scanner based on Arduino.

Key words: Fingerprint scanner, Arduino, smart system, Authentification.

الملخص

لطالما كان تحديد الهوية والمصادقة عليها صعبًا ، لا سيما مع تطور عمليات الاحتيال والتزوير والسرقة مع تقدم التكنولوجيا. في مجال التعليم ، يعتبر التحقق من هوية الطالب أمرًا رتيبًا ويستغرق وقتًا طويلاً للمراقب والطلاب ، خاصة أثناء الامتحانات. الهدف الرئيسي من هذا المشروع هو إنشاء نظام مصادقة ذكي يضمن السماح للطلاب المصرح لهم فقط بالدخول إلى قاعة الامتحان دون أي تدخل بشري باستخدام ماسح بصمات الأصابع قائم على الاردوينو.

الكلمات المفتاحية: *ماسح بصمات الأصابع ، أردوينو ، نظام ذكي ، مصادقة.*

Résume

L'identification et l'authentification d'identité ont toujours été difficiles, notamment avec le développement des opérations de fraude, de contrefaçon et de vol avec les progrès de la technologie. Dans le domaine de l'éducation, valider l'identité de l'étudiant est monotone et nécissite beaucoup de temps pour les étudiants et le surviellant, surtout pendant les examens. L'objectif principal de ce projet est de créer un système d'authentification intelligent qui garantit que seuls les étudiants autorisés sont autorisés à entrer dans la salle d'examen sans aucune intervention humaine à l'aide d'un scanner d'empreintes digitales basé sur Arduino.

Mots clés: scanner d'empreintes digitales, Arduino, système intelligent, authentification.

Contents

List of Figures

List of Tables

General introduction

Authentication was and still an important process that helps in person identification. The process of authentication is time-consuming, tedious and tiring especially in numerous population. With the progress of technology, the process of authentication has changed and developed over time.

One of the proposed solution for make authentication easy and faster without losing credibility is biometrics and its digitization. This solution isn't flawless and doesn't guarantee 100% credibility but it's still the best developed one.

At first, a biometrics-based authentication system was limited for governments (passports, police, criminal identification ...etc), after that, it was spread to other private and economical institutions.
In education, the most authentication approach applied in those systems is still identity-based authentication. However, in reality, an identity-based authentication is not enough to verify a student identity, we can take advantage of biometrics and applied it in monitoring the entry of students or checking their identities.

Our objective is to make an easy authentication system based on Fingerprint to help the invigilator in exams and reduce the consumed time. This lead us to ask a few questions, how will the system make the process easier? and how can the system fastened the process?

The importance of this study resides in the margin of nowadays technologies and the proposed algorithms in fingerprint recognition to improve the process of authentication.

In this work, we proposed a fingerprint-based examination hall authentication system. The system is designed to accept only the verified students by their fingerprint. The system consists of a fingerprint scanner connected to a microcontroller circuit. The microcontroller (Arduino) send the fingerprint image to the embedded system engine to check the validity of the fingerprint then send the results to the micro-controller.

This report will contain four chapters

- **Chapter 1:** Will contain a background of the subject and more details about our motivation.
- **Chapter 2:** Will contain other similar works and their evaluation.

- **Chapter 3:** Contain the architecture of the proposed system and some definitions of the hardware parts.
- **Chapter 4:**The last chapter will describe the implementation of the system and the obtained results.

Finally the general conclusion.

Chapter 1

An Overview for Authentication and Fingerprint-based Systems

1.1 Introduction

The idea of security is as old as humanity itself. The oldest methods of security is a simple mechanical lock whose authentication element was the key, IDs, smart cards and passwords. The main problem of this method is the possibility of losing it or forgetting it. In the 20th century, especially in recent years and with increased technology, the biometrics are becoming as the magical solution for security. They are much expanded in the various areas of our life (identification, Authentication). In this chapter we will give an overview of the authentication problem and the different proposed solutions and techniques.

1.2 The authentication problem

The authentication *"is the act of proving an assertion, such as the identity of a computer system user. In contrast with identification, the act of indicating a person or thing's identity, authentication is the process of verifying that identity. It might involve validating personal identity documents".*[httb]

Authentication plays an important role in several systems in the World. The most authentication approach applied in the past is identity- based authentication (still used). Where the person gives the identity card and the guard checks it. After the development of technology and scanning methods, it was required to find other ways to authenticate, like biometrics based solution

1.3 The Authentication system

The Authentication is the process of verifying individuals' identities. It enables a valid user to access system resources. Traditional authentication systems are knowledge-based, for example, requiring a password. There are 10 requirements for robust remote authentication based on passwords. For example, the password must not be saved on the client's device, cannot be discovered by the server and must be encrypted once transmitted on a network. Lamport in 1981 proposed the one-time password approach for remote authentication using a password table, but this has several weaknesses. For example, it can be attacked if the passwords in the password table are modified or stolen. Much research has focused on improving the efficiency and security of authentication schemes. Passwords can facilitate non-repudiation, as they can be forgotten, lost, shared, or even broken by simple dictionary attacks. Thus, it is impossible to confirm the authenticity of the claimed user. To overcome the weaknesses of knowledge-based methods, biometric patterns that are part of the person, such as fingerprints, faces and irises, are proposed as a practical solution for remote authentication systems.[Alk16]

1.4 Biometrics solution

The biometric solution is the best alternative authentication method because of its characteristics, by extracting features that are unique, the chance of any two people having the same trait will be minimum or impossible, Biometric systems work by first capturing a sample of the feature, and then transformed it using some sort of mathematical function into a biometric template. Which can then be objectively compared with other templates in order to determine the user's identity. The features can be captured from voice or iris, face, gait, or fingerprint ...etc.[Mas03]

The International Standardization Organization (ISO) defines the term biometrics, or biometric Recognition, as being "the automated recognition of individuals based on their biological and behavioral characteristics" [ISO].

The definition uses the word 'automatic' to imply the design of algorithms to be executed by a machine system to recognize individuals. The system could be assisted by a human to get better results. The 'recognition' aims to associate an identity with an individual based on some physical characteristics exhibited intrinsically by his body parts and/or some behavioural characteristics created by the body.In the literature, these characteristics are referred to as "identifiers", "traits", "indicators", or "modalities".

A biometric characteristic (or trait) **Figure 1.1** is a measurable physical or behavioral characteristic of an individual that is distinguishable. It determines how an individual is going to be recognized.

An important issue in designing a practical biometric system is to answer the question: what characteristics should the system employ to make a decision about the individual identity? Each biometric trait has its own strengths and weaknesses, the choice typically depends on the application domain and, sometimes, on the population intended to be identified. In some cases, more than one characteristics are chosen. There are some requirements that a typical biometric characteristics must fulfill:[Bel17; KJa+97]

1. **Universality:** Which means every individual using the application should reign (have) the characteristics. As an example, we can't use the signature in an environment where most of the population don't write, and we cannot use the iris characteristics to identify blind persons.

2. **Uniqueness:** The meant characteristics should be sufficiently distinct across individuals to recognize between two persons.

3. **Permanence:** The biometric characteristics should be resistant to changing in time at least with respect to the operating recognition system period. A trait that changes significantly over time is not a useful biometric.

4. **collectability:** The biometric characteristics must be quantitatively measurable to be further processed by a machine. Suitable devices connected to the machine can be used to acquire and digitize the biometric trait to be transferred later to the recognition system.

5. **Performance:** The application must ensure an acceptable degree of performance. This includes the matching accuracy/time, environmental factors that affect the

identification accuracy as well as the resources devoted to building the overall recognition system.

6. **Acceptability:** this indicates how much people that are intended to be identified using this Characteristics are willing to cooperate with the system by presenting their biometric.

7. **Circumvention:** It measures the robustness of the system; i.e. how much is easy to fool the system to make it taking wrong decision or to compromise information about the users Biometric data. It is hard to find a single biometric characteristic that fulfills all the requirements. A practical biometric system should have acceptable recognition accuracy and speed with reasonable resource requirements, harmless to the users, accepted by the intended population, and sufficiently robust to various fraudulent attacks.

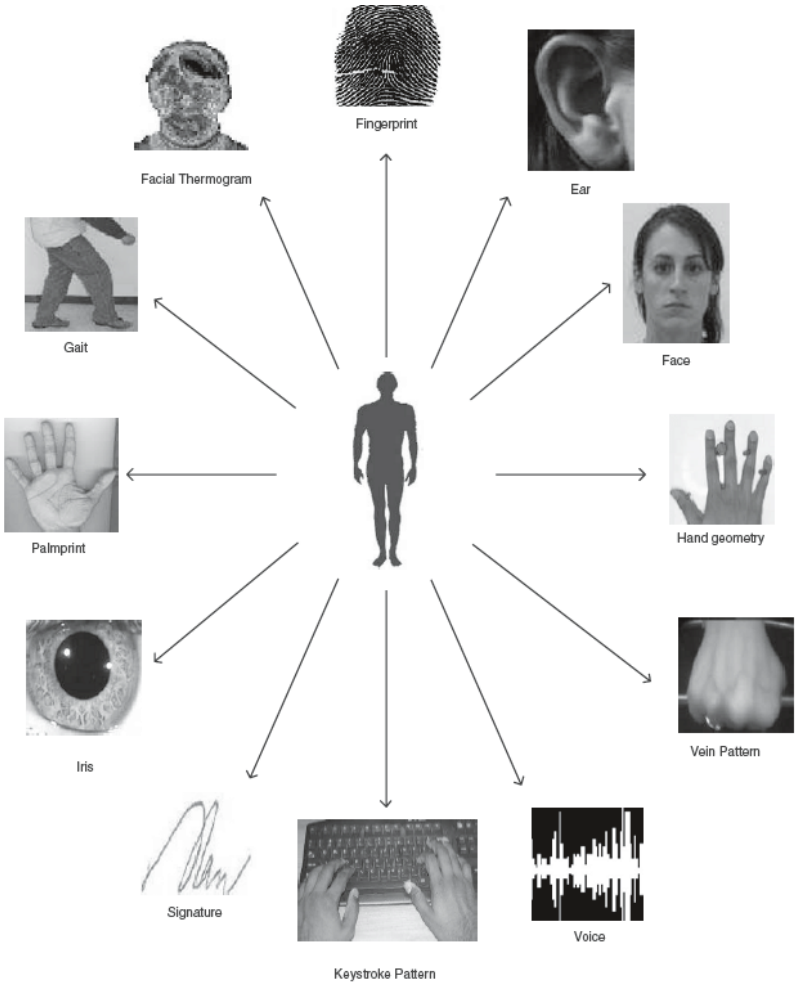


Figure 1.1: *Examples of Biometrics traits[KFA08].*

Below, we will give a description of a group of Biometrics generally used in Authentication systems:

- **Face:**
  Face recognition system is a task that human perform routinely and effortlessly in their daily lives using their memories, but it is not the case for the computers which must undergo a learning process (supervised and unsupervised) via artificially inducing codes, features so they can recognize a person. But this learning can be successfully applied only if images of individuals are given in controlled conditions (static background, neutral frontal face ...etc), which makes recognition more difficult when uncontrolled condition like varying lighting and facial expression changes are posed.

  Face recognition as one of the primary biometrics technologies, became more and more important due to the rapid advances in technologies such as digital cameras and sensors, and the increased demand on enhance security systems that are expected to identity faces present in images and videos automatically.[ZJP05; SMJ12]

- **Gait:**
  is the peculiar way one walks and is a complex spatio-temporal biometric. Gait is not supposed to be very distinctive, but is sufficiently characteristic to allow verification in some low-security application. is a behavioural biometric and may not stay invariant, especially over a large period of time, due to large fluctuations of body weight, a major shift in the body weight, major injuries involving joints or brain, or due to inebriety. Acquisition of gait is similar to acquiring facial pictures and hence it may be an acceptable biometric. Because gait-based systems use a video-sequence footage of a walking person to measure several different movements of each articulated joint, it is computing and input-intensive.[Mal+06]

- **Iris:**
  The iris is a thin circular diaphragm, which lies between the cornea and the lens of the human eye. A front-on view of the iris is shown in Figure 1.1. Formation of the iris begins during the third month of embryonic life. The unique pattern on the surface of the iris is formed during the first year of life, and pigmentation of the stroma takes place for the first few years. Formation of the unique patterns of the iris is random and not related to any genetic factors. The only characteristic that is dependent on genetics is the pigmentation of the iris, which determines its colour.

  The iris is perforated close to its Centre by a circular aperture known as the pupil. The function of the iris is to control the amount of light entering through the pupil, and the sphincter and the dilator muscles, which adjust the size of the pupil, do this. The average diameter of the iris is 12 mm, and the pupil size can vary from 10% to 80% of the iris diameter, the iris consists of a number of layers, the lowest in the epithelium layer, which contains dense pigmentation cells. The stromal layer lies above the epithelium layer and contains blood vessels, pigment cells and the two iris muscles. The density of stromal

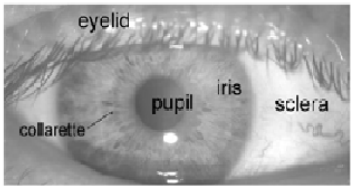


Figure 1.2: *A front-on view of the human eye.*

pigmentation determines the color of the iris. The externally visible surface of the multi-layered iris contains two zones, which often differ in color. An outer ciliary zone and an inner pupillary zone, and these two zones are divided by the collarette-which appears as a zigzag pattern.

These characteristics make it very attractive for use as a biometric for identifying individuals. Image processing techniques can be employed to extract the unique iris pattern from a digitized image of the eye, and encode it into a biometric template, which can be stored in a database. When a subject wishes to be identified by an iris recognition system, their eye is first photographed, and then a template created for their iris region. This template is then compared with the other templates stored in a database until either a matching template is found or not.

Although prototype systems had been proposed earlier, it was not until the early nineties that Cambridge researcher, John Daugman, implemented a working automated iris recognition system. The Daugman system is patented and the company Iridian Technologies now owns the rights. Even though the Daugman system is the most successful and most well-known, many other systems have been developed like Wildes system.[Mas03]

- **Voice:**
  Voice verification uses a microphone-recording device to capture a sample of a user's voiceprint. Measurements of many characteristics must be taken, including cadence, pitch, and tone. Voice verification considers a hybrid of physical and behavioral biometric types. On the physical side, the shape of your throat and larynx helps to predetermine your voiceprint. But then again, your experiences help influence such things as inflect and dialect. Besides, although difficult to do, alter their voiceprint. Additionally, it is important to make sure that the distinction between voice verification and voice recognition is understood.

  Voice recognition is a technique that can decipher words that have been spoken, and is not an authentication technique. On the other hand voice verification is simple to implement. Because most workstations come with a microphone of some sort, pre-installed, new hardware is usually not needed. It may also be implemented using current telephone systems. Voice verification has run into some opposition and has been accused of being hard to use from an end-user perspective. At times, it is difficult to enroll in the system as background noises, and static as well as the common cold can cause problems at enrollment and during verification.[GA17]

- **Fingerprint:**
  Fingerprints have certain natural traits that make them ideal for use in biometric systems. Fingerprints are unique. No two people on record have been found to have the same fingerprints. Fingerprint identification has been used for many years. Most fingerprint systems operate in authentication, rather than identification mode. Fingerprint scanning can be done in several different ways. In our study, we use fingerprint as a biometrics-based authentication system, and try to make one for Access control to the examination hall.

1.5 Fingerprint-based Authentication system

1.5.1 History

Biometric signs contain fingerprint, iris, face, gait, palm, speech, signature, etc. Among them, the fingerprint is the one that has been used for a long time. The earliest dated prints of human hands and feet were made about 4000 years ago during the pyramid-building era in Egypt. Also, one small portion of a palm print, not known to be human, has been found impressed in hardened mud at a 10,000-year-old site in Egypt. It was common practice for the Chinese to use inked fingerprint on official documents. The oldest existing documents so endorsed dated from the 3rd century BC, and it was still an effective practice until recent times. Even though it is recorded that the Chinese used their fingerprint to establish identity in courts, researchers fail to know whether the Chinese were fully aware of the uniqueness of a fingerprint or whether the physical contact with documents had some spiritual significance.

Dr. Henry Faulds probably made the greatest advances in fingerprint science in the late 19th and early 20th centuries. He became interested in fingerprint after 1874 while he was working at a hospital in Tokyo, Japan. After careful experiments and observations, he believed that superficial injury did not alter fingerprint patterns and as the injury healed fingerprints patterns returned to their former patterns. In a letter written to Nature in October 1880, be described pattern formations on the fingers and stated how good sets of fingerprints may be obtained by using "a common slate or smooth board of any kind, or a sheet of tin, spread over very thinly with printer's ink". This technique, still in use today, appears to be a botanical technique called nature-printing. His most important conclusion was: 1) Fingerprints do not change, 2) Fingermarks left on objects by bloody or greasy fingers "may lead to the scientific identification of criminals".

Sir William Herschel, an English administrator in India, commenced placing the inked palm and thumb impressions of some members of the local population on contracts. These prints were used as a form of a signature on the documents because of the high level of illiteracy in India and frequent attempts at forgery. Throughout his life, Herschel took his own fingerprints and noticed that no change had occurred in them in over 50 years. He also had a small collection of fingerprints and used his technique of hand printing to detect forgeries of legal documents. The fingerprints are taken from prisoners were also of great interest to him, and he had the opportunity to see the same prisoners fingerprinted several times over some years with no change occurring in their fingerprints. However, Herschel never claimed that he had developed a method of registering and identifying

criminals, nor did he foresee any crime scene application as Faulds had done.

In 1892, Sie Francis Galton published an accurate and in-depth study of fingerprint science, which included an attempt at fingerprint classification system to facilitate the handling of large collections of fingerprints. Although Galton's work proved to be sound and became the foundation of modern fingerprint science, his approach to classification was inadequate.

Juan Vucetich, an Argentine police officer who corresponded with Galton, devised his own fingerprint classification system, which was put into practice in September 1891. In March 1982, Vucetich opened the first fingerprint bureau at San Nicholas, Buenos Aires, Argentina. In June 1892 at Necochea, Argentina, Francisca Rojas claimed that she had been brutally attacked and a neighbor named Velasquez had murdered her two children. However, Velasquez refused to confess to the murder of two children. Nine days after the crime, a search of the crime scene was carried out and a number of fingerprints in blood were found on a doorpost of the woman's hut. To people's surprise, Vucetich's fingerprint bureau found that these fingerprints were identical with the inked fingerprints of Rojas's. When confronted with this evidence, Rojas confessed to the murder of her children, and in July 1892 she was found guilty of their murder and sentenced to life imprisonment.

Sir Edward Henry, who had been taught in fingerprint by Galton, established the famous Henry System, which is a systematic and effective method of classifying fingerprints. The classes he used are Right Loop (R), Left Loop(L), Whorl (W), Arch (A), and Tented Arch (T). Examples from each class are shown in the figure. Henry published his book classification and Uses of Fingerprints in 1900. In 1901, he was appointed as Assistant Commissioner of Police at New Scotland Yard was fully functional, and the first British court conviction by fingerprint was obtained in 1902.

Approximately 10 years after the publication of Henry's book, police forces and prison authorities throughout the English-speaking world were using his classification system.

After Galton and Henry, work on fingerprint recognition was extended and refined. In the early 20th century, fingerprints were formally used as valid signs of identity by law-enforcement agencies. However, manual fingerprint identification is tedious, time-consuming and expensive. Therefore, in 1960, the Home Office (UK) and the Paris Police Department initiated studies on the automatic fingerprint-based biometric systems.[BT04]

1.5.2 Fingerprint for Authentication Systems

Fingerprint authentication refers to the automated method of verifying a match between two human fingerprints[Rah18]. Automated fingerprint recognition technologies have been grown up to be used not only in criminals' identification but also in a wide range of applications such as control access, computer log-in, and e-commerce due to its high accuracy and acceptability as well as its low-cost technology.

The research area that is dealing with fingerprints is called dactyloscopy. It is a science of the papillary lines on the inside of human fingers. The shapes of the papillary lines, their course, and direction, are very different for every person. According to the shapes that the papillary lines create, it is possible to determine several base patterns that serve to sort all of the shapes.[MSl18]

1.5.2.1 Classifications patterns for Fingerprints

For classification of an individual fingerprint four patterns are used as a standard:[MSl18]

- **ARCH:** the papillary lines, called ridge lines often, creates simple arcs as shown in the right of **Figure 1.3** .
- **RADIAL:** the ridgelines create a loop that leads in left side. On the right side from the middle of the loop is a mark, the so-called delta. Between delta and the middle must be at least one line as shown in the left of **Figure 1.3** .

Figure 1.3: *Arch and Radial pattern.*

- **WHORL:** the ridgelines create circular, oval, spiral, two-loop shapes and contain at least two deltas with at least one line as shown in the right of **Figure 1.4** .
- **ULNAR:** the ridgelines create a loop, which leads in the right side. On the left side from the middle is the delta. Between delta and the middle must be at least one line as shown in the left of **Figure 1.4** below.

Figure 1.4: *Whorl and Ulnar pattern.*

Scientists have found that family members often share the same general fingerprint patterns, leading to the belief that these patterns are inherited.[Rah18]

1.5.2.2 Fingerprints' Acquisition and Processing

Practically, the acquisition of fingerprint images was performed by using the so-called "ink-technique": the subject's finger was spread with black ink and pressed against a paper card, the card was then scanned by using a common paper-scanner, producing the final digital image. this kind of process is referred to as off-line fingerprint acquisition or off-line sensing. A particular case of off-line sensing is the acquisition of a latent fingerprint from a crime scene. Nowadays, most systems use live-scan digital images acquired by directly sensing the finger surface with an electronic fingerprint scanner. No ink is required in this method, and all that a subject has to do is to press his/her finger against the flat surface of the live-scan scanner. the most important part of a fingerprint scanner is the sensor (or sensing element), which is the component where the fingerprint image is formed. Almost all the existing sensors belong to one of the three families: optical, solid-state, and ultrasound.[KFA08]

- **Optical sensors:**the finger touches the top side of a glass prism, but while the ridges enter in contact with the prism surface, the valleys remain at a certain distance, the left side of the prism surface is illuminated through a diffused light. the light entering the prism is reflected at the valleys, and absorbed at the ridges. the light rays exit from the right side of the prism and are focused through a lens onto a CCD or CMOS image sensor.

- **Solid-stat sensors:** also known as silicon sensors, became commercially available in the middle 1990s. All silicon-based sensors consist of an array of pixels, each pixel being a tiny sensor itself. The user external CCD/CMOS image sensors are needed. Four main effects have been proposed to convert the physical information into electrical signals: capacitive, thermal, electric field, and piezoelectric.

- **Ultrasound sensors:**Ultrasound sensing may be viewed as a kind of echography. A characteristic of sound waves is the ability to penetrate materials, giving a partial echo at each impedance change. This technology is not yet mature enough for large-scale production.

the fingerprint sensor is an important property of modern Fingerprint-based Authentication Systems (FBAS's) which generally operate in live-scan mode. The quality of the captured image is dependent on the technology used by the reader. Acquiring the fingerprint image is a key step for digital processing, the other steps are shown in the **Figure 1.5** below.

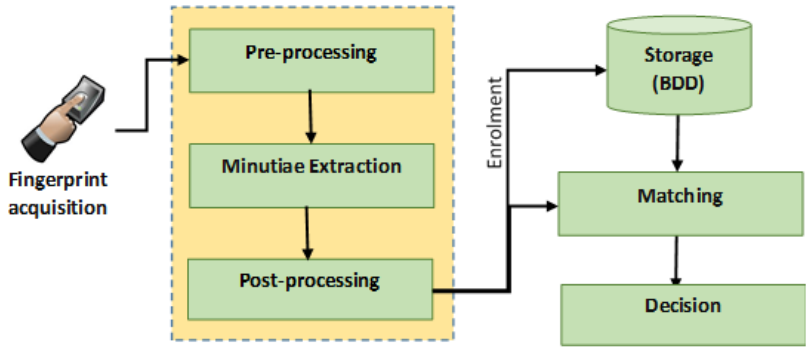


Figure 1.5: *General scheme for a Fingerprint-Based Authentication system.*

A **.Pre-processing:** Captured fingerprint images usually suffer from the irrelevant background that affects image quality and feature clarity, Especially when using ink or bad quality fingerprint sensor. Therefore, sundry pre-processing steps are desired to improve the appearance of fingerprint features and to simplify the task of minutiae extraction.

1 **.Enhancement:** A fingerprint image enhancement algorithm receives an input fingerprint image, applies a set of intermediate steps on the input image like as normalization, histogram equalization, filtering, etc, and finally outputs the enhanced image. The goal of each enhancement algorithm is to enhance the image quality of the ridge structures in the recoverable regions and weaken or eliminate the unrecoverable regions.[HWJ98]

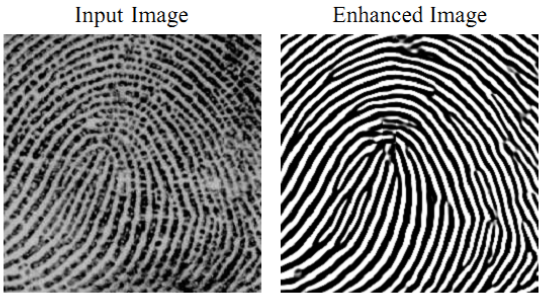


Figure 1.6: *Fingerprint image before and after enhancement.*

2 **.Segmentation:** Fingerprint segmentation refers to the process of decomposing a fingerprint image into two disjoint regions: foreground and background. The foreground consists in the useful ridge structure that constitutes the region of interest (ROI) 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. The process is of great importance to the features-extraction steps since it speeds up the recognition process and avoids the apparition of false ridges that lead to false minutiae.

Kenneth Nilsson and Josef Bigun proposed another method, they tried to use Linear Symmetry Features as a Pre-processing step[NB01]. And there are other methods as Normalization which are used to change the range of pixel intensity values and to improve the image quality (noise reducing from image), to standardize the intensity values in an image by adjusting the range of grey-level values so that it lies within the desired range of values.[MSl18]

B **.Minutiae Extraction:**or features extraction is an important and vital step in the matching process between two fingerprints, the important thing in fingerprint image is the minutiae. Minutiae are local discontinuities in the fingerprint pattern. A total of 150 different minutiae types have been identified. In practice, only ridge ending and ridge bifurcation types are used in fingerprint recognition[BBM11] . The **Figure 1.7**below shows some of these types.
Many algorithms have been developed for minutiae extraction. A fingerprint minu-

Figure 1.7: *Minutiae type.*

tiae detection algorithm is applied to extract the correct minutiae points. Various algorithms have been described in the literature. They are categorized as grayscale-based or binary-based methods[Alk16] [Wie09]. In grayscale methods, the minutiae are extracted directly from grayscale images using ridgeline following [MM97]. Conversely, in binary-based methods the minutiae are extracted not directly from grayscale images, but after Binarization, thinning, or both.

1 **.Binarization:** The task of Binarization converting a segmented fingerprint image from the grey-scale range [0, 255] to the binary range {0, 1}. '1' labels indicate ridges whereas '0' values represent valleys and background[Rah18]. A good binarization method must:

i. Improve the clarity of ridge structures of fingerprint images.
ii. Maintain their integrity.
iii. avoid the introduction of spurious structures or artefacts
iv. Retain the connectivity of the ridges while maintaining separation between ridges.

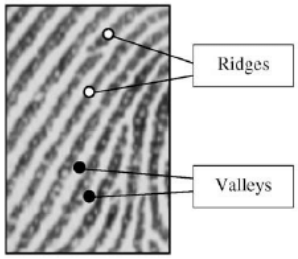


Figure 1.8: *Ridges and Valleys of a fingerprint.*

A simple and direct method to apply it is to determine a global sill (thresholds) **th** and affect the value '0' to all pixels having grey values lower than **th** and '1' to those higher.[Bel17]

$$B(x,y) = \begin{cases} 1 & \text{si } s(x,y) > th \\ 0 & \text{sinon.} \end{cases}$$

There is another way that implies dividing the image into regions that have similar grey-scale values then apply binarization to each region individually and it is said to be the best.[ZX06]

2 **.Thinning :** Thinning is a process of extracting a skeleton from an object in a digital image. A skeleton of an image can be thought of as a one-pixel thick line through the middle of an object, which preserves the topology of that object. Thinning is a morphological operation that successively erodes away the foreground pixels and is a fundamental step in many image processing and pattern recognition algorithms[KTD11]. It is generally accepted that fingerprint thinning algorithms should have the following characteristics:[XLN09]

i. Preserving the original connectivity.
ii. Obtaining the center skeleton of the original image.
iii. Thorough thinning.
iv. Keeping the skeleton intact.

3 **.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 **(Table 1.1)**. 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.

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

Table 1.1: *Pixels Neighborhood*

the CN for a ridge pixel P is given as:

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

Where P_i 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:

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 1.2**, 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.[CPP14]

CN	Property
0	Isolated Point
1	Ridge Ending Point
2	Continuing Ridge
3	Bifurcation Point
4	Crossing Point

Table 1.2: *properties of the CN*

C **.Post-processing:** after the minutiae are extracted, it is necessary to employ a post-processing stage in order to validate the minutiae. **Figure 1.9** below illustrates some examples of false minutiae structures, which include the spur, hole, triangle and spike structures. It can be seen that the spur structure generates false ridge endings, whereas both the hole and triangle structures generate false bifurcations. The spike structure creates a false bifurcation and a false ridge ending point.

The majority of the proposed approaches for image post-processing based on a series of structural rules used to eliminate spurious minutiae. For example, a ridge ending point that is connected to a bifurcation point, and is below a certain threshold distance is eliminated. However, rather than employing a different set of heuristics each time to eliminate a specific type of false minutiae, some approaches incorporate the validation of different types of minutiae into a single algorithm.[BSB11]

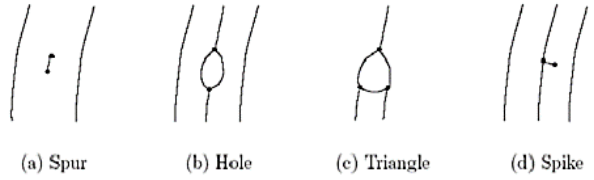


Figure 1.9: *Examples of false minutiae structures.*

D **.Matching:** A fingerprint matching algorithm compares two fingerprint images represented by their templates and return either a degree of similarity or a binary decision of matched or not matched. One template is generally stored in a database, and the other consists in the input query features, that the system has to identify. A large number of automatic fingerprint matching algorithms have been proposed. They can be coarsely classified into three families: correlation-based matching, minutiae-based matching and other features based matching:[Wan+06]

1 **.Correlation-based approach:** both templates consist of raw data (pixels) to be compared in terms of grey-levels.

2 **.Minutiae-based methods**: template features consist in minutiae. The goal is to maximize the number of paring minutiae. This approach inspires its comparison principles from the manner that the expert examiners do in manual matching.

3 **.feature-based matching:** in low-quality fingerprints, minutiae lose their reliability. In such a case, some non-minutiae features, such as pores, ridge contours, orientation field and frequency map, etc. could be used to consolidate the matching results.[Bel17]

Given a fixed set of computational resources, minutiae-based matching is considered the best, with the highest matching capability. However, there are a couple of challenges for this approach:

- Missing and spurious minutiae must be taken into consideration. In other words, the matching algorithm must accommodate points in one set that do not have a corresponding point in the other set.
- General minutiae-based matching methods are computationally expensive.
- The difficulty for minutiae-based methods is nonlinear deformations of fingerprints. If the deformations are not explicitly modelled, a perfect alignment of the point sets will not be possible. In this case, the alignment algorithm must try to find the optimal alignment according to some criteria.[Wan+06]

1.5.3 Minutia-based matching principle

Matching algorithm compares two minutiae sets: template $T = \{m_1, m_2, ..., m_j\}$ from reference fingerprint and input $Q = \{m_1, m_2, ..., m_i\}$ from the query, each

minutia is principally described in its 2D coordinates (x, y), its direction $\theta \in [0, 2\pi[$ and eventually its type t(bifurcation or ending).

A minutia $m_i^t(x_i^t, y_i^t, \theta_i^t)$ in T is said to be in matching with a minutia $m_i^q(x_i^q, y_i^q, \theta_i^q)$ in Q if:

$$\begin{cases} ED(m_i^t, m_j^q) = \sqrt{(x_i^t - x_j^q)^2 + (y_i^t - y_j^q)^2} \leq th_{ed} \\ \lambda(m_i^t, m_j^q) = min(|\theta_i^t - \theta_j^q|, 2\pi - |\theta_i^t - \theta_j^q|) \leq th_\theta \end{cases}$$

ED (.,.) represents the Euclidean distance between two points and $\lambda(.,.)$ Is their minimal directional difference. The thresholds th_{ed} and th_θ are tolerance boxes introduced to substitute for the deformations caused by the non-linear skin-distortion and displacements errors introduced by the features extraction algorithm.
The alignment of the two fingerprints can be recovered by finding the parameters of the translation Δx and Δy as well as the rotation angle α (scaling factor is supposed to be 1). Since there is a large number of such transformations, the adequate parameters can be determined by transforming the minutiae of Q in the coordinate system of T and selecting those parameters that optimize the distance between T and the transformed Q. Formally, let

$$\tilde{Q} = \left\{ \ \tilde{m}_j^q(\tilde{x}_j^q, \tilde{y}_j^q, \tilde{\theta}_j^q) \ \right\}_{j=1,N}$$

be the transformed template Q using the parameters Δx, Δy and α

$$\begin{cases} \begin{bmatrix} \tilde{x}_j^q \\ \tilde{y}_j^q \end{bmatrix} = \begin{bmatrix} \cos(\alpha) \sin(\alpha) \\ -\sin(\alpha) \cos(\alpha) \end{bmatrix} \begin{bmatrix} x_j^q \\ y_j^q \end{bmatrix} + \begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix} \\ \tilde{\theta}_j^q = \theta_j^q + \alpha \end{cases}$$

Hence, we define a Boolean function align to designate that a minutia m_i^t from T is aligned with a minutia m_i^q from Q :

$$aling(m_i^t, \tilde{m}_j^q) = \begin{cases} 1 & if(ED(m_i^t, \tilde{m}_j^q) \leq th_{ed} \text{) and } \lambda(m_i^t, \tilde{m}_j^q) \leq th_\theta \\ 0 & otherwise \end{cases}$$

The optimal transformation values $\tilde{\Delta x}$,$\tilde{\Delta y}$, and $\tilde{\theta}$ correspond to the parameters that maximize the alignment of the two sets T and $\tilde{Q}$:

$$Maximize_{\Delta x, \Delta y, \alpha}(\sum_{i=1}^{N} Align(m_i^t, \tilde{m}_{Im(i)}^q))$$

to:

$$\forall i = 1 \cdots M, K = 1 \cdots M, i \neq K \Rightarrow Im(i) \neq IM(K) or Im(i) = IM(K) = Null.$$

where Im(.) is a pairing (mapping) function that associates to each minutia index in T an index in $\tilde{Q}$ (so in Q). The pairing is subject to the conditions that each minutia in T must be paired at most with one or no minutiae in Q and vice versa.

The matching problem is not as easy as it just has been viewed, the determination of the optimal parameters is a hard problem that must be undertaken carefully. In fact, once a minutia m_T is paired with m_Q according to a certain transformations does not mean that the two minutiae are true pairs since the decision was taken based only on the minutiae features independently of its local context. Since the relative transformation between two fingerprints is unknown in advance, the correspondence between minutiae is very ambiguous and each minutia of one fingerprint can be matched to any minutiae of the other fingerprint. To let the matching be more reliable, additional local information, called minutia descriptor, are added to describe each minutiae-based on which the comparison is achieved.[Bel17]

1.6 Conclusion

In this chapter, we briefly presented the Authentication system between past and present, its evolution and the latest used technologies. In the next chapter, we will describe the Biometrics technology and how we can use it in the Authentication system especially physical Biometrics characteristics.

Chapter 2

Literature Review

2.1 Introduction

The existing of an automatic Authentication system for exam Hall is necessary. Because of, the Cheating accidents, identity theft, also to facilitate the invigilation process for the professors.

In this chapter we will discuss some related works, trying to demonstrate the points that others failed to cover and the strong points in those systems. Explaining the differences between them, and what will our system include eventually.

2.2 Fingerprints analysis techniques for Authentication systems

Biometrics is one of the most proficient authentication techniques. It provide a method to validate the identity to enhance the protection from any misleading actions. It can be used for personal authentication. Due to its security-associated applications currently, biometrics is the subject of intense research by academic and private institutions. However, each trait has its specific challenges and particular issues. Though various biometric techniques have certain concerns, fingerprint is accepted by many researchers because fingerprint recognition systems have received a great of interest due to its easiness and efficiency in identity authentication. It provides a powerful tool for access control, security and real-world applications. Fingerprints are the most common and trusted biometrics for individual identification or authentication. There are two types of systems that help automatically establish the identity of a person: 1) authentication (verification) systems and 2) identification systems. In authentication systems, a person desired to be identified submits an identity claim to the system, and the system either accepts or rejects the submitted claim of identity (Am I who I claim I am?). In an identification system, the system establishes a subject's identity (or fails if the subject is not enrolled in the system database) without the subject's having to claim an identity (Who am I?).

2.3 related works

Each researcher took one of the techniques and tried to improve it based on previous works where many automated Authentication systems were developed. They adopted different ways to determine the goal, each of those researches worked to determine the image characteristics achieve the best scores an accurate fingerprint features sensing. Another thing that was debated is the quality of the photos, those images may be not Clear because of the quality of the sensor, or the properties of the skin (sweat and grease). Without forgetting to try to ameliorate the quality of security (More secure) and make the system as fast as possible. Besides, collect the technology for making a full system based on fingerprint for example exam hall through the sensors and designing a control system.

As we know several systems and projects are built for Authentication. Where they used many techniques, Whether it is a complete system or part of a system. Those systems

can be categorized into :

- Software-based systems.
- Hardware-based systems.

2.3.1 Software-based systems:

when we say software-based systems, we mean the way use to analyze the fingerprint, for example, enhance the photo, The methodology used to determine the characteristics extracted for conformity (matching) ...etc.
Many methods have appeared in the literature over the years. the most popular algorithm for enhancing fingerprint images is Hong enhance algorithm, Hong And her team try to combine a range of technologies to enhance fingerprint images. First, normalize the input fingerprint image. second, estimate the orientation of the fingerprint image. third, computing the frequency image from the normalized input fingerprint image and the estimated orientation image.
Fourthly, Region mask estimation by classifying each block in the normalized input fingerprint image into a recoverable or an unrecoverable block and the last one is filtering by Gabor filter, they obtained a good result [HWJ98].
After improving photo quality some researchers try to reduce the time of the thinning process, In 1986 T. Y. ZHANG and C. Y. SUEN are among the first Who present work in this field, the algorithm aims to remove the boundary and corner points of the digital patterns. endpoints and pixel connectivity are preserved. Each pattern is thinned down to a "skeleton" of unitary thickness [TC84]. experimental results show that this method is very effective but in specific patterns, and the fingerprint image is not one of the test patterns.
With the appearance of the Artificial neural networks and their models, Dacheng Xu, Bailiang Li and Anton Nijholt proposed a PCNN template-based method for binary fingerprint image thinning[XLN09], here we can see this algorithm is time-consuming but giving a good result special for fingerprint image and promote the robustness of the minutiae extraction algorithm, where the famous one is Crossing Number concept (CN). In the paper of Feng Zhao and Xiaoou Tang Where used this method to extract fingerprint minutiae using some techniques to improve the system[ZT06], this method helped facilitating the further study of the statistics of fingerprints. On the opposite side, we can see another way to extract the minutiae.
In 1997 Dario Maio and Davide Maltoni suggested a method to extract directly from the image without any pre-processing by following the ridgelines on the grey-scale image, by "sailing" according to the fingerprint directional image[MM97]. but if we compare between both we find the CN concept produce false points (false minutiae) where we need to create something (method or algorithm) to remove them, here where Marius Tico and Pauli Kuosmanen proposed an algorithm operates onto the thinned binary image of the fingerprint, to eliminate the false minutiae, The proposed algorithm can detect and cancel the minutiae associated with most of the false minutia structures which may be encountered in the thinned fingerprint image[TK00].
furthermore, in the previous work where it was talked about CN concept(Feng Zhao and

Xiaoou Tang work), they also try to reduce the number of the false minutiae set according to some heuristic rules[ZT06]. In the last, matching methods are used to compute the similarity of two image after extracting the points of minutiae (bifurcation and end ridge) by calculating the euclidean distance between each two minutiae (template and query)[Par04].
The implementation of minutiae based fingerprint identification system using the crossing number concept by Atul S. Chaudhari, Girish K. Patnaik, Sandip S. Patil where builte a process for fingerprint recognition passing through normalaize the fingerprint input, after that segmentation, enhancement and binirization and all of that called preprocessing. next step called minutiae extraction where thinning the enhance picture and detect the minutiaes. at last enrolled the results of minutiae extraction in the database to use it for matching or, use it for identification with another image stored in the database.[CPP14]

the matching process does not guarantee a complete and comprehensive match in every cases, Rather, it provides approximate results in all cases, and a perfect match rarely occurs. some times the matching process accept the imposter users and refuse the genuine users but scarcely and this called false accpte rate (FAR) and false reject rate (FRR) respectively, all of that comes back to the image, detection and extraction method, the false minutiae and the matching method itself.[htte]

$$FAR = \frac{imposterscoresexceedingthreshold}{allimposterscore}$$

$$FRR = \frac{genuinescoresfallingbelowthreshold}{allgenuinescore}$$

The concept of threshold is coming to illustrate the matching score between two fingerprint image, when we say this two-finger is matching that means the results of matching (matching score) super or equal a threshold.[JRR09]

$$Matchingscore = \frac{MatchingMinutiae}{Max(NT, NI)}$$

Where, NT and NI represent the total number of minutiae in the template and query matrices respectively. By this definition,Matching Minutiae represent the number of minutiae matching, the matching score takes on a value between 0 and 1. Matching score of 1 and 0 indicates that data matches perfectly and data is completely mismatched respectively.

The threshold is determined by obtaining the best matching result when trying different thresholds, As [KJa+97] did, when choose 10 as threshold obtained a 90.24% as accuracy rate, choose 8 as threshold obtained a 92.68% as accuracy rate, and when choose 7 obtained a 93.76% as accuracy rate.

$$Accuracy(\%) = \frac{(100 - (FAR + FRR))}{2}$$

2.3.2 Hardware-based systems:

Here, when we say hardware-based systems we mean the various components used to build a full authentication system, in the literature's, Some researchers have tried to combine different techniques to find satisfactory solutions. Most works agreed on one set of devices with the increase or decrease of some devices, as described below:

- Arduino on different models (Mega, Uno, Yun): to link the different cut of the system and use his IDE to compile the code.
- Liquid Crystal Display (LCD or TFT Touch Shield LCD colour): to communicate with the user.
- real-time clock (RTC) module: is used to obtain the current time, date and day for the fingerprint reader.
- Fingerprint scanner (ZFM20, R307, R305); to read the fingerprint.
- SD card: to store the fingerprint images (database).
- Buzzer or LED: to notify the user whether or not the fingerprint has been authenticated.
- Servo Moter: to open the door if the authentication is right.

These parts are often used to build and design of a low-cost biometric fingerprint system and subsequent implementation of this system in practice. Therefore Martin Magdin and al created a system that is capable of recognizing fingerprints from a user and then processing them, they developed a mobile application to control it and the authentication part build by Arduino [MSl18]. Many problems can be solved such as students' attendance as happened in Malaysia they designed and developed a portable classroom attendance system based on Arduino and fingerprint(**Figure 2.1** below), The Portable Attendance System was enabled with a security mechanism to protect the data from being tampered by the student. It uses a cryptographic technique that substitutes substituting each letter of the alphabet with the letter which is a number of places further from that alphabet [Zai+14].in addition to building an attendance system by fingerprint identification to manage the fingerprints data by centralizing the identification process that is done in each fingerprint sensor[Muc+17], or to solve the problem of door lock by integrating the hardware(Arduino, servo motor, ...etc) with the door as Subhankar Chattoraj and Karan Vishwakarma [CV16].
At last, In Jordan proposed a novel secure fingerprint-based authentication system for student's examination system, the main purpose of the study is to control and manage the attendance procedure of students in the examination classroom. Therefore, a web application (by PHP) pages have been developed to manage the system and the authentication with Arduino over the ethernet card[AAZ19].
Managing authentication using fingerprints ensures integrity, accelerates the process, decreases error rate and fastens the verification process, where in [AAZ19], they revealed that the needed time for students' attendance verification using the manual process is

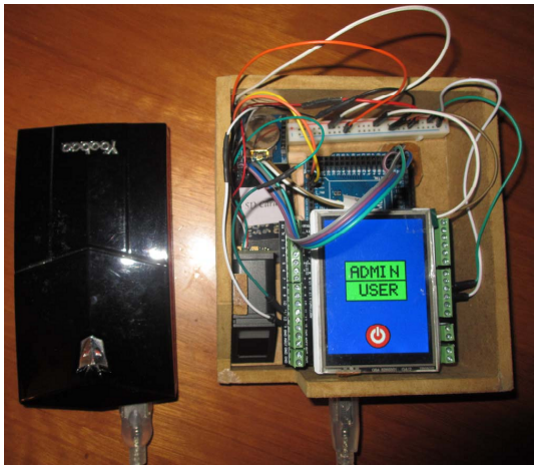


Figure 2.1: *Malaysia portable classroom attendance system[Zai+14].*

23.66 second per student, more than 6.65 second using fingerprints.

All of these previous systems based on Arduino and used its libraries. The cost of this technology is very economical, low cost off the shelf components and is based on the Arduino platform which is FOSS (Free Open Source Software), where any person can design and developed his own system.

The table below classifies existing systems, trying to present for each the database used, year, time or success rate, average error rate and the method used.
These works are classified based on their technology used and chronological order:

Table 2.1: *Similar systems.*

N	**Year**	**Method used**	**DB used**	**Time or Success Rate**	**Average Error Rate**
Software					
1	1998	Enhancement [HWJ98]	MSU (700 live-scan, 10 per individual)	2.49(s)	/
2	1984	Thinning [TC84] [XLN09]	B and Chinese character	0.505(s)	/
3	2009		FVC 2004	75.0269(s)	/
4	1997	Detection [MM97] [ZT06]	NIST and FBI sample set	2.22(s)	34.55%
5	2007		Their own Database	/	27.5%
6	2000	[TK00]	DB of Biometric System Lab Italy	/	

N	Year	Method used	DB used	Time or Success Rate	Average Error Rate
7	1997	Matching [Par04] [CPP14] [KJa+97]	NIST 9	92.68%	
8	2004		Biometric System Laboratory, University of Bologna	75%	/
9	2014		FVC 2000 (DB1 and DB2) and FVC 2002 (DB1 and DB2)	99.885%	/
Hardware					
10	2013	Arduino usage [AAZ19] [Muc+17] [MSl18]	Their Own Database	83.3%	/
11	2017		Their Own Database	98.875%	/
12	2019		Their Own Database	98%	/

In all the previous work we can see that work on hardware only or in software only, by trying to improve some former algorithms in time or the results, besides, to Integration of various electronic parts and sensing devices to build a full system.

So we will try to blend these two parts to create a system that can recognize fingerprints by enhancing the software and the hardware parts as we will introduce it int the next two chapters.

2.4 Conclusion

In this chapter, we presented an overview of the most important methods used to analyze fingerprints, as well as some effective systems based on fingerprint. We also categorized similar works to represent their methods and approaches to show their results and try to criticize them.
In the next chapter, we will describe the general architecture of our system, the used methods and approaches.

Chapter 3

System Architecture

3.1 Introduction

The design phase is a critical step in deciding the technical choices. In this chapter, we will propose an architecture of an integrated system with two parts; hardware and software, explain in details the interrelation between them and the role of each module of our system.

3.2 Architecture

To identify the system and the way it works, we are going through Architecture of the different parts that create the system.

3.2.1 Fingerprint system:

It is the system that links the interface, the fingerprint sensor, and the database management system to carry out the above operations. **Figure3.1** explains how the system works.

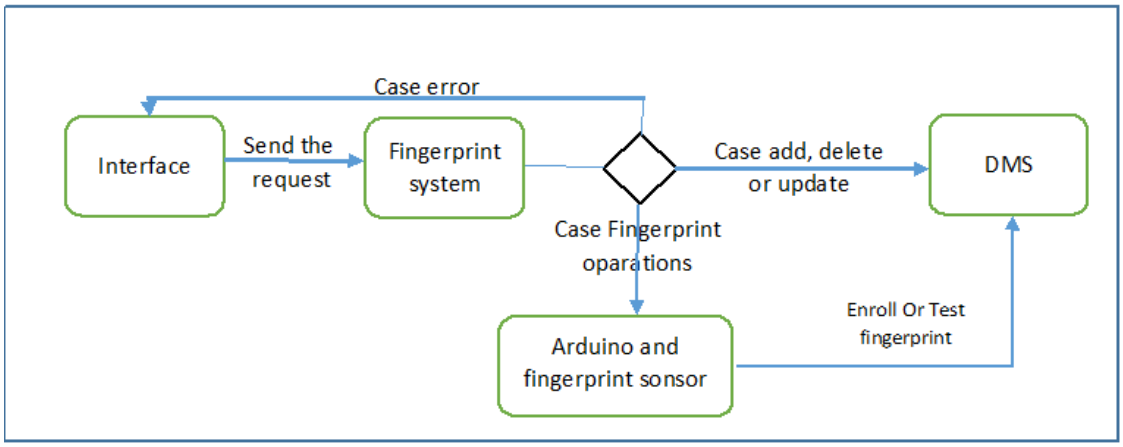


Figure 3.1: *General Architecture of the Fingerprint System.*

3.2.2 User System

The following diagrams, **Figure3.2** and **Figure3.3** represent the general architecture in which the system operates.

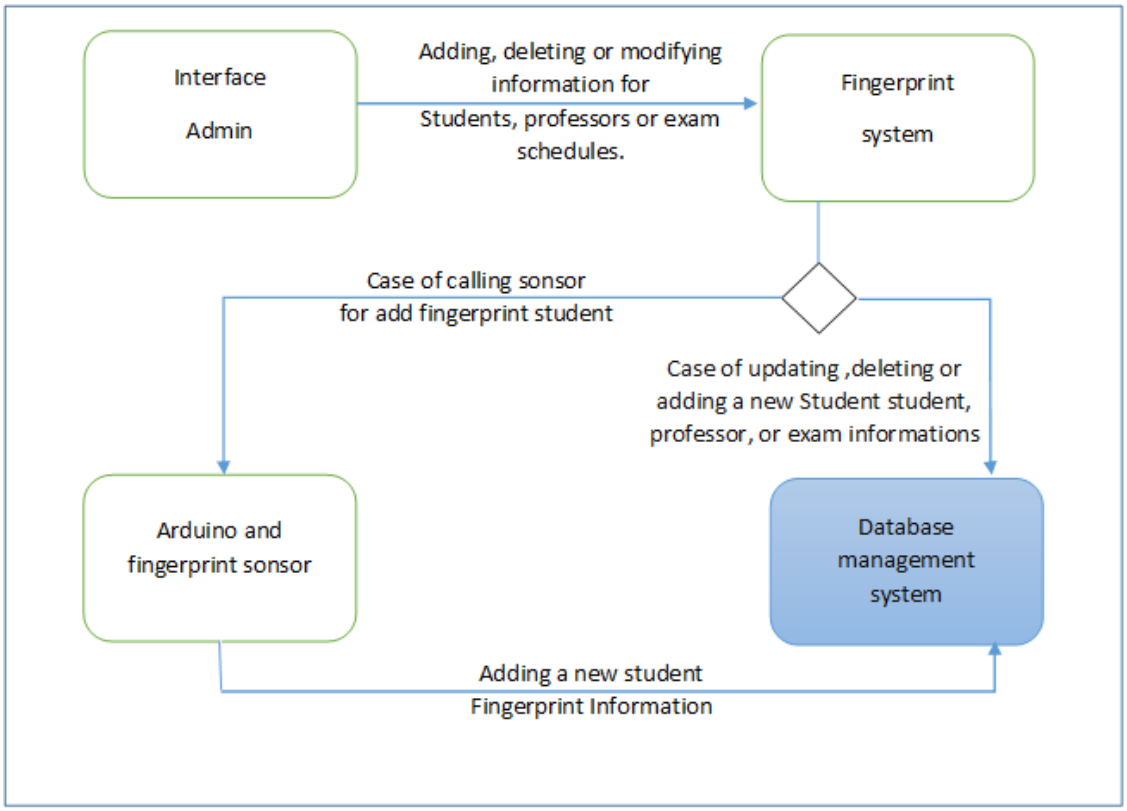


Figure 3.2: *General Architecture for Admin.*

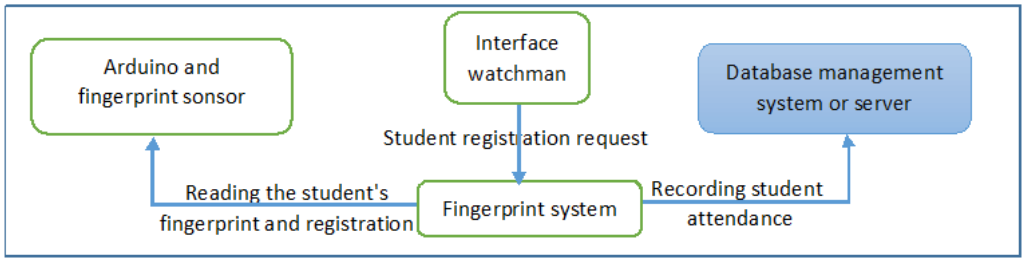


Figure 3.3: *General Architecture for Invigilator.*

Users' roles:

It is the way the user interacts with the database. There are two types of users: the invigilator and the universal controller. **Table3.1** represents the operations that can be performed by each one of them.

Admin	Invigilator
Add a student, professor or test schedule	Registration of attending students
Add a group of students or professors (scheduled)	Edit account information
Delete student, professor schedule or test	
Modify student, professor information or exam schedule	
Convicted student management	
Edit account information	

Table 3.1: *Options of Admin and Invigilator.*

Database management system:

It is the executor of system requests and responsibilities for running the database and carrying out operations on it.

Arduino and fingerprint sensor:

Is responsible for reading the fingerprint information and entering it into the system.

3.3 Fingerprint System Work

For registering a fingerprint in our database, we proposed the following process to do that. The fingerprint authentication process goes through several stages. The following diagram (**Figure 3.4**) explains the path we took to enroll or test fingerprints.

3.3.1 Enhancement

the strategies of enhancement come from trying to improve the quality of the fingerprint picture by making its features more clearly. Fingerprint image contains two features valleys and ridge, the valleys produce the background with white color, The ridge is in the foreground with black color, In our proposed method, we use Hong algorithm for enhancing fingerprint image, this algorithm takes a fingerprint image to normalize it to reduce the variations in grey level values along ridges and valleys, which facilitates the subsequent processing steps after that orientation image estimation and frequency image estimation, at last region mask and filtering. The (**Figure 3.5**). Illustrates the results of applying the algorithm.

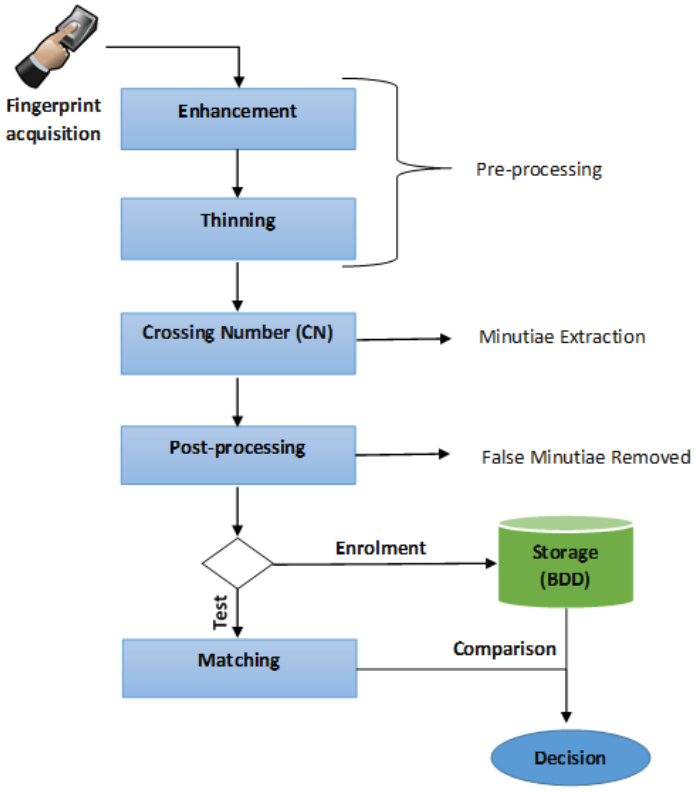


Figure 3.4: *The General Architecture for Proposed system.*

(a) Before Enhancement

(b) After Enhancement

Figure 3.5: *Enhancement Result*

3.3.2 Thinning

The process of thinning making the ridge in fingerprint image one pixel. we chose to use Zhang and Suen algorithm for thinning, this algorithm don't take too much time compared to another, So they take as input binary fingerprint image and try to reduce the number of pixel in each ridge the result in the (**Figure 3.6**) below.

(a) Binary Image

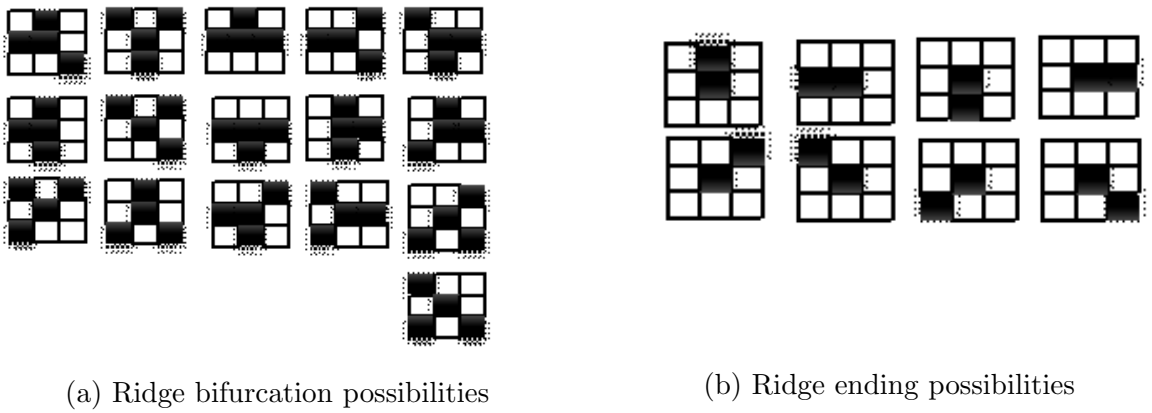
(b) Image Thin

Figure 3.6: *Thinning Result*

3.3.3 Crossing Number (CN) Concept

To compare two images we need to find The same thing in both. In fingerprint image we need to find the minutiae the ridge ending and the ridge bifurcation. The most used method to detect and extract the minutiae. The crossing number concept inserts a binary thinned picture and a table containing the minutiae is output like we illustrate in chapter 1. We noticed that method treating all the pixels of the fingerprint images and consume time especially in image Contain a lot of pixels.

Our proposed method is to reduce the time of the CN by skipping the pixel that does not contain a minutiae (ridge ending and ridge bifurcation), we can see all possibilities of ridge ending and ridge bifurcation in the **Figure 3.7** below:



(a) Ridge bifurcation possibilities

(b) Ridge ending possibilities

Figure 3.7: *binary representation of Ridge endings and bifurcation (The black pixel (square) means 0 and the white means 1).*

By calculating the frequency of zero in the blocks of all the possibilities of minutiae, the results numbers are multiples of two. Therefore, when executing our improved CN, it skips all blocks where the sum of zeros isn't a multiple of two.

3.3.4 Post-processing

The method that detects and extracts the minutiae, it leaves a set of false minutiae that should be ignored. There is a common characteristic of these false minutiae, they are very close to each other. So we use the proposed method in [CW16] to ignore the false minutiae.

- Rule 1: if the distance between a termination and a bifurcation is smaller than D1, then these two minutiae could be false minutiae. We should remove these two minutiae. Experimentally, D1 is set to 10.

- Rule 2: if the distance between two terminations is smaller than D2, then these two minutiae could be false minutiae. We should remove these two minutiae. Experimentally, D2 is set to 6.

- Rule 3: if the distance between two bifurcations is smaller than D3, then these two minutiae could be false minutiae. We should remove these two minutiae. Experimentally, D3 is set to 6.

3.3.5 Enrollment

in this step, the system stores the data extracted from the fingerprint picture after enhancing it, thinning, minutiae extracting and removing the false one to compare it with another one.

3.3.6 Test, Matching and Decision

To compare two enrolled fingerprint images, we used the Minutia-based matching method which compares the distances between extracted minutiae and its orientation to the one stored in the database after that it computed the matching score.

3.4 Protection and encryption

The information of students, professors, and exams is very sensitive and must be perfectly secured and this is to prevent any outside interferences. We have encrypted the data and this is to protect the information in the event that the database is compromised. We propose an encryption algorithm is shown below.

```
fonction Encryption(word:chaîne de caractère):
Variables
        n,i,key1,key2 : entiers
        w : chaîne de caractère
Début:
        n <- Longueur(word)
        key1 <- order_en_ASCII(word[0])
        key2 <- order_en_ASCII(word[n-1])
        w <- caractère(order_en_ASCII(word[n-1])+key1)
        pour i <- 1 à n-1 faire:
                si(i mod 2 = 0) alors:
                        w <- w + caractère(order_en_ASCII(word[i])+key1)
                sinon:
                        w <- w + caractère(order_en_ASCII(word[i])+key2)
                fin_si
        fin_pour

        w <- w + caractère(order_en_ASCII(word[0])+key2)
        w <- w + caractère(key1)
        w <- w + caractère(key2)

        Encryption <- w //return w
Fin
```

(a) Encryption function

```
fonction Decryption(word:chaîne de caractère):
Variables
        n,i,key1,key2 : entiers
        w : chaîne de caractère
Début:
        n <- Longueur(word)
        key1 <- order_en_ASCII(word[n-2])
        key2 <- order_en_ASCII(word[n-1])
        w <- caractère(order_en_ASCII(word[n-3])-key2)
        pour i <- 1 à n-3 faire:
                si(i mod 2 = 0) alors:
                        w <- w + caractère(order_en_ASCII(word[i])-key1)
                sinon:
                        w <- w + caractère(order_en_ASCII(word[i])-key2)
                fin_si
        fin_pour

        w <- w + caractère(order_en_ASCII(word[0])-key1)

        Decryption <- w //return w
Fin
```

(b) Decryption function

Figure 3.8: *Encryption and Decryption Function*

3.5 Database schema

In order for the system to be integrated, we conducted an in-depth study of all aspects of the system. The database diagram is presented in the **Figure 3.9**.

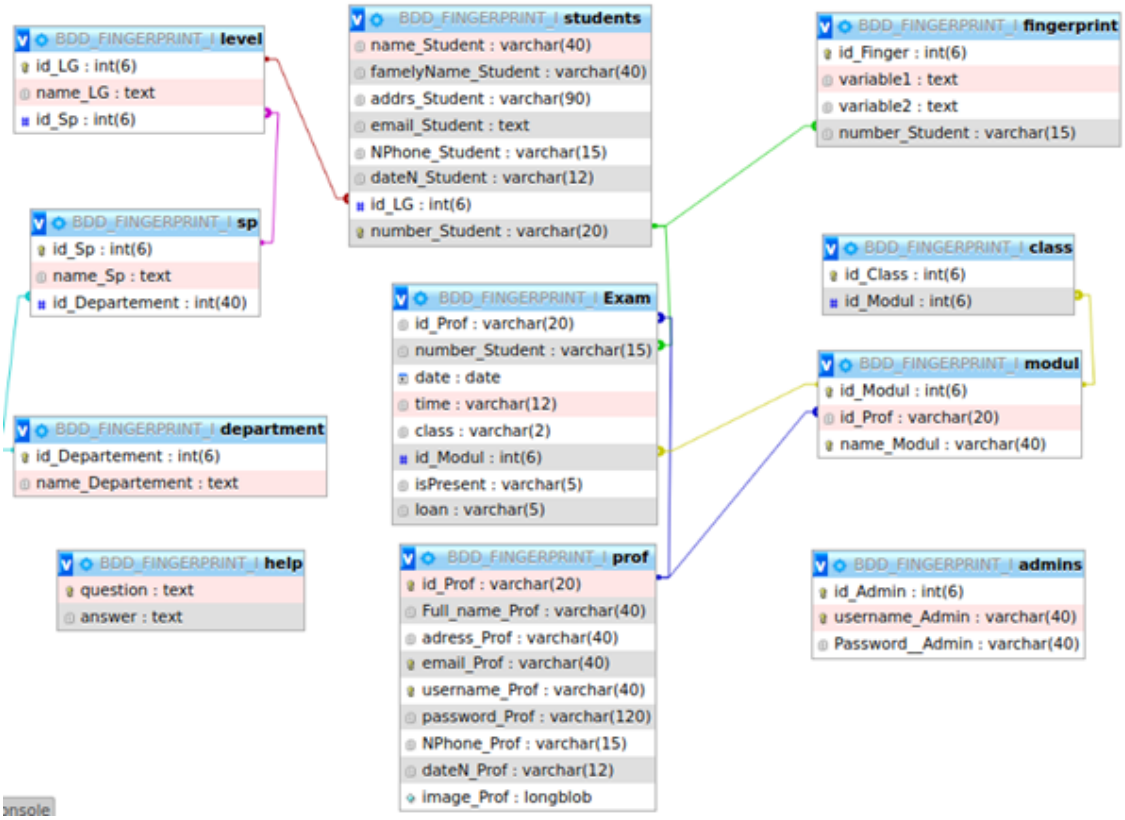


Figure 3.9: *Database schema.*

3.6 Conclusion

In this chapter, we presented how our system works and its different components, diagrams, and key algorithms along with the relations between all the different parts of the system. In the next chapter, we will provided definitions of the languages and the working environment we used to realize this system, its implementation and the final results.

Chapter 4

Implementation and Results

4.1 Introduction

In this chapter we are going to define the objectives and requirements of the project. Besides of that we are going to define and explain most of the hardware and software we are using in this project. Along with a description of the algorithms implementation and the obtained results, followed with a discussion.

Requirements

The minimum requirements for this project are:

- knowledge in C programming language.
- Knowledge in Python programming language.
- Arduino Kit.
- Knowledge in electronics.
- database knowledge.
- Internet connection.
- A Computer.

4.2 Definitions

4.2.1 Python:

Python is a high-level programming language designed to be easy to read and simple to implement. It is open-source, which means it is free to use, even for commercial applications. Python can run on Mac, Windows, and Unix systems and has also been ported to Java and .NET virtual machines.

Python is considered a scripting language, like Ruby or Perl and is often used for creating Web applications and dynamic Web content. It is also supported by a number of 2D and 3D imaging programs, enabling users to create custom plug-ins and extensions with Python. Examples of applications that support a Python API include GIMP, Inkscape, Blender, and Autodesk Maya.

Scripts written in Python (.PY files) can be parsed and run immediately. They can also be saved as a compiled programs (.PYC files), which are often used as programming modules that can be referenced by other Python programs.[httf]

4.2.2 Qt Designer :

Qt Designer is the Qt tool for designing and building graphical user interfaces (GUIs) with Qt Widgets. You can compose and customize your windows or dialogs in a what-you-see-is-what-you-get (WYSIWYG) manner, and test them using different styles and resolutions.

Widgets and forms created with Qt Designer integrate seamlessly with programmed code, using Qt's signals and slots mechanism, so that you can easily assign behavior to graphical elements. All properties set in Qt Designer can be changed dynamically within the code. Furthermore, features like widget promotion and custom plugins allow you to use your own components with Qt Designer.

Note: You have the option of using Qt Quick for user interface design rather than widgets. It is a much easier way to write many kinds of applications. It enables a completely customizable appearance, touch-reactive elements, and smooth animated transitions, backed up by the power of OpenGL graphics acceleration.[htta]

4.2.3 Ubuntu:

Ubuntu (pronounced oo-BOON-too) is an open source Debian-based Linux distribution. Sponsored by Canonical Ltd., Ubuntu is considered a good distribution for beginners. The operating system was intended primarily for personal computers (PCs) but it can also be used on servers. The word "ubuntu" is from the African Zulu language and translates as "humanity to others".

The primary version of Ubuntu employs GNOME (GNU Network Object Model Environment, pronounced gah-NOHM), a graphical user interface (GUI) and set of desktop applications for Linux. GNOME is intended to make Linux easy to use for non-programmers and is similar to the Windows desktop interface.[httd]

4.2.4 XAMPP:

XAMPP (or) is a free and open-source cross-platform web server solution stack package developed by Apache Friends, consisting mainly of the Apache HTTP Server, MariaDB database, and interpreters for scripts written in the PHP and Perl programming languages. Since most actual web server deployments use the same components as XAMPP, it makes transitioning from a local test server to a live server possible. XAMPP's ease of deployment means a WAMP or LAMP stack can be installed quickly and simply on an operating system by a developer, with the advantage a number of common add-in applications such as Wordpress and Joomla! can also be installed with similar ease using Bitnami.[httg]

4.3 Platforms

To Create any system choosing the right platform is a must, and for our system, we chose for the software part :

4.3.1 PyCharm IDE

Definition

PyCharm is an integrated development environment (IDE) used in computer programming, specifically for the Python language. It is developed by the Czech company JetBrains. It provides code analysis, a graphical debugger, an integrated unit tester, integration with version control systems, and supports web development with Django as well as Data Science with Anaconda.
PyCharm is cross-platform, with Windows, macOS and Linux versions. There is the Community Edition, and also there is Professional Edition with extra features – released under a proprietary license.

Why PyCharm IDE

- Cross-platform, Windows, macOS and Linux versions.
- Intelligent Coding Assistance
- Ease to use.

4.3.2 Arduino

Definition

The Arduino Integrated Development Environment (IDE) is a cross-platform application (for Windows, macOS, Linux) that is written in functions from C and C++. It is used to write and upload programs to Arduino compatible boards, the Arduino IDE supplies a software library. User-written code only requires two basic functions, for starting the sketch and the main program loop, that are compiled and linked with a program stub main().
The environment is written in Java and based on Processing and other open-source software. In October 2019 the Arduino organization began providing early access to a new Arduino Pro IDE with debugging and other advanced features.

Why Arduino IDE

- Arduino is to easy to use.
- flexible for advanced users.
- Open source and extensible open source.
- Runs on Mac, Windows, and Linux.

- Simple, clear programming environment.

Device characteristics(Hardware)

The system is implemented on DELL LATITUDE E5430 with the following specification:

- Cpu : intel(R) Core(TM) i5-3320M CPU @2.60GHz.
- RAM : 4GB.
- Exploitation System : Ubuntu.

4.4 Models & Sensors

Before going any further we will explain the sensor that we used.

4.4.1 Fingerprint Sensor:

DY50 optical fingerprint sensor, that used to capture a digital image from the human finger.

Figure 4.1: Fingerprint sensor

4.4.2 Keypad:

is one of the most commonly used input devices in microprocessor applications. In a standard keypad wired as an X-Y switch matrix, normally-open switches connect a row to a column when pressed. If a keypad has 12 keys, it is wired as 3 columns by 4 rows. A 16 key pad would have 4 columns by 4 rows. As usual it's packed with zero documentation, thus it took couple of hours to get to work. Anyway the keypad is a perfect blend of art and technology with a price tag far below rubies.[htth]

Figure 4.2: *Keypad*

4.4.3 LCD:

liquid crystal display is very popular and broadly used in electronics projects as they are good for displaying information like sensors data for the project, and also they are very cheap.[httc]

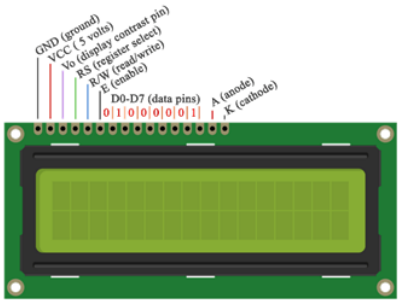


Figure 4.3: *LCD*

4.5 Implementation

After going through the platform and defining it and the requirement of the project, now we will explain the implementation of the system. Our system contains two main parts: Hardware and Software.

4.5.1 Hardware

We created a prototype for the authentication device the picture below show the chart for this prototype.

Arduino is a microcontroller board connect to the computer through USB capel, and

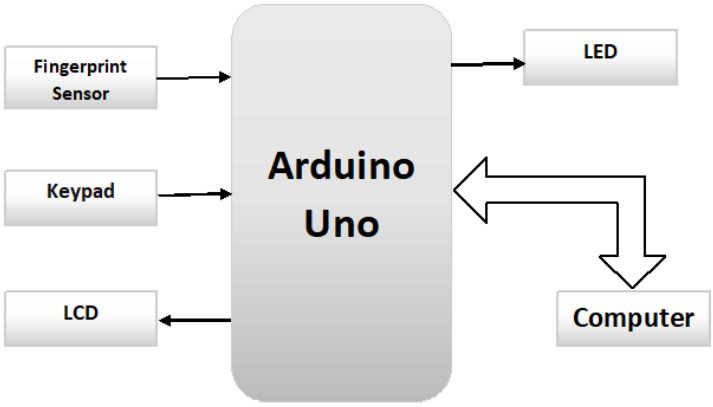
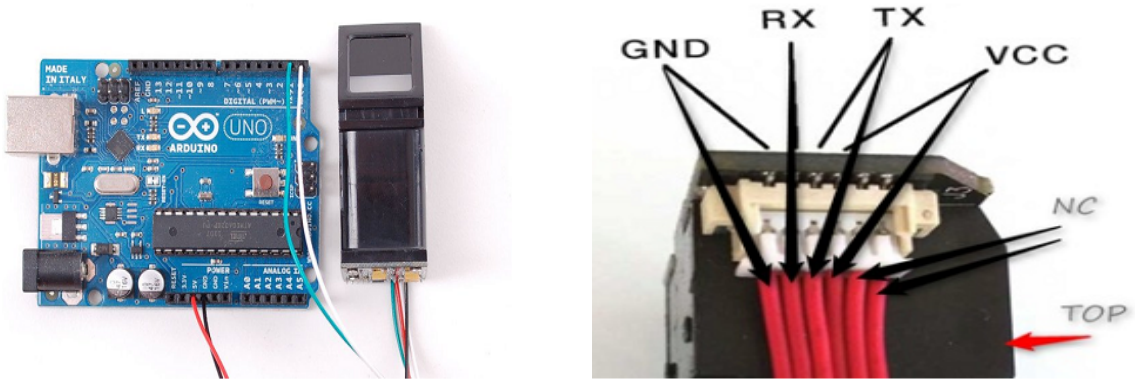


Figure 4.4: *Authentication Device Prototype*

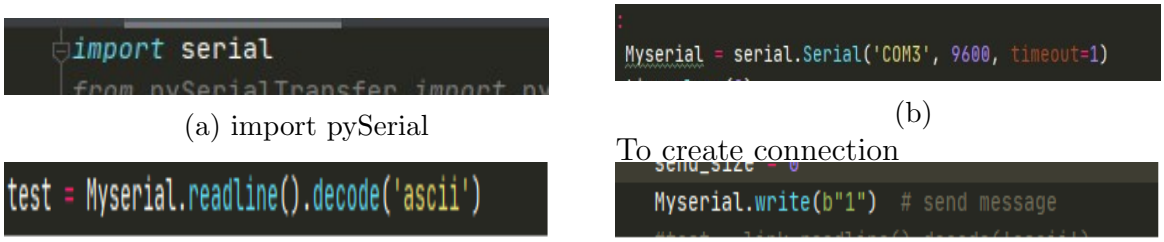
have a digital and analogue pin to link the different sensors together, It also has an energy entrance. The fingerprint sensor connects to the Arduino board through pin 0 and pin 1(RX, TX respectively), the Figure below show how connected. The first wire from the left is ground, then the two data pins RX and TX, then power.[Dad]



(a) *Pin and Wire* (b) *Fingerprint Wire*

Figure 4.5: *Arduino and Fingerprint sensor Connection*

Keyboard to entre the student number they try authenticate to link the finger query withe the finger stored in the database. if the student is ok then the green LED shines, if not the red LED shines. The computer (Python) and Arduino connect by a serial. in python said need pySerial library to read data come from arduino or write data in arduino (send).**Figure4.7** and in Arduino said need to begin the Serial in setup function**Figure**



(a) import pySerial

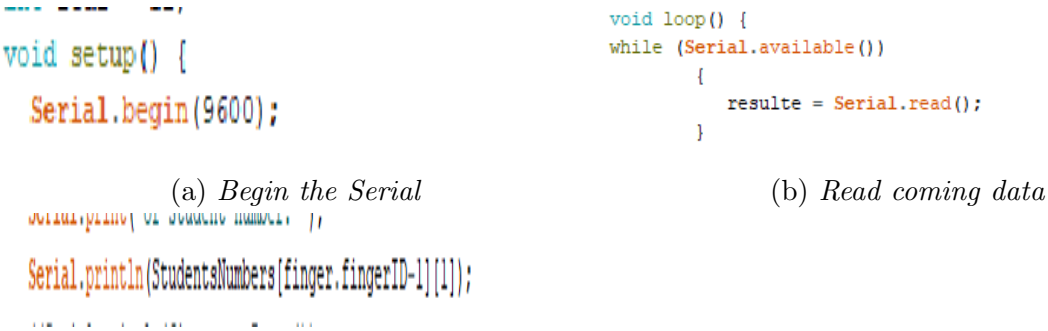
(b) To create connection

(c) *Read coming data*

(d) *Write data in Serial*

Figure 4.6: *pySerial library*

4.7a.and test the serial if available and read data **Figure 4.7b**, or send data by **Figure 4.7c**.



(a) *Begin the Serial*

(b) *Read coming data*

(c) *Write data in Serial*

Figure 4.7: *Arduino Configuration*

4.5.2 Software

To manage the system we created an application. It is managed by an administrator and the invigilator, the following descriptions show the interface of the system.

Login interface:

The **Figure 4.8** appears to the user (admin and invigilator), which is a login interface where the user enters the username and password, and the system verifies the validity of the inputs.

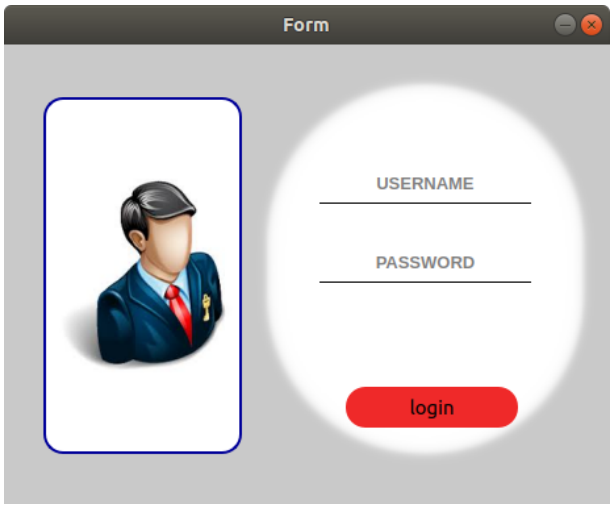


Figure 4.8: *login Page*

Student information:

If the account type is ADMIN, the user will be transferred to the Student Information Control Interface **Figure 4.9**.

On this page, the user can view the list of students and their most important information in the large table. He can also delete, add and modify student information. He can also search for student information by entering the student's number in the search box and pressing the search button. The system will display all student information in the small table as well. The system also allows the possibility of adding a user group from external sources by pressing the XLS import button. Shown in **Figure 4.9**. The student fingerprint information can also be added by specifying the student's number and then selecting the button scan FP.

Professors Information:

In this **Figure 4.10** the user can add, delete and modify the professor's information, and he can also add a group of professors from external sources. The most important information about the professors is displayed in the main table, and all the professor's information is displayed in the sub-table on the right of the screen.

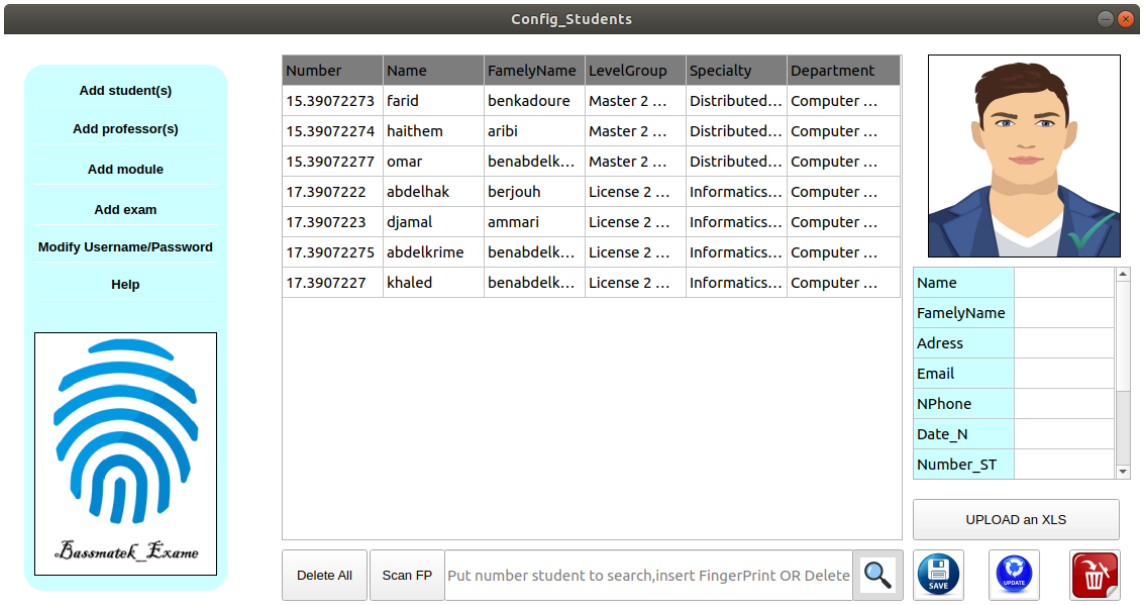


Figure 4.9: *Student Information .*

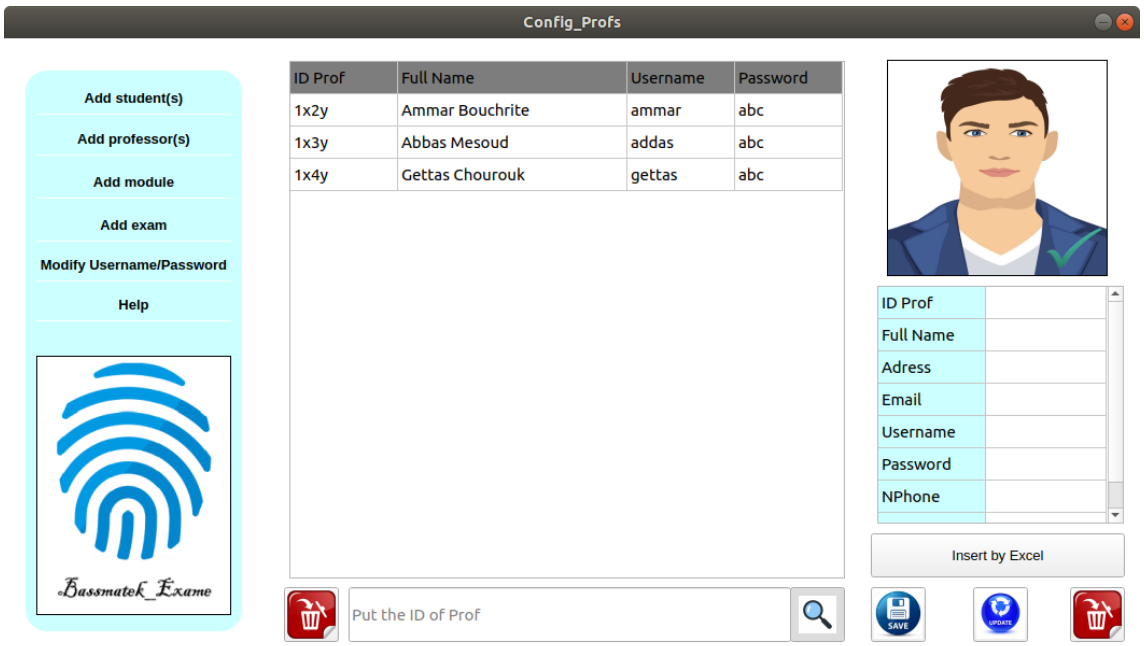


Figure 4.10: *Professors' Information.*

Modules Information:

The user can add a unit by typing the name of the unit and specifying the unit professor. Units are also displayed in the main table in the interface. **Figure 4.11**

Figure 4.11: *modules information.*

Exam information:

In picture below **Figure 4.12**, the user can add, delete, update and specify the contents of the table. He can also specify the section, level, and section for this table. Students are assigned directly according to the entered data. The picture also represents the control of special cases of students **Figure 4.13**, such as convicted students

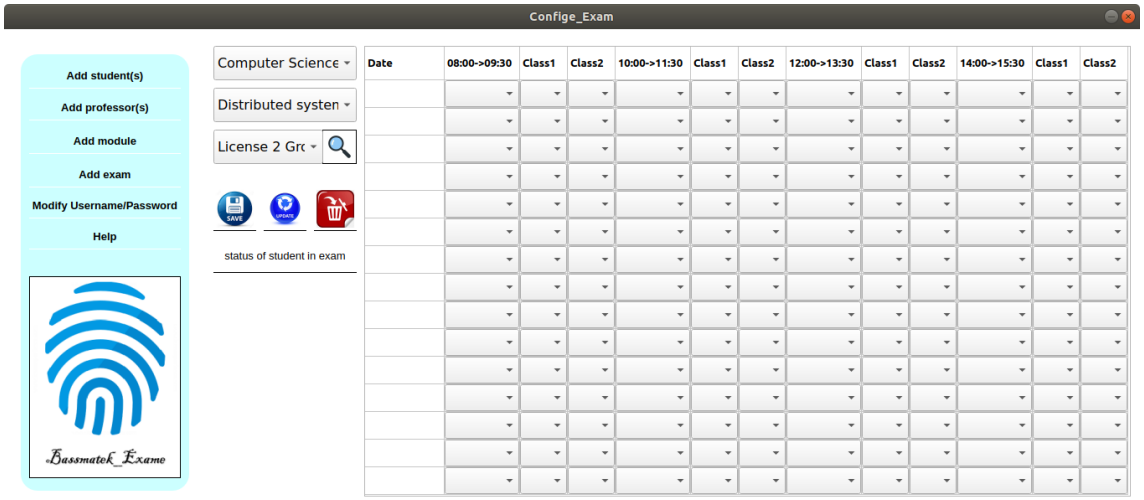


Figure 4.12: *Exam Information.*

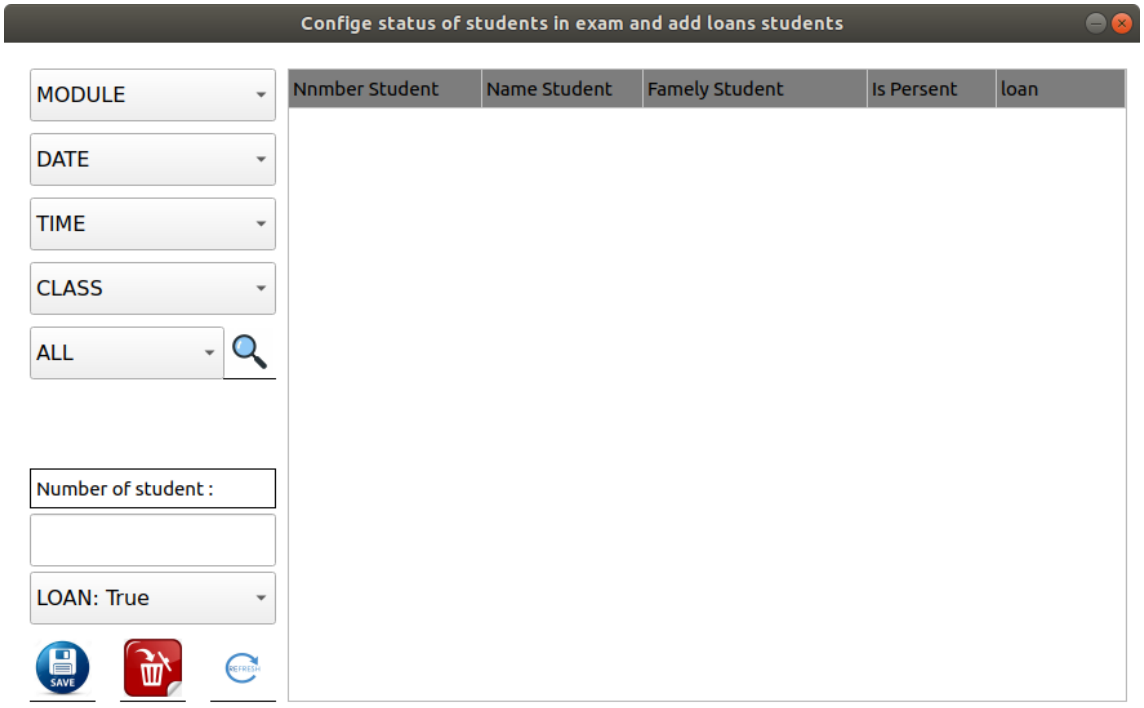


Figure 4.13: *students status configuration in exams.*

Edit username and password:

The user modifies the required information as shown in **Figure 4.14**

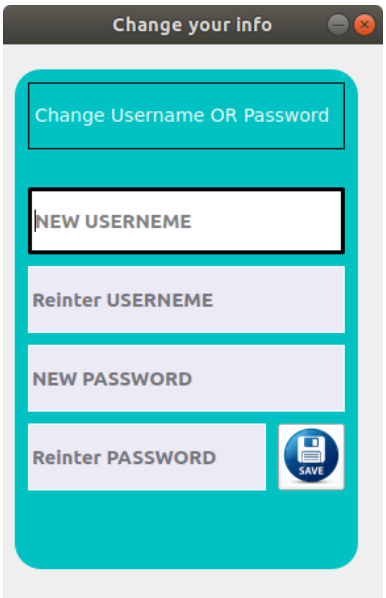


Figure 4.14: *Edit Username and Password.*

Help page:

User can select one of the common questions and the answer will be displayed. He can also add a new question, and it will be answered within a maximum of 48 hours.**Figure4.15**

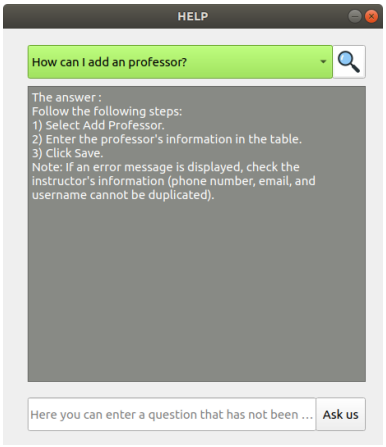


Figure 4.15: *Help Page.*

Invigilator page:

If the type of account is invigilator, the account number is displayed in the case of registration. In the case of attendance registration, where you can view the folder, record the student's attendance you will find this in**Figure4.16**.

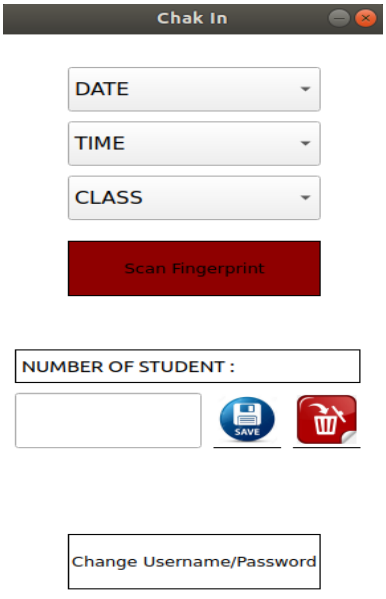


Figure 4.16: *Invigilator Page.*

To capture the image of fingerprint need the SFGDemo program, which works with the DY50 fingerprint sensor we chose it can capture, enroll and match but we just need it to capture the fingerprint image and use as input in our system.

Startup the SFGDemo software and click Open Device from the bottom left corner. Select the COM port used by the Arduino. And press OK when done. You should see the following, with a blue success message and some device statistics in the bottom cornerFigure 4.17.

If you get an error when you Open Device, check your wiring and try again.

Click on capture button and wait until the photo appear after that click in save image button to save the image the computer in the specific place to upload it by our system to analyze.**Figure 4.18**

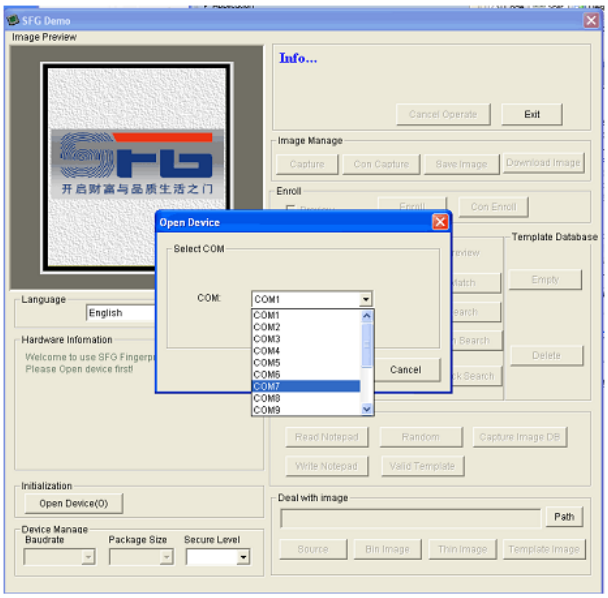


Figure 4.17: *SFGDemo Programme.*

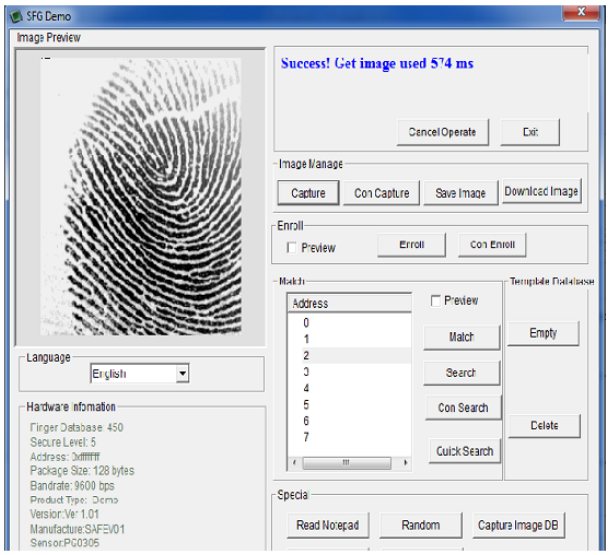


Figure 4.18: *Capture and Save Image.*

4.6 Results

The desired objectives was to propose an algorithm to reduce the time of the method of detecting and extract the minutiae, then use it to create the main process of recognizing the fingerprint image to reducing fraud. We create a data-set to test, it contains 26 pairs of grey-scale fingerprint photos in total 52 image (each two image from the same finger), Test each image alone in the proposed algorithm and the origin algorithm, and we reserved the execution time for each one and compared them. the results show in the table below.**Table 4.1**

When integrating the proposed method in the process of recognizing fingerprint described in chapter 3, we obtained a good results as illustrated in **Table 4.2**.
The database used to calculate the Accuracy rate contains six images.

Input Image	**Proposed Method**	**Origin Algorithm**	**Difference time**
1_1.*jpg*	0.360862017	0.366303921	0.005441904
1_2.*jpg*	0.344538927	0.366765022	0.022226095
2_1.*jpg*	0.343019009	0.365927219	0.022908211
2_2.*jpg*	0.341825962	0.362597942	0.02077198
3_1.*jpg*	0.339992046	0.364133835	0.024141788
4_1.*jpg*	0.338831902	0.362483025	0.023651123
5_1.*jpg*	0.348424911	0.368148088	0.019723177
6_1.*jpg*	0.341071844	0.362489223	0.021417379
11_2.*jpg*	0.352180958	0.340438128	-0.01174283
12_1.*jpg*	0.353384018	0.3471632	-0.006220818
13_2.*jpg*	0.339978933	0.341012955	0.001034021
14_1.*jpg*	0.335419178	0.332638979	-0.002780199
17_2.*jpg*	0.361101151	0.368350029	0.007248878
16_1.*jpg*	0.356666088	0.361410141	0.004744053
16_2.*jpg*	0.351830959	0.364562035	0.012731075
26_1.*jpg*	0.351877928	0.355177164	0.003299236

Table 4.1: *Comparison Result.*

BDD	**FAR**	**FRR**	**Accuracy Rat**
Our database	0.15	0.33	99.76%

Table 4.2: *Accuracy Rat.*

4.7 Discussion

We can notice that the proposed method did not succeed in all fingerprint images, for example, the image 11_2.jpg the origin CN gave a better time than the the proposed method. But the proposed method generated better results than the CN in the most case.

we think it is related to the the number of minutiae extracted from the image where 11_2.jpg contain 95 minutiae, and 1_2.jpg contain 75 minutiae. But it 's not verified because we had not enough time to run all the necessary tests.

The system obtained a good result and overcame identity fraud effectively, but the big problem is the use of the SFGDemo to capture the image and use it as an input to the system.

4.8 Conclusion

In this chapter, we discussed the platform used and the reason for choosing it. After that, we did go through the implementation with both of its part Hardware and Software.

Passing by the results and ending with discussion, clarifying some of the advantages and inconveniences of the implemented system.

General Conclusion

In this thesis, we tried to solve the Authentication problem in the hall exam using several technologies like Arduino and image processing. The objective of this system is to fight counterfeiting. The other objective is to reduce the authentication process time. The system uses a fingerprint sensor to capture the finger image. Storing this image in the database as a template, and test the finger image with the template in the test process and give the results of matching and generates the lists of the present students.

The system implementation was made with Arduino IDE and PyCharme IDE for the desktop application and set of sensors. the system can be divided into two parts the arduino application which does send and receive data to and from Python programme and the Python program that do the process of recognition.

We achieved a system capable of :

- Fingerprint Recognition.
- Identify students by fingerprint.
- Compare two fingerprints.
- Scheduling students' attendance for the exam.

What distinguishes our system from other systems is the low cost and the good accuracy rate. Walking through the different chapters we described and clarify
the system architecture, faced limitations, some hypothesis and achieved objectives.

perspectives

As for future perspectives, we will try to strengthen our system with a better fingerprint sensor in order to make it more flexible and test it on a larger database to obtain a fixed accuracy rate. We'll also enhance it to work remotely using only the fingerprint scanner without the need of any computer which we couldn't ensure due to time constraint and the pandemic. Likewise, we can improve the efficiency of our system by adding cameras to detect students' motions to spot those who are trying to cheat using deep learning techniques.

Bibliography

[AAZ19] Abdullah Alshbtat, Mohammad Alfraheed, and Nabeel Zanoon. "A Novel Secure Fingerprint-based Authentication System for Student's Examination System". In: *International Journal of Advanced Computer Science and Applications* 10 (2019), pp. 515–519.

[Alk16] Mohammed Ahmad A Alkhathami. "Watermarking Techniques for Genuine Fingerprint Authentication". PhD thesis. 2016, pp. 14–15.

[BBM11] Kuntal Barua, Samayita Bhattacharya, and D.Kalyani Mali. "Fingerprint Identification". In: *Global Journal of Science and Technology* 11 (2011).

[Bel17] Foudil Belhadj. "Biometric system for identification and authentication". PhD thesis. 2017.

[BSB11] Roli Bansal, Priti Sehgal, and Punam Bedi. "Minutiae Extraction from Fingerprint Images - a Review". In: *International Journal of Computer Science Issues* 8 (2011).

[BT04] Bir Bhanu and Xuejun Tan. *Computational Algorithms for Fingerprint Recognition*. Kluwer Acadimec publishers, 2004.

[CPP14] Atul S. CHAUDHARI, Girish K. PATNAIK, and Sandip S. PATIL. "Implementation of Minutiae Based Fingerprint Identification System Using Crossing Number Concept". In: 18 (2014).

[CV16] ubhankar Chattoraj and Karan Vishwakarma. "A Biometric Solution for Door Locking System using Real time Embedded System and Arduino as the Microcontroller". In: *IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)* 11 (2016), pp. 1–5.

[CW16] Letian Cao and Yazhou Wang. "Fingerprint image enhancement and minutiae extraction algorithm". In: *Department Of technology linnaeus university* (2016).

[Dad] Lady Dada. "Adafruit Optical Fingerprint Sensor". In: *Adafruit Learning System* ().

[GA17] Ahmed Baita Garko and Abdulaziz Ahmad. "Design and Modeling of a Student Verification System in an Examination in Nigeria Using Biometric Fingerprint Technology". In: *International Journal of Advanced Academic Research Sciences, Technology and Engineering* 3 (2017).

[htta] https://doc.qt.io/qt-5/qtdesigner-manual.html. In: *13/9/2020* ().

[httb] https://en.wikipedia.org/wiki/Authentication. In: *15/2/2020* ().

[httc] https://howtomechatronics.com/tutorials/arduino/lcd-tutorial/. In: *13/9/2020* ().

[httd] https://searchdatacenter.techtarget.com/definition/Ubuntu. In: *13/9/2020* ().

[htte] https://stackoverflow.com/questions/30503766/how-can-i-calculate-the-failed-acceptance-rate-and-false-recognition-rate. In: *20/9/2020* ().

[httf] https://techterms.com/definition/python. In: *13/9/2020* ().

[httg] https://www.definitions.net/definition/XAMPP. In: *13/9/2020* ().

[htth] https://www.electroschematics.com/arduino-with-keypad/. In: *13/9/2020* ().

[HWJ98] Lin Hong, Yifei Wan, and Anil Jain. "Fingerprint Image Enhancement: Algorithm and Performance Evaluation". In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* (1998). DOI: 10.1109/34.709565.

[JRR09] RAVI. J, K. B. RAJA, and VENUGOPAL. K. R. "FINGERPRINT RECOGNITION USING MINUTIA SCORE MATCHING". In: *International Journal of Engineering Science and Technology* (2009), pp. 35–42.

[KFA08] Anil K.jain, Patrick Flynn, and Arun A.Ross. *Handbook of Biometrics*. Springer science + Business Media, 2008.

[KJa+97] K.Jain et al. "An Identity-Authentication System Using Fingerprints". In: *Proceedings of the IEEE* 85 (1997).

[KTD11] N.P. Khanyile, J.R. Tapamo, and E. Dube. "A Comparative Study of Fingerprint Thinning lgorithms". In: (2011).

[Mal+06] Davide Maltoni et al. *Handbook of Fingerprint Recognition*. Springer, 2006.

[Mas03] Libor Masek. "Recognition of Human Iris Patterns for Biometric Identification". In: *Engineering degree of the School of Computer Science and Software Engineering The University of Western Australia* (2003).

[MM97] Dario Maio and Davide Maltoni. "Direct Gray-Scale Minutiae Detection In Fingerprints". In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 19 (1997).

[MSl18] Magdin Martin, koprda Stefan, and Ferenczy l'ubor. "Biometrics Authentication of Fingerprint with Using Fingerprint Reader and Microcontroller Arduino". In: (2018). DOI: 10.12928/TELKOMNIKA.v16i2.7572.

[Muc+17] M A Muchtar et al. "Attendance fingerprint identification system using arduino and single board computer". In: *2nd International Conference on Computing and Applied Informatics* (2017), pp. 1–6.

[NB01] Kenneth Nilsson and Josef Bigun. "Using Linear Symmetry Features as a Preprocessing Step for Fingerprint Images". In: *Springer-Verlag Berlin Heidelberg* (2001).

[Par04] Philippe Parra. "Fingerprint minutiae extraction and matching for identification procedure". In: *Department of Computer Science and Engineering University of California, San Diego* (2004).

[Rah18] Ashish Ernest Rahul. "Fingerprint Recognition System Using Arduino". In: *International Journal of Research in Engineering, Science and Management* 1 (2018).

[SMJ12] Muhammad Sharif, Sajjad Mohsin, and Muhammad Younas Javed. "A Survey: Face Recognition Techniques". In: *Research Journal of Applied Sciences, Engineering and Technology* (2012).

[TC84] T.Y.ZHANG and C.Y.SUEN. "A Fast Parallel Algorithm for Thinning Digital Patterns". In: *Communications of the ACM* 27 (1984), pp. 236–239.

[TK00] Marius Tico and Pauli Kuosmanen. "An Algorithm for Fingerprint Image Postprocessing". In: *IEEE* (2000), pp. 1735–1739.

[Wan+06] Chengfeng Wang et al. "An efficient algorithm for fingerprint matching". In: *IEEE* (2006).

[Wie09] Lukasz Wieclaw. "A Minutiae-Based Matching Algorithms in Fingerprint Recognition Systems". In: *Journal of Medical Informatics and Technologies* 13 (2009).

[XLN09] Dacheng Xu, Bailiang Li, and Anton Nijholt. "A Novel Approach Based on PCNNs Template for Fingerprint Image Thinning". In: *Eigth IEEE/ACIS International Conference on Computer and Information Science* (2009).

[Zai+14] Nur Izzati Zainal et al. "Design and Development of Portable Classroom Attendance System Based on Arduino and Fingerprint Biometric". In: *Proc.of the IEEE 5th International Conference on Information and Communication Technology for the Muslim World (ICT4M)* (2014).

[ZJP05] Stan Z.li, Anil K. Jain, and Salil Prabhakar. *Handbook of Face Recognition*. Springer science + Business Media, 2005.

[ZT06] Feng Zhao and Xiaoou Tang. "Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction". In: *Pattern recognition society* (2006), pp. 1271–1281.

[ZX06] Yuheng Zhang and Qinghan Xiao. "An Optimized Approach for Fingerprint Binarization". In: *International Joint Conference on Neural Networks* (2006).