**DESIGN AND CONSTRUCTION OF A FINGERPRINT BIOMETRIC AUTHENTICATION SYSTEM**

**BY**

**OKORO EFE CHRISTOPHER**

**ENG1303573**

**DEPARTMENT OF ELECTRICAL AND ELECTRONICS ENGINEERING**

**FACULTY OF ENGINEERING**

**UNIVERSITY OF BENIN**

**BENIN CITY**

**NIGERIA**

****

**MARCH, 2019.**

**DESIGN AND CONSTRUCTION OF A FINGERPRINT BIOMETRIC AUTHENTICATION SYSTEM**

**BY**

**OKORO EFE CHRISTOPHER**

**ENG1303573**

**A PROJECT SUBMITTED TO THE DEPARTMENT OF ELECTRICAL AND ELECTRONICS ENGINEERING, FACULTY OF ENGINEERING, UNIVERSITY OF BENIN, BENIN CITY**

**IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELORS DEGREE IN ELECTRICAL AND ELECTRONICS ENGINEERING (B.ENG)**

**MARCH, 2019.**

# CERTIFICATION

This is to certify that this project was designed and constructed by **OKORO EFE CHRISTOPHER**, of the Department of Electrical and Electronics Engineering, University of Benin, Benin City, Edo State, Nigeria.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**PROF. F.O EDEKO DATE**

PROJECT SUPERVISOR

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ENGR. MRS. E. OMOZE DATE**

ASST. PROJECT SUPERVISOR

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**PROF. S.A IKE DATE**

HEAD OF DEPARTMENT

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ENGR. J. EGWAILE DATE**

PROJECT COORDINATOR

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**EXTERNAL EXAMINER**  **DATE**

# DEDICATION

This project is dedicated to the almighty infinite God.

# ACKNOWLEDGEMENTS

First and above all, I acknowledge the mercies, love and kindness of God for the journey of my academic pursuit and for the knowledge and understanding throughout my years in University of Benin and also for the strength to carry on to the end. Thank you almighty God.

I owe deep and unending appreciation to my Parents, Mr and Mrs Emmanuel Okoro for their belief in my abilities and support all through this journey. To my siblings: Mr Okoro Collins, Mrs Ufuoma Akpota and Mrs Elohor Siode, thank you all for your support, care and encouragement; I love you all.

I sincerely acknowledge the selfless commitment of my lecturers and project supervisors, Prof. F.O. Edeko and Engr. Mrs E. Omoze, I appreciate all your efforts to make this project a reality”. To all my lecturers who have contributed in molding me thus far, I say a very big thank you.

Never would I forget support from friends: Anoule Samuel, Nathan Doreen, Audu Charity, John Esan, Oshodin Andrew. May God reward you abundantly, I pray, Amen.

**Table of Contents**

[CHAPTER ONE 2](#_Toc531173337)

[1.0 INTRODUCTION 2](#_Toc531173338)

[1.1 PROBLEM STATEMENT 3](#_Toc531173339)

[1.2 AIM 4](#_Toc531173340)

[1.3 OBJECTIVES 4](#_Toc531173341)

[1.4 RELEVANCE 4](#_Toc531173342)

[1.5 SCOPE 5](#_Toc531173343)

[CHAPTER TWO 6](#_Toc531173344)

[LITERATURE REVIEW 6](#_Toc531173345)

[2.0 INTRODUCTION 6](#_Toc531173346)

[2.1 THE SCIENCE OF FINGERPRINTS 6](#_Toc531173347)

[2.2 REVIEW OF SIMILAR PAST PROJECTS 12](#_Toc531173348)

[2.3 COMPONENTS REVIEW 15](#_Toc531173349)

[CHAPTER THREE 30](#_Toc531173350)

[METHODOLOGY 30](#_Toc531173351)

[3.0 INTRODUCTION 30](#_Toc531173352)

[3.1 CIRCUIT MODE OF OPERATION 30](#_Toc531173353)

[3.2 SYSTEM DESIGN 37](#_Toc531173354)

[CHAPTER FOUR 64](#_Toc531173355)

[CONSTRUCTION, TESTING AND RESULTS 64](#_Toc531173356)

[4.0 INTRODUCTION 64](#_Toc531173357)

[4.1 CONSTRUCTION 64](#_Toc531173358)

[4.2 TESTING 68](#_Toc531173359)

[4.3 RESULT 68](#_Toc531173360)

[4.4 SYSTEM PERFORMANCE AND EVALUATION 70](#_Toc531173361)

[CHAPTER FIVE 73](#_Toc531173362)

[CONCLUSION AND RECOMMENDATION 73](#_Toc531173363)

[5.0 CONCLUSION 73](#_Toc531173364)

[5.1 RECOMMENDATION 73](#_Toc531173365)

[REFERENCES 75](#_Toc531173366)

# LIST OF FIGURES

Figure 2.1: Ridges and Valleys of a Fingerprint 6

Figure 2.2: Minutiae types 7

Figure 2.3: Loop, Whorl & Arch pattern examples. 8

Figure 2.4: An official Arduino Uno R2 with description of the I/O locations. 17

Figure 2.5: Diagram of the crystal and equivalent circuit 24

Figure 2.6: Voltage regulator (7805) pin diagram -----------------------------------25

Figure 2.7: Power supply circuit 26

Figure 2.8: Capacitors ----------------------------------------------------------------------27

Figure 3.1: Registration interface. 30

Figure 3.2: Fingerprint scanning interface. 31

Figure 3.3: Enrollment Flow Chart 32

Figure 3.4: Interface for selection of Bluetooth module. 33

Figure 3.5: Verification interface. 34

Figure 3.6: Student’s record after verification. 35

Figure 3.7: Verification flow chart 36

Figure 3.8: Block Diagram 37

Figure 3.9: Circuit diagram 38

Figure 3.10: Power supply circuit 39

Figure 3.11: R307 Fingerprint Module Pin Description 41

Figure 3.12: ATMega328 Microcontroller pins description 44

Figure 3.13: HC-05 Bluetooth Module pin description 48

Figure 4.1: Completed Project with Casing 65

Figure 4.2: Casing opened showing enclosed components 65

# ABSTRACT

Examination malpractice is an unlawful conduct exhibited by a candidate in an examination towards the attainment of academic success with no significant efforts. These unlawful acts affect the credibility of any examination. Examination malpractices have consistently remained an issue of concern to scholars in

Nigerian educational system. One of the types of examination malpractices is impersonation; which is an act of intentionally pretending to be another person for the purpose of fraud. Checking students into an examination hall has been with the presentation of school identification cards, examination cards, library cards, school fees receipts and clearance cards. It has been observed and presented that students tend to forge these moveable physical identity by presenting an imitated copy suiting the candidate appearing for the examinations. In this paper, a fingerprint biometric technique was presented with the aim to curb the problem of examination impersonation. Students were selected to test the proposed system by registered many students and purposely leaving out few students during enrolment. The proposed system was able to authenticate the enrolled students and prevented false identities claimed by false students. Based on these highlighted discoveries, recommendations were made; these include: financial supports should be provided to procure more fingerprint scanners to cater for a large number of students and alternative source of power should be provided in case the battery fails during authentication.

# 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 (Anil Jain et al):

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 the pitfalls of a verification system, more specifically, 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.

## 1.1 PROBLEM STATEMENT

Authentication has always been a major challenge in all types of examination. Verification of the authentic candidates for an examination is not an easy task, and also it consumes a lot of time and process. Often times, the issue of impersonation poses a major challenge to the determination of the true performance of candidates the examination was meant for. For this reason, the idea of developing a Fingerprint based exam hall authentication system that is designed to register students for an exam by taking their fingerprints prior to the exam then pass only users verified by their fingerprint scan and block non-verified users from taking the exam, was birthed.

