# CHAPTER ONE

## INTRODUCTION

Fingerprint verification is an important biometric technique for personal identification. Biometrics is a technology that uniquely identifies a person based on his physiological or behavioral characteristics. It relies on an individual’s characteristics to make personal identification and therefore can inherently differentiate between an authorized person and an unauthorized person. Any human physiological or behavioral characteristic can be used to make a personal identification as long as it satisfies the following requirements:

1. **Universality**- This means that every person should have the characteristic.
2. **Uniqueness** - This indicates that no two persons should be the same in terms of the characteristic in question.
3. **Permanence** - This means that the characteristic should be invariant with time. That is, at every point in the lifetime of the individual, this characteristic should be the same.
4. **Collectability** - This indicates that the characteristic can be measured quantitatively.
5. **Performance** – This refers to the achievable identification accuracy, the resource requirements to achieve acceptable identification accuracy, and the working or environmental factors that affect the identification accuracy.
6. **Acceptability** - This indicates to what extent people are willing to accept the biometric system.
7. **Circumvention** – This means that it should be difficult to bypass the system.

The human fingerprint meets these requirements, others being the iris and DNA. However, the latter are harder to implement and usually not as cost friendly as the fingerprint.

Generally, there are two types of systems that help automatically establish the identity of a person:

1. Authentication (verification) systems
2. Identification systems.

In a verification system, a person desired to be identified submits an identity claim to the system, usually via a magnetic stripe card, login name, smart card, etc. and the system either rejects or accepts the submitted claim of identity. 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 having to claim an identity. This project is channeled towards the development of an examination authentication system that eliminates impersonation. It would achieve this by taking advantage of a unique feature of identification – the fingerprint. In our system, the student would not need to provide any means of identification, rather the system will identify whether or not the student is permitted to write the examination using an inherent characteristic (fingerprint) of the student.

Anil J. and Hong L. [1] compared different biometric technologies and found out that fingerprint is the most widely used technology in the world as it accounts for approximately $100 million of forensic applications. They developed a fingerprint matching algorithm based on point matching (minutiae matching) instead of the traditional image based and ridge-pattern matching. The reason for their choice is the need to develop a robust, simple and fast verification algorithm and to keep the template (image prints) size small.

O. Akinola and A. Abayomi-Alli [2] developed a microcontroller based fingerprint examination pass system using C# programming language and Futronic FS80 scanner. The system and its interface was develop using Microsoft Visual Studio 2010. Their system worked in two modes: enrollment/registration mode during which the student’s information alongside fingerprint is stored into the database and authentication mode during which a print is compared with the data available in the database to determine if the owner of the print is eligible for the exam. Their system gave a convenience value of 98.67% when tested with 75 students.

Another interesting research work which illuminates the world of fingerprint identification is the work of James Stephen, and Prasad Reddy [3]. This work identifies the flaws in minutiae based fingerprint system. The study proposed the Singular Value Decomposition system (SVD) for the acquisition of images, extraction of features and matching of patterns. The first stage involved acquiring of images through a fingerprint user interface while the feature extraction stage involved the extraction of the features from the images through the Singular Value Decomposition algorithm by splitting it into vectors and taking into consideration, their vectorial positions. The matching stage was achieved through the Euclidean distance algorithm.

Oyediran Mayowa Oyedepo and Wahab Wajeed Bolanle [4] proposed a standalone handheld biometric system. Their system uses Arduino MEGA, Adafruit fingerprint sensor, HC-05 Bluetooth module. The Arduino microcontroller acts as a link between the sensor and the Bluetooth module and converts the data received from the fingerprint sensor to a string that can be sent over Bluetooth. It also parses the data received from the PC and sends appropriate commands to the FPS. They used Arduino because it has multiple serial ports to communicate with both the Bluetooth module and the fingerprint sensor. Like most biometrics system, it has two modes of operation also, registration and verification. Their system successfully identified and verified registered students and also generates a report of registered students in real time.

Our system will make use a microcontroller and mobile device along with the FPS (fingerprint sensor) to register/enroll students and thereafter verify them for the examination. It will solve the problem of portability and convenience for administrators carrying out authentication process, by eliminating the requirement of a PC, and replacing it with a mobile device.

## 1.1 PROBLEM STATEMENT

Authentication has always been a major challenge in all types of examination. Verification of the authentic candidate is not an easy task, and also it consumes a lot of time and process. Often times, the issue of impersonation becomes a major challenge in determining the performance of a candidate the examination was meant for. This led to the development of Fingerprint based exam hall authentication system that is designed to register students for an exam by taking their fingerprints and to pass only users verified by their fingerprint scan and block non verified users from taking the exam.

## 1.2 AIM

The aim of this project is to design and implement a finger print based biometric authentication system for examination purposes.

## 1.3 OBJECTIVES

To create a system that is capable of tracking impersonators in the examination system using finger print biometrics and mobile device. To reduce rate of corruption in the educational sector and increase the rate of self-confidence on students. To demonstrate the possibility of computer technology in the satisfaction of human needs and also enforce strict security measures that ensure unregistered students do not write exams for other registered students.

## 1.4 METHODOLOGY

The project design and implementation utilizes a microcontroller to communicate with the fingerprint module and the Bluetooth module. The Bluetooth module interacts with the phone by sending the scanned prints during registration to the database and also retrieving the data from the database during the verification stage.

The project has the following features:

* Registration of students.
* Authentication during examination.
* Feedback on the number of students that were authenticated for a particular exam.
* Portable data transfer among different devices.

The mobile application to be used for communication is developed using Java (android) programming language for the interface and the compiler employed is android studio with Java SDK 23. The microcontroller code is written with C++.

The system operates in two modes, registration and verification. During the registration stage, student’s records are entered into the database via the interface in the android device. Fingerprints taken with fingerprint sensor (FPS) are processed by the microcontroller and sent via Bluetooth to the android device for storage as an image file. During verification stage, the fingerprint collected is compared with prints in the database. If a match is found, it pops open the student’s info indicating that the student is eligible for the examination otherwise an exception is thrown indication that the student is not eligible for the examination.

## 1.5 RELEVANCE

With the increasing rate of exam malpractices in the educational sectors, the Universities management decides to incorporate a reliable security means to ensure that these activities of exam impersonators are checkmated. The activities of these exam impersonators have seen the educational sector suffer some serious form of corruption ranging from students to students to students to supervisors. So it became necessary for the educational body to set up strategies to stop this corruption in the educational sector.

The system uses finger prints biometrics and mobile device, that will help ensure that only students with their fingerprints registered during registration period are allowed into the examination hall. As opposed to existing fingerprint biometric systems, this proposed system makes it easier to carry out the authentication process. Existing solutions make use of a laptop or PC device as the interface for registration and authentication. This has a few cons including the size which makes it less portable and the requirement for power. Our system will employ a mobile device for authentication process. The invigilator would no longer need to carry a laptop to the examination hall. Using his mobile phone or any other available mobile phone (with the application installed and the right database files loaded), he can authenticate students smoothly.

This system being easy to deploy and also cost friendly, would contribute in stopping any activity of corruption in the form of impersonation in the educational sector. Hard work would be encouraged as every registered student knows he/she is going to write the exam by him or herself. Consequently, the society will produce more reliable and trustworthy graduates that can match up to their qualifications. The impersonation which has been eating the educational system thereby encouraging laziness among students would be eliminated and standard of student educational performance would be increased.

## 1.6 SCOPE

This system allows the registration of students with their details such as name and mat number as well as their fingerprint scans. This data is stored in a database and can be extracted as a file and transferred from one device to another. The microcontroller used for the project however, cannot store information exceeding 5MB. Therefore, registration data for a particular examination should not exceed this limit.

The system is designed to work with mobile devices, specifically android phones, through which authentication can be carried out. The system does not work with PC or laptop devices.

This system makes use of a Bluetooth module with a range of 10m. Therefore, the distance between the mobile device and the microcontroller unit should not exceed this limit.

# CHAPTER TWO

# LITERATURE REVIEW

## INTRODUCTION

In this chapter, a review of all the components used in this project is discussed.

## Fingerprint Module

## Microcontroller

## Bluetooth module

## Crystal Oscillator

## Voltage Regulator

## Capacitors

## 2.7 Resistors

## REFERENCES

1. Anil Jain􀀀, Lin Hong.An Identity Authentication System Using Fingerprints.
2. O. A. Akinola1, A. Abayomi-Alli (August, 2015). Development of a Microcontroller Based Fingerprint Examination Access Control System.
3. James Stephen, Prasad Reddy (2012). Implementation of Easy Fingerprint Authentication with Euclidean and Singular Value Decomposition Algorithm. International Journal of Software Computer Application, 3(2), 1-15.
4. Oyediran Mayowa Oyedepo, Wahab Wajeed Bolanle. Development of An Examination Authentication Embedded System Based on Fingerprint Approach.