## 1.2 AIM

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

## OBJECTIVES

* To create a system that is capable of tracking impersonators in the examination system using fingerprint biometrics and mobile device.
* To implement a system that will help 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 enforce strict security measures that ensure unregistered students do not write exams for other registered students.

## 1.4 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.

## 1.5 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. More specifically, this system can enroll a maximum of 1000 students.

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

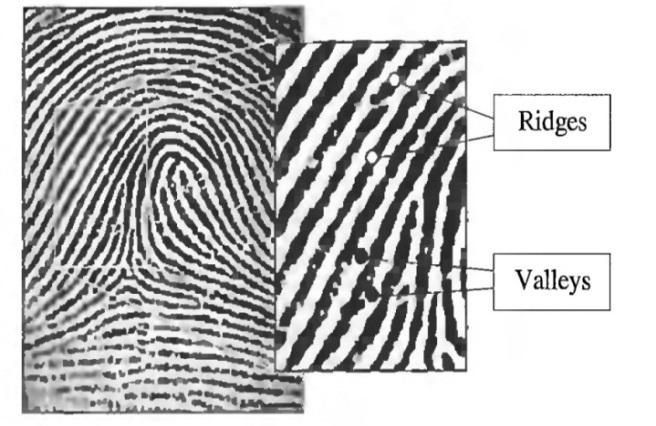
## LITERATURE REVIEW

### 2.0 INTRODUCTION

Before beginning this project, extensive study and research was carried out to understand the fundamentals of fingerprint biometrics system. This chapter gives an insight into the theoretical framework as well as previous studies conducted by past researchers relating to this project.

### 2.1 THE SCIENCE OF FINGERPRINTS

Fingerprints are unique patterns made from friction ridges (raised) and furrows (recessed) which appears on the pads of the fingers and thumbs. A friction ridge is a raised portion of the epidermis on the finger while a furrow is a valley or depression between ridges. These friction ridges, sometimes known as “epidermal ridges” are caused by the underlying interface between the dermal papillae of the dermis and the interpapillary (rete) pegs of the epidermis (SWGFAST, 2012). These epidermal ridges serve to amplify vibrations triggered, for example, when fingertips brush across an uneven surface, better transmitting the signals to sensory nerves involved in fine texture perception. These ridges may also assist in gripping rough surfaces and may improve surface contact in wet conditions.

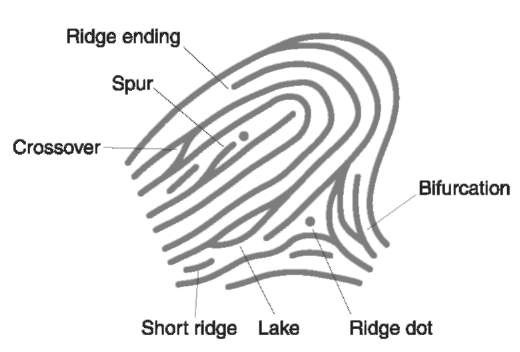


**Fig 2.1: Ridges and Valleys of a Fingerprint**

However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows but by a feature known as **Minutia** which are some abnormal points on the ridges (Lukasz W., 2009). Minutiae are major features of a fingerprint, using which comparisons of one print with another can be made.

There exist a variety of minutia types including ridge ending, ridge bifurcation, short ridge, island, spur, crossover, delta, core, etc of which ridge ending and ridge bifurcation are the most significant and heavy in usage.

1. **Ridge Ending:** The abrupt end of a ridge.
2. **Ridge Bifurcation:** A single ridge that divides into two ridges.



**Fig 2.2: Minutiae types**

#### 2.1.1 Fingerprint Recognition

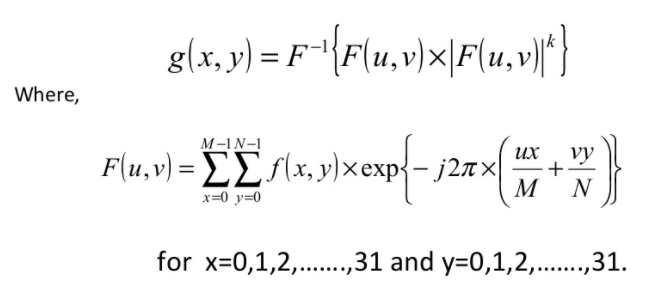
Fingerprint recognition is the process of comparing questioned fingerprint against another to determine if the impressions are from the same finger or palm. A person’s fingerprint pattern (the print left when an inked finger is pressed onto paper), is that of the friction ridges on that particular finger (Saferstein R., 2007). Friction Ridge patterns are grouped into three distinct types—loops, whorls, and arches—each with unique variations, depending on the shape and relationship of the ridges:



**Fig 2.3: *Loop, Whorl & Arch pattern examples****.*

* **Loops -** prints that recurve back on themselves to form a loop shape. Divided into radial loops (pointing towards the radius bone, or thumb) and ulnar loops (pointing towards the ulna bone, or pinky), loops account for approximately 60 percent of pattern types.
* **Whorls -** form circular or spiral patterns, like tiny whirlpools. There are four groups of whorls: plain (concentric circles), central pocket loop (a loop with a whorl at the end), double loop (two loops that create an S-like pattern) and accidental loop (irregular shaped). Whorls make up about 35 percent of pattern types.
* **Arches –** create a wave-like pattern and include plain arches and tented arches. Tented arches rise to a sharper point than plain arches. Arches make up about 5 percent of all pattern types.

The general pattern types (loop, whorl or arch) help us group fingerprints into categories for proper and further analysis. Analysts use these general pattern types to make initial comparisons and include or exclude a known fingerprint from other further analysis. To match a print, the analyst uses the minutiae to identify specific points on the unknown fingerprint with the same information in a known fingerprint. Several researches and algorithms have been developed over the decades to create more accurate and efficient matching systems to ascertain the origin (match) of a given fingerprint.

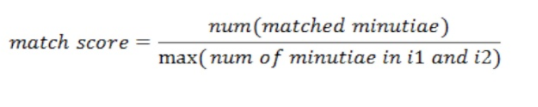
(Sandeep Kuma Panda et al, 2014) in their research identified three major stages for fingerprint recognition – Preprocessing stage, Minutia Extraction and Minutia Match. The preprocessing stage involved a technique known as Histogram Equalization which entailed improving the global contrast of an image by adjusting the intensity distribution on a histogram. Further enhancement was done using Fourier transform:

Thereafter, the 8-bit Gray fingerprint image was transformed into a 1-bit image with 0-value for ridges and 1-value for furrows. Further preprocessing techniques such as Block direction Estimation and ROI (Region of Interest) to remove noise were also carried out.

The Minutia extraction process involved Ridge Thinning – which is the elimination of redundant pixels of ridges till the ridges are just one pixel wide. This was achieved by iterative, parallel thinning algorithm. Thereafter, Minutia marking was done using the concept of Crossing Number (CN) which is a widely used technique for minutia extraction.

The Minutia matching stage involved two sub stages: -

* **Alignment stage**: - Given two fingerprint images to be matched, any one minutia from each image is chosen and the similarity of the two ridges associated with the two referenced minutia points is calculated.
* **Match stage**: After obtaining two sets of transformed minutia points, the elastic match algorithm is used to count the matched minutia pairs by assuming two minutiae having nearly the same position and direction are identical.



At the end of their project, they were able to achieve a match score of 0.67 for the same finger and 0.37 for different fingers which is adequate enough to identify a correct fingerprint.

(Lukasz Wieclaw, 2014) in his study made comparison between different minutiae-based matching algorithms. One of the popular extraction methods he explored was the Direct Grey-Scale Method by Maio and Maltoni [5]. Their basic idea is ridge tracing, by sailing according to the local orientation. The ridge line algorithm attempts to locate at each step, the local maxima, relative to a section perpendicular to the local ridge direction. The algorithm avoids revisiting the same ridge, by keeping track of the points traced so far. They also compared their method to binarization and thinning approaches and concluded that ridge following, significantly reduce computation time.

He also highlighted the Linear Symmetry (LS) filter method by (Nilsson et al, 2001) who proposed that this algorithm based on the concept that minutiae are local discontinuities of the LS vector field. Two types of symmetries - parabolic symmetry and linear symmetry are adapted to model and locate the points in the grey-scale image, where there is lack of symmetry.

In modern days, these extraction and matching process are abstracted and carried out by dedicated electronic devices. We now have complete modules that handle fingerprint recognition. Mobile devices, laptops, locks, etc now have fingerprint sensors that obtain, process and compare prints. A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. Many technologies have been used including optical, capacitive, RF, thermal, piezoresistive, ultrasonic, piezoelectric, MEMS. The fingerprint module we are going to employ is an optical biometric fingerprint reader/sensor (R307) module with TTL UART interface for direct connections to a microcontroller UART. It can store the fingerprint data in the module and can be configured in 1:1 or 1: N mode for identifying a person. This module can directly interface with any 3.3V or 5V microcontrollers, but a suitable level converter/serial adapter is required for interfacing with the serial port of a PC. R307 Fingerprint Module consists of optical fingerprint sensor, high-speed DSP processor, high-performance fingerprint alignment algorithm, high-capacity FLASH chips and other hardware and software composition, stable performance, simple structure, with fingerprint entry, image processing, fingerprint matching, search and template storage and other function.

### 2.2 REVIEW OF RELATED WORKS

* 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 were developed 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 vectoral 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.

Although these systems proposed in the above project worked well in their various use cases, one particular problem that is prevalent in these systems is its dependability on a PC or laptop device for the verification process. This poses as a problem of portability and high dependability on the need for a power supply. The system developed in this project will make use of 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

### 2.3 COMPONENTS REVIEW

#### 2.3.1 Fingerprint Module

A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. Many technologies have been used including optical, capacitive, RF, thermal, piezoresistive, ultrasonic, piezoelectric, MEMS. The fingerprint module we are going to employ is an optical biometric fingerprint reader/sensor (R307) module with TTL UART interface for direct connections to a microcontroller UART. It can store the fingerprint data in the module and can be configured in 1:1 or 1: N mode for identifying a person. This module can directly interface with any 3.3V or 5V microcontrollers, but a suitable level converter/serial adapter is required for interfacing with the serial port of a PC. R307 Fingerprint Module consists of optical fingerprint sensor, high-speed DSP processor, high-performance fingerprint alignment algorithm, high-capacity FLASH chips and other hardware and software composition, stable performance, simple structure, with fingerprint entry, image processing, fingerprint matching, search and template storage and other function.

Fingerprint processing includes two parts, fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1:N). When enrolling, user needs to enter the finger two times. The system will process the two finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through the sensor and system will generate a template of the finger and compare it with templates of the finger library (database in this case).

For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1:N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure.

The module itself does all complex tasks behind reading and identifying the fingerprints with an on-board optical sensor and fingerprint algorithm. When simple commands are sent, the fingerprint scanner can store different fingerprints.

The database of prints can be downloaded from the unit and distributed to other modules. Although a number of fingerprint reader/sensor modules with slight variations are available now, most have a 4-pin external connection interface. By way of the serial interface, fingerprint reader/sensor module can communicate with a microcontroller that runs on 3.3V or 5V power supply. TX/TD pin of the module connects with RXD (RX-IN pin of the microcontroller), and RX/RD pin connects with TXD (TX-OUT pin of the microcontroller).

#### 2.3.2 Microcontroller

A microcontroller is a self-contained system with peripherals, memory and a processor that can be used as an embedded system. A microcontroller contains one or more CPUs (processor cores) along with memory and programmable input/output peripherals. In this work arduino microcontroller (ATmega328) is used. Arduino is an open-source electronics platform based on easy-to-use hardware and software. Arduino boards are able to read inputs - light on a sensor, a finger on a button, or a Twitter message - and turn it into an output - activating a motor, turning on an LED, publishing something online. The board can be told what to do by sending a set of instructions to the microcontroller on the board. To do so the Arduino programming language (based on Wiring), and the Arduino Software (IDE), based on Processing are used. Arduino is used in this project because of the advantages it offers which include:

* **Inexpensive** - Arduino boards are relatively inexpensive compared to other microcontroller platforms. The least expensive version of the Arduino module can be assembled by hand, and even the pre-assembled Arduino modules cost less than $50
* **Cross-platform** - The Arduino Software (IDE) runs on Windows, Macintosh OSX, and Linux operating systems. Most microcontroller systems are limited to Windows.
* **Simple, clear programming environment** - The Arduino Software (IDE) is easy-to-use for beginners, yet flexible enough for advanced users to take advantage of as well.
* **Open source and extensible software** - The Arduino software is published as open source tools, available for extension by experienced programmers. The language can be expanded through C++ libraries, and people wanting to understand the technical details can make the leap from Arduino to the AVR C programming language on which it's based. Similarly, you can add AVR-C code directly into your Arduino programs if you want to.
* **Open source and extensible hardware** - The plans of the Arduino boards are published under a Creative Commons license, so experienced circuit designers can make their own version of the module, extending it and improving it. Even relatively inexperienced users can build the breadboard version of the module in order to understand how it works and save money.

##### 2.3.2.1 ATMega328 Hardware

Most Arduino boards consist of an Atmel 8-bit AVR microcontroller (ATmega8, ATmega168, ATmega328, ATmega1280, ATmega2560) with varying amounts of flash memory, pins, and features. The 32-bit Arduino Due, based on the Atmel SAM3X8E was introduced in 2012. The boards use single or double-row pins or female headers that facilitate connections for programming and incorporation into other circuits. These may connect with add-on modules termed *shields*. Multiple and possibly stacked shields may be individually addressable via an I²C serial bus. Most boards include a 5V linear regulator and a 16 MHz crystal oscillator or ceramic resonator. Some designs, such as the LilyPad, run at 8 MHz and dispense with the onboard voltage regulator due to specific form-factor restrictions.

Arduino microcontrollers are pre-programmed with a boot loader that simplifies uploading of programs to the on-chip flash memory. The default bootloader of the Arduino UNO is the optiboot bootloader. Boards are loaded with program code via a serial connection to another computer. Some serial Arduino boards contain a level shifter circuit to convert between RS-232 logic levels and transistor–transistor logic (TTL) level signals. Current Arduino boards are programmed via Universal Serial Bus (USB), implemented using USB-to-serial adapter chips such as the FTDI FT232. Some boards, such as later-model Uno boards, substitute the FTDI chip with a separate AVR chip containing USB-to-serial firmware, which is reprogrammable via its own ICSP header. Other variants, such as the Arduino Mini and the unofficial Boarduino, use a detachable USB-to-serial adapter board or cable, Bluetooth or other methods. When used with traditional microcontroller tools, instead of the Arduino IDE, standard AVR in-system programming (ISP) programming is used.



**Fig 2.4: An official Arduino Uno R2 with description of the I/O locations.**

The Arduino board exposes most of the microcontroller's I/O pins for use by other circuits. The *Diecimila,* *Duemilanove*, and current *Uno* provide 14 digital I/O pins, six of which can produce pulse-width modulated signals, and six analog inputs, which can also be used as six digital I/O pins. These pins are on the top of the board, via female 0.1-inch (2.54 mm) headers. Several plug-in application shields are also commercially available. The Arduino Nano, and Arduino-compatible Bare Bones Board and Boarduino boards may provide male header pins on the underside of the board that can plug into solderless breadboards. The Atmel 8-bit AVR RISC-based microcontroller used in this project combines 32 kB ISP flash memory with read-while-write capabilities, 1 kB EEPROM, 2 kB SRAM, 23 general purpose I/O lines, 32 general purpose working registers, three flexible timer/counters with compare modes, internal and external interrupts, serial programmable USART, a byte-oriented 2-wire serial interface, SPI serial port, 6-channel 10-bit A/D converter (8-channels in TQFP and QFN/MLF packages), programmable watchdog timer with internal oscillator, and five software selectable power saving modes. The device operates between 1.8-5.5 volts. The device achieves throughput approaching 1 MIPS per MHz.

##### 2.3.2.2 Microcontroller Software

A program for Arduino hardware may be written in any programming language with compilers that produce binary machine code for the target processor. Atmel provides a development environment for their 8-bit AVR and 32-bit ARM Cortex-M based microcontrollers: AVR Studio (older) and Atmel Studio (newer).

##### 2.3.2.3 IDE

The Arduino integrated development environment (IDE) is a cross-platform application (for Windows, macOS, Linux) that is written in the Java programming language. It originated from the IDE for the languages Processing and Wiring. It includes a code editor with features such as text cutting and pasting, searching and replacing text, automatic indenting, brace matching, and syntax highlighting, and provides simple one-click mechanisms to compile and upload programs to an Arduino board. It also contains a message area, a text console, a toolbar with buttons for common functions and a hierarchy of operation menus. The source code for the IDE is released under the GNU General Public License, version 2.

The Arduino IDE supports the languages C and C++ using special rules of code structuring. The Arduino IDE supplies a software library from the Wiring project, which provides many common input and output procedures. 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() into an executable cyclic executive program with the GNU toolchain, also included with the IDE distribution. The Arduino IDE employs the program *avrdude* to convert the executable code into a text file in hexadecimal encoding that is loaded into the Arduino board by a loader program in the board's firmware.

A program written with the Arduino IDE is called a *sketch*. Sketches are saved on the development computer as text files with the file extension **.ino**. Arduino Software (IDE) pre-1.0 saved sketches with the extension **.pde**.

A minimal Arduino C/C++ program consist of only two functions:

* *setup()*: This function is called once when a sketch starts after power-up or reset. It is used to initialize variables, input and output pin modes, and other libraries needed in the sketch.
* *loop()*: After *setup()* function exits (ends), the *loop()* function is executed repeatedly in the main program. It controls the board until the board is powered off or is reset

#### 2.3.3 Bluetooth Module

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs). Invented by Dutch electrical engineer Jaap Haartsen, working for telecom vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables.

Bluetooth operates at frequencies between 2402 and 2480 MHz, or 2400 and 2483.5 MHz including guard bands 2 MHz wide at the bottom end and 3.5 MHz wide at the top. This is in the globally unlicensed (but not unregulated) industrial, scientific and medical (ISM) 2.4 GHz short-range radio frequency band. Bluetooth uses a radio technology called frequency-hopping spread spectrum. Bluetooth divides transmitted data into packets, and transmits each packet on one of 79 designated Bluetooth channels. Each channel has a bandwidth of 1 MHz. It usually performs 800 hops per second, with Adaptive Frequency-Hopping (AFH) enabled.

A master BR/EDR Bluetooth device can communicate with a maximum of seven devices in a piconet (an ad-hoc computer network using Bluetooth technology), though not all devices reach this maximum. The devices can switch roles, by agreement, and the slave can become the master (for example, a headset initiating a connection to a phone necessarily begins as master—as initiator of the connection—but may subsequently operate as slave).

The Bluetooth Core Specification provides for the connection of two or more piconets to form a scatternet, in which certain devices simultaneously play the master role in one piconet and the slave role in another.

At any given time, data can be transferred between the master and one other device (except for the little-used broadcast mode). The master chooses which slave device to address; typically, it switches rapidly from one device to another in a round-robin fashion. Since it is the master that chooses which slave to address, whereas a slave is (in theory) supposed to listen in each receive slot, being a master is a lighter burden than being a slave. Being a master of seven slaves is possible; being a slave of more than one master is possible. The specification is vague as to required behavior in scatternets.

Bluetooth is a standard wire-replacement communications protocol primarily designed for low power consumption, with a short range based on low-cost transceiver microchips in each device. Because the devices use a radio (broadcast) communications system, they do not have to be in visual line of sight of each other; however, a quasi-optical wireless path must be viable. Range is power-class-dependent, but effective ranges vary in practice.

|  |  |  |  |
| --- | --- | --- | --- |
| **Class** | **Max. permitted power** | | **Typ. range (m)** |
| **(mW)** | **(dBm)** |
| **1** | 100 | 20 | ~100 |
| **2** | 2.5 | 4 | ~10 |
| **3** | 1 | 0 | ~1 |
| **4** | 0.5 | −3 | ~0.5 |

***Table 2.1 Ranges of Bluetooth devices by class***

Officially Class 3 radios have a range of up to 1 meter (3 ft.), Class 2, most commonly found in mobile devices, 10 meters (33 ft.), and Class 1, primarily for industrial use cases,100 meters (300 ft.).[2] Bluetooth Marketing qualifies that Class 1 range is in most cases 20–30 meters (66–98 ft.), and Class 2 range 5–10 meters (16–33 ft.). The actual range achieved by a given link will depend on the qualities of the devices at both ends of the link, as well as the air conditions in between, and other factors.

The effective range varies depending on propagation conditions, material coverage, production sample variations, antenna configurations and battery conditions. Most Bluetooth applications are for indoor conditions, where attenuation of walls and signal fading due to signal reflections make the range far lower than specified line-of-sight ranges of the Bluetooth products.

HC‐05 module is an easy to use Bluetooth SPP (Serial Port Protocol) module, designed for transparent wireless serial connection setup. The HC-05 Bluetooth Module can be used in a Master or Slave configuration, making it a great solution for wireless communication. This serial port Bluetooth module is fully qualified Bluetooth V2.0+EDR (Enhanced Data Rate) 3Mbps Modulation with complete 2.4GHz radio transceiver and baseband. It uses CSR Bluecore 04‐External single chip Rluetooth system with CMOS technology and with AFH (Adaptive Frequency Hopping Feature). By default the factory setting is SLAVE. The Role of the module (Master or Slave) can be configured only by AT COMMANDS. The slave modules cannot initiate a connection to another Bluetooth device, but can accept connections. Master module can initiate a connection to other devices.

##### 2.3.3.1 PIN DESCRIPTION

The HC-05 Bluetooth Module has 6 pins. They are as follows:

**ENABLE**:

When enable is pulled LOW, the module is disabled which means the module will not turn on and it fails to communicate. When enable is left open or connected to 3.3V, the module is enabled i.e the module remains on and communication also takes place.

**Vcc**:

Supply Voltage 3.3V to 5V

**GND**:

Ground pin

**TXD & RXD**:

These two pins acts as an UART interface for communication

**STATE**:

It acts as a status indicator. When the module is not connected to/paired with any other Bluetooth device, signal goes Low. At this low state, the led flashes continuously which denotes that the module is not paired with other device. When this module is connected to/paired with any other Bluetooth device, the signal goes High. At this high state, the led blinks with a constant delay say for example 2s delay which indicates that the module is paired.

**BUTTON SWITCH**:

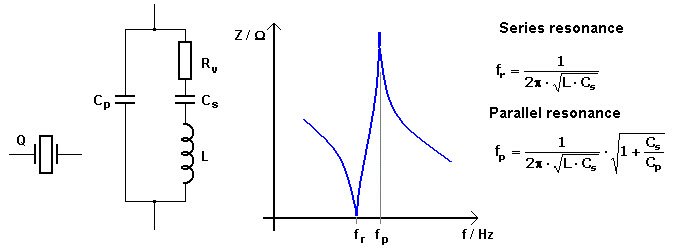
This is used to switch the module into AT command mode. To enable AT command mode, press the button switch for a second. With the help of AT commands, the user can change the parameters of this module but only when the module is not paired with any other BT device. If the module is connected to any other bluetooth device, it starts to communicate with that device and fails to work in AT command mode.

#### 2.3.4 Crystal Oscillator

A crystal oscillator is an electronic oscillator circuit that uses the mechanical resonance of a vibrating crystal of piezoelectric material to create an electrical signal with a precise frequency. This frequency is often used to keep track of time, as in quartz wristwatches, to provide a stable clock signal for digital integrated circuits, and to stabilize frequencies for radio transmitters and receivers. A crystal oscillator, particularly one made of quartz crystal, works by being distorted by an electric field when voltage is applied to an electrode near or on the crystal. This property is known as electrostriction or inverse piezoelectricity. When the field is removed, the quartz - which oscillates in a precise frequency - generates an electric field as it returns to its previous shape, and this can generate a voltage. The result is that a quartz crystal behaves like an RLC circuit.

Crystal oscillator circuit usually works on the principle of the inverse piezoelectric effect. The applied electric field will produce a mechanical deformation across some materials. Thus, it utilizes the vibrating crystal’s mechanical resonance that is made with a piezoelectric material for generating an electrical signal of a particular frequency.

Usually quartz crystal oscillators are highly stable, consists of good quality factor (Q), they are small in size, and are economically related. Hence, quartz crystal oscillator circuits are more superior compared to other resonators like LC circuits, turning forks.



***Fig 2.5: Diagram of the crystal and equivalent circuit***

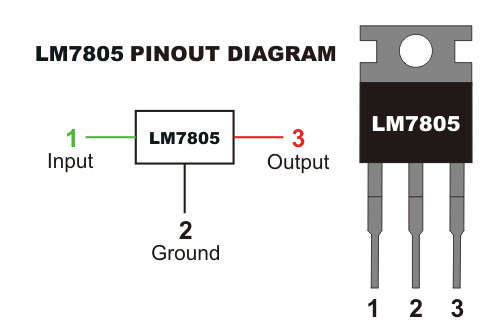
The equivalent electrical circuit also describes the crystal action of the crystal. This is shown above. The basic components used in the circuit, inductance L represents crystal mass, capacitance Cs represents compliance, and Cp is used to represent the capacitance that is formed because of crystal’s mechanical moulding, resistance R represents the crystal’s internal structure friction, The quartz crystal oscillator circuit diagram consists of two resonances such as series and parallel resonance, i.e., two resonant frequencies.

Generally, in the design of microprocessors and microcontrollers, crystal oscillators are used for the sake of providing the clock signals. A 16MHz crystal ships in with the ATMega328 microcontroller. This particular crystal oscillator which is having cycle rate at 16MHzis used to generate clock pulses which are required for the synchronization of all the internal operations in the microcontroller.

#### 2.3.5 Voltage Regulator

A voltage regulator is an electronic circuit that provides a stable DC voltage independent of the load current, temperature and AC line voltage variations. A voltage regulator may use a simple feed-forward design or may include negative feedback. There are two types of voltage regulators. Linear and switching voltage regulators. Linear voltage regulator acts as a voltage divider and it’s the most commonly used type when designing low power and low cost circuit. Switching regulators are used when there is a large difference between input and output voltage.

The **voltage regulator IC 7805** is actually a member of 78xx series of voltage regulator ICs. It is a fixed linear voltage regulator. The xx present in 78xx represents the value of the fixed output voltage that the particular IC provides. For 7805 IC, it is +5V DC regulated power supply. This regulator IC also adds a provision for a heat sink. The input voltage to this voltage regulator can be up to 35V, and this IC can give a constant 5V for any value of input less than or equal to 35V which is the threshold limit.



***Fig 2.6: Voltage regulator (7805) pin diagram***

PIN 1-INPUT

The function of this pin is to give the input voltage. It should be in the range of 7V to 35V. We apply an unregulated voltage to this pin for regulation. For 7.2V input, the PIN achieves a maximum efficiency.

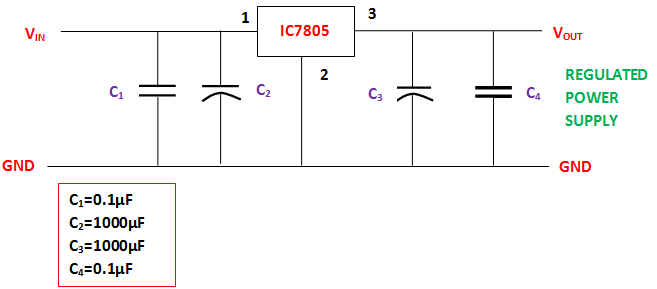
PIN 2-GROUND

For output and input, this pin is equally neutral (0V).

PIN 3-OUTPUT

This pin is used to take the regulated output.

Voltage regulator is used in the power supply circuit to provide a constant 5V dc supply to the microcontroller, fingerprint module and the bluetooth module.



***Fig 2.7: Power supply circuit***

#### 2.3.6 Capacitors

A capacitor is a passive two-terminal electrical component that stores potential energy in an electric field. The physical form and construction of practical capacitors vary widely and many capacitor types are in common use. Most capacitors contain at least two electrical conductors often in the form of metallic plates or surfaces separated by a dielectric medium. A conductor may be a foil, thin film, sintered bead of metal, or an electrolyte. The non-conducting dielectric acts to increase the capacitor's charge capacity. Materials commonly used as dielectrics include glass, ceramic, plastic film, paper, mica, and oxide layers. Capacitors are widely used as parts of electrical circuits in many common electrical devices. Unlike a resistor, an ideal capacitor does not dissipate energy.



***Fig 2.8: Capacitor***

In this project, capacitors are used in two major areas – decoupling (bypass) in the IC and power supply filtering. A decoupling capacitor’s job is to suppress high-frequency noise in power supply signals. They take tiny voltage ripples, which could otherwise be harmful to delicate ICs, out of the voltage supply. Also since they resist a sudden change in voltage, they are connected in parallel in the power supply circuit to reduce ripples in the power supply.

#### 2.3.7 Resistors

A resistor is a passive two-terminal electrical component that implements electrical resistance as a circuit element. In electronic circuits, resistors are used to reduce current flow, adjust signal levels, to divide voltages, bias active elements, and terminate transmission lines, among other uses.

In this project, resistors are used in LED current limiting. Resistors are key in making sure LEDs don’t blow up when power is applied. By connecting a resistor in series with the LED, current flowing through the two components can be limited to a safe value.

# CHAPTER THREE

## METHODOLOGY

### 3.0 INTRODUCTION

This chapter will cover a detailed explanation of methodology adopted to make this project complete and working well.

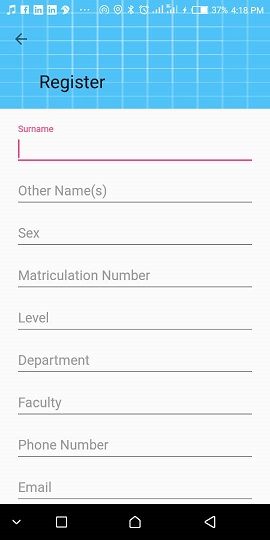
### 3.1 CIRCUIT MODE OF OPERATION

The working principle of the project can be classified into two stages:

* 1. Enrollment stage
  2. Verification stage

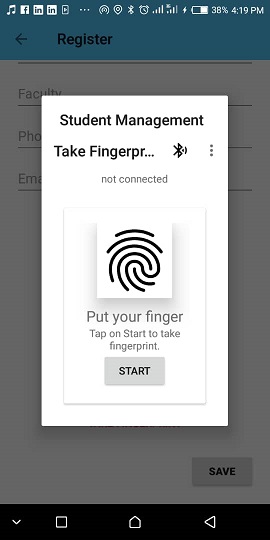
#### 3.1.1 Enrollment Stage

The enrollment stage is the stage where students’ details are registered into the system. During the enrollment stage, the android mobile device is connected to the circuit via Bluetooth. The student’s record is entered into the system via the interface in the android device shown below.



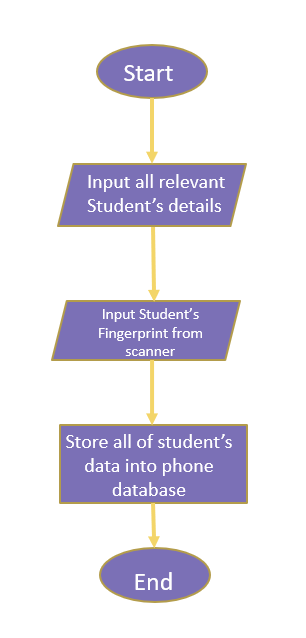
***Fig 3.1 Registration interface.***

The required details include the student’s surname, other names, sex, matriculation number, level, etc. The matriculation number is unique and must be entered because it is used in saving the student’s passport. Also it prevents the student’s passport form being taken twice as it fetches the previously stored passport when registering the student for another course. It also prevents wastage of memory slot in the mobile device. Thereafter, the passport of the student is taken. Finally, the fingerprint is taken with the fingerprint module twice and stored. The interface for taking the fingerprint is shown below.



***Fig 3.2: Fingerprint scanning interface.***

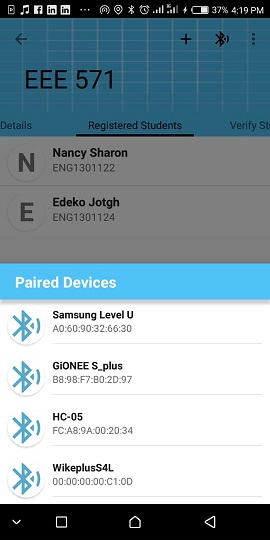
The details collected are then stored in the database for that student.



**Fig 3.3: Enrollment Flow Chart**

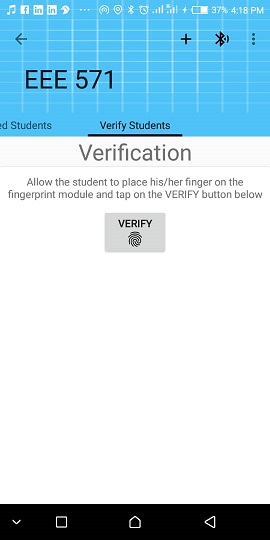
#### 3.1.2 Verification Stage

During the verification stage, the android device is connected to the circuit again via Bluetooth. This is done by selecting the Bluetooth module in the list of paired devices as shown below.



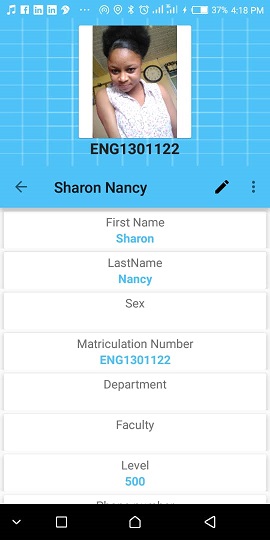
***Fig 3.4 Interface for selection of Bluetooth module.***

The course to verify the student against is selected. The student places his/her finger on the fingerprint scanner, and a “verify” command is sent from the mobile device to the fingerprint module through the microcontroller. The interface for the verification process is shown below.

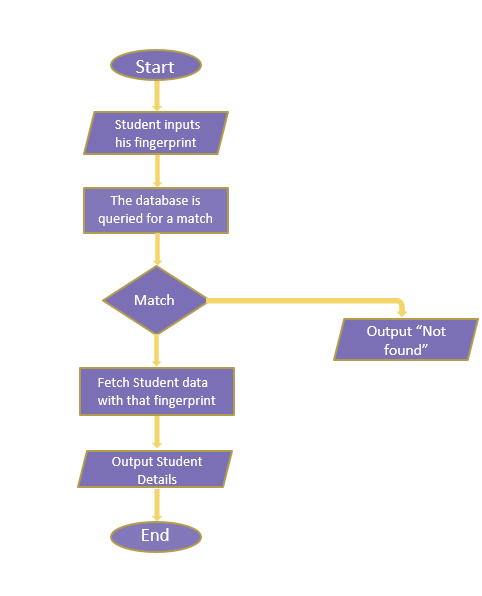


***Fig 3.5: Verification interface.***

The fingerprint on the scanner is compared with prints in the memory. If a match is found, it pops open the student’s info indicating that the student is eligible for the examination. If no match is found, an error message is displayed. The verified student’s interface is shown below.



***Fig 3.6: Student’s record after verification.***



**Fig 3.7: Verification flow chart**

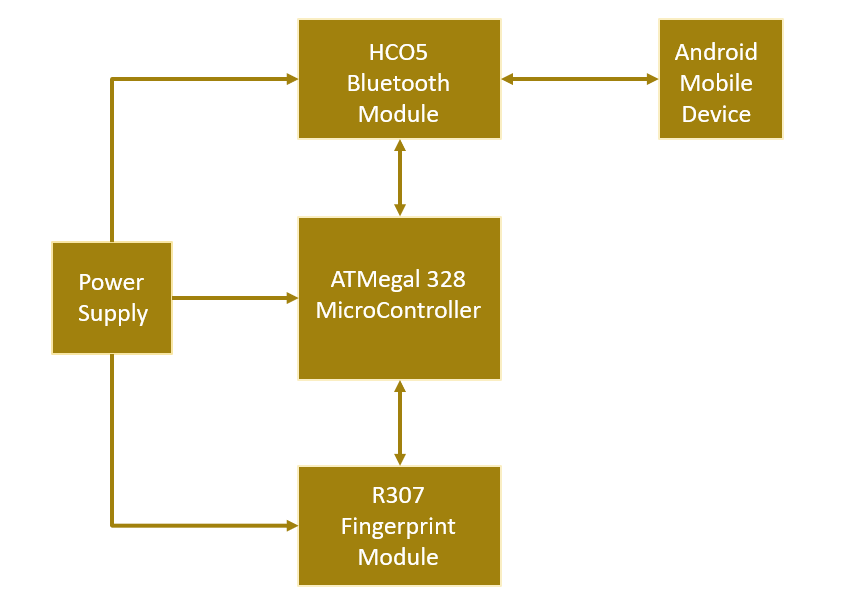
### 3.2 SYSTEM DESIGN

The system design can be classified into two categories:

1. Hardware Design of the system
2. Software Design of the System

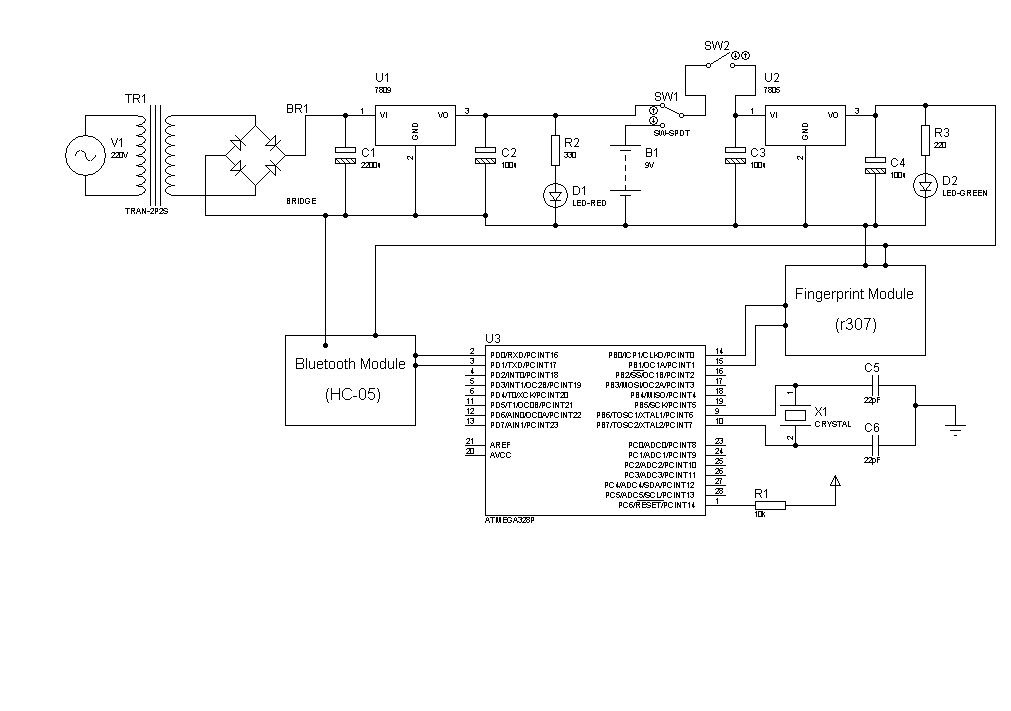
#### 3.2.1 HARDWARE DESIGN OF THE SYSTEM

The hardware system comprises of the microcontroller, fingerprint module, Bluetooth module, crystal oscillator, resistors, LEDs and capacitors. This section describes how these components interact and fit together to make up our fingerprint authentication system. A simple block diagram to illustrate how the major components of the system interact is shown below.



**Fig 3.8: Block Diagram**

The complete circuit diagram of the project is shown below.

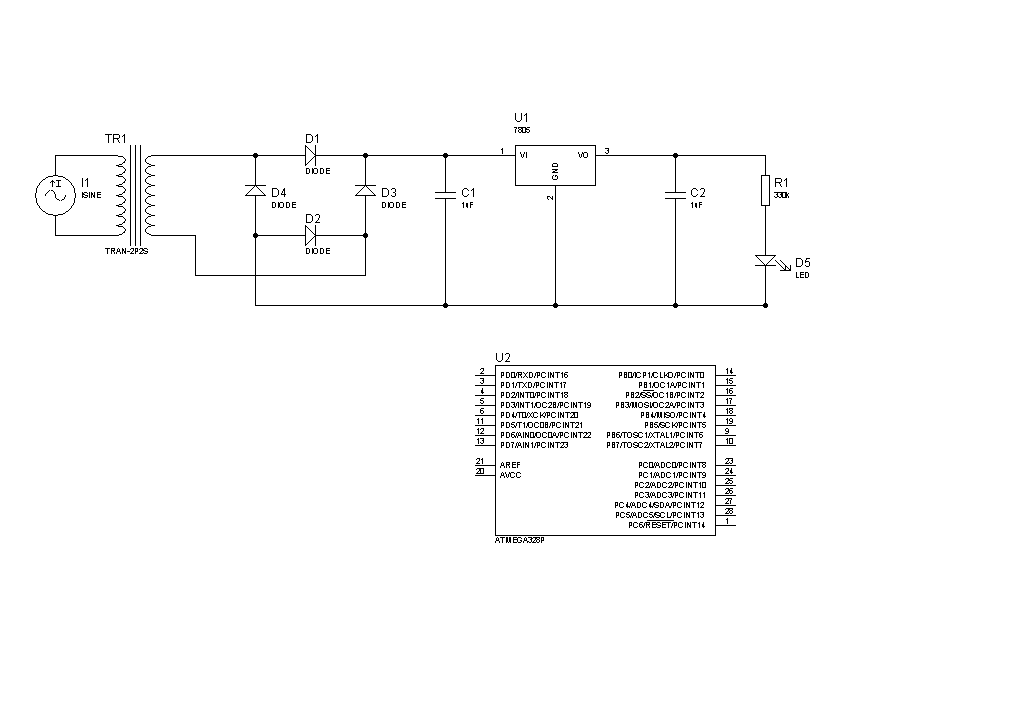


***Fig 3.9: Circuit diagram***

##### 3.2.1.1 POWER SUPPLY

For the purpose of this project, a dual power supply system is employed. A 9V battery source and a power supply circuit. The reason for this choice is due to the short life span of the battery and the instability of power supply. The battery provides the power required by the microcontroller, fingerprint module and the Bluetooth module when power supply is unavailable. However, these components make use of standard 5V for their operation. Therefore, a 7805 IC voltage regulator is employed to ensure a constant voltage supply of 5V gets to the various components.

The power supply circuit is shown below.



***Fig 3.10: Power supply circuit***

The transformer is a 220/18V step down transformer. The secondary is chosen to be 18V because of the unstable voltage from the supply authority at the primary. C1 is 2200µF while C2 is 1000 µF. R1 is 330Ω. These values are specified in the datasheet of the voltage regulator (7805) used. The LED indicates the availability of power in the circuit. The current through the LED is given by:

Where V = voltage in the circuit.

Vd = forward bias voltage drop (1.8V).

R = resistance of the resistor.

From the formula above, the current limiting resistor needed with the LED with a chosen current value of 0.9mA is

This current is within the safe limit of the LED.

##### 3.2.1.2 SWITCHING

Two switches are used in the overall circuit. One switch (SW1) switches between main supply and battery while the other powers the main components of the circuit. The first switch (SW1) is a single pole double throw switch. One of the throw terminals is connected to the battery while the other is connected to the supply from the mains. The pole of this switch is connected to the pole of the other switch (SW2) that powers the main components. The output (throw) is connected to the input of the voltage regulator (7805).

##### 3.2.1.3 FINGERPRINT MODULE

This component has an optical sensor, which means it is capable of sensing the presence of a finger. It then renders the image, finds the features of that finger and then searches in its memory for a fingerprint with the same characteristics. All of this is achieved in less than a second. It can be connected to a microcontroller or a system with TTL serial, and packets of data is sent to take photos, detect prints, hash and search. It also consists of a high-speed DSP processor, high-performance fingerprint alignment algorithm, high-capacity FLASH chips and other hardware and software composition. It has a stable performance and a simple structure.

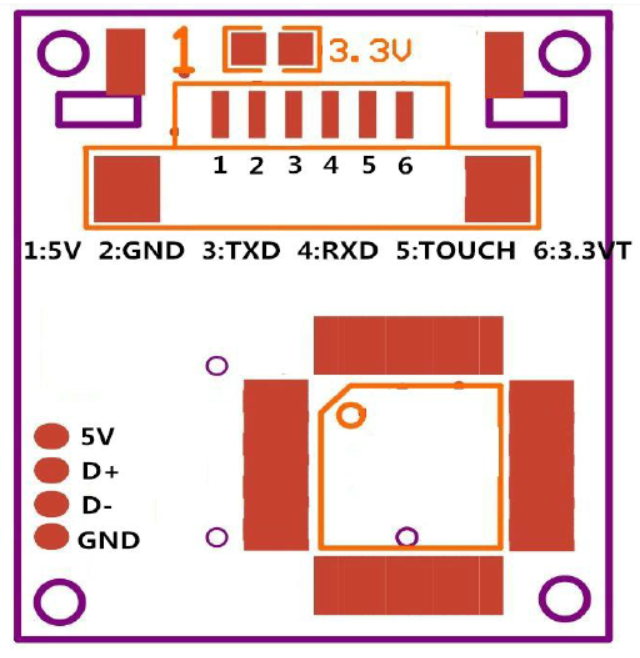
|  |  |
| --- | --- |
| **Power** | DC 4.2V-6V |
| **Working Current** | Typical: 50mA |
| **Image Acquiring Time** | <0.5s |
| **Storage Capacity** | 1000 |
| **False Acceptance Rate** | <0.001% |
| **False Rejection Rate** | <0.1% |
| **Average Search Time** | < 1s (1:1000) |
| **Interface** | UART(TTL logical level)/ USB 2.0 |
| **Matching Mode** | 1:1 and 1:N |
| **Character File Size** | 256 bytes |
| **Template Size** | 512 bytes |

***Table 3.1 Fingerprint module specifications.***

|  |  |  |  |
| --- | --- | --- | --- |
| Pin Number | Name | Type | Function Description |
| 1 | 5V | in | Power input (DC 4.2V-6V) |
| 2 | GND | - | Signal ground. Connected to power ground |
| 3 | TXD | out | Data output. TTL logical level |
| 4 | RXD | in | Data input. TTL logical level |
| 5 | Touch | out | Finger detection signal (maximum output current: 50mA) |
| 6 | 3.3V | In | Finger detection power (DC3.3V - 5V, I about 5uA) |

***Table 3.2 Fingerprint module pin description***

**Fig 3.11: R307 Fingerprint Module Pin Description**



**Hardware Connection**

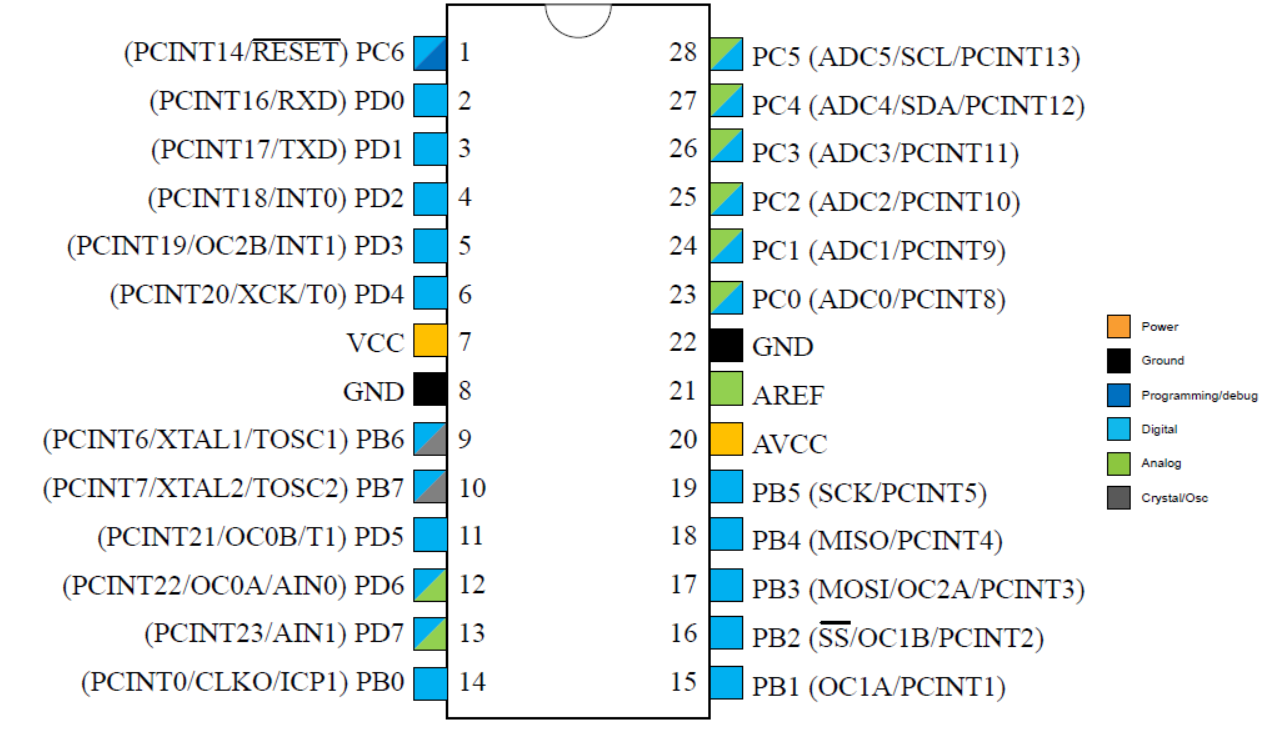
Via serial interface, the Module is connected with the Microcontroller unit of 5V power: TXD (pin 3 of P1) connects with RXD (receiving pin of MCU), RXD (pin 4 of P1) connects with TXD (transferring pin of MCU). Should the upper computer (Microcontroller) be in RS-232 mode, a level converting circuit MAX232 is added between the Module and Microcontroller.

##### 3.2.1.4 ATMEGA 328 MICROCONTROLLER

**ATmega328**is an eight (8) bit Microcontroller. It can handle the data sized of up to eight (8) bits. It is an AVR based micro-controller. Its built-in internal memory is around 32KB. It operates ranging from 3.3V to 5V. It has an ability to store the data even when the electrical supply is removed from its biasing terminals. Its excellent features include the cost efficiency, low power dissipation, programming lock for security purposes, and real timer counter with separate oscillator.

**Specification**

The ATmega328/P provides the following features: 32Kbytes of In-System Programmable Flash with Read-While-Write capabilities, 1Kbytes EEPROM, 2Kbytes SRAM, 23 general purpose I/O lines, 32 general purpose working registers, Real Time Counter (RTC), three flexible Timer/Counters with compare modes and PWM, 1 serial programmable USARTs , 1 byte-oriented 2-wire Serial Interface (I2C), a 6-channel 10-bit ADC (8 channels in TQFP and QFN/MLF packages) , a programmable Watchdog Timer with internal Oscillator, an SPI serial port, and six software selectable power saving modes. The Idle mode stops the CPU while allowing the SRAM, Timer/Counters, SPI port, and interrupt system to continue functioning. The Power-down mode saves the register contents but freezes the Oscillator, disabling all other chip functions until the next interrupt or hardware reset. In Power-save mode, the asynchronous timer continues to run, allowing the user to maintain a timer base while the rest of the device is sleeping. The ADC Noise Reduction mode stops the CPU and all I/O modules except asynchronous timer and ADC to minimize switching noise during ADC conversions. In Standby mode, the crystal/resonator oscillator is running while the rest of the device is sleeping. This allows very fast start-up combined with low power consumption. In Extended Standby mode, both the main oscillator and the asynchronous timer continue to run.



**Fig 3.12: ATMega328 Microcontroller pins description**

**Pin Descriptions**

* **VCC:** Digital supply voltage.
* **GND:** Ground.
* **Port B (PB[7:0]) XTAL1/XTAL2/TOSC1/TOSC2**

Port B is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port B output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port B pins that are externally pulled low will source current if the pull-up resistors are activated. The Port B pins are tri-stated when a reset condition becomes active, even if the clock is not running. Depending on the clock selection fuse settings, PB6 can be used as input to the inverting Oscillator amplifier and input to the internal clock operating circuit.

Depending on the clock selection fuse settings, PB7 can be used as output from the inverting Oscillator amplifier. If the Internal Calibrated RC Oscillator is used as chip clock source, PB[7:6] is used as TOSC[2:1] input for the Asynchronous Timer/Counter2 if the AS2 bit in ASSR is set.

* **Port C (PC[5:0])**

Port C is a 7-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The PC[5:0] output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port C pins that are externally pulled low will source current if the pull-up resistors are activated. The Port C pins are tri-stated when a reset condition becomes active, even if the clock is not running.

* **PC6/RESET**

If the RSTDISBL Fuse is programmed, PC6 is used as an I/O pin. Note that the electrical characteristics of PC6 differ from those of the other pins of Port C. If the RSTDISBL Fuse is unprogrammed, PC6 is used as a Reset input. A low level on this pin for longer than the minimum pulse length will generate a Reset, even if the clock is not running. Shorter pulses are not guaranteed to generate a Reset. The various special features of Port C are elaborated in the *Alternate Functions of Port C* section.

* **Port D (PD[7:0])**

Port D is an 8-bit bi-directional I/O port with internal pull-up resistors (selected for each bit). The Port D output buffers have symmetrical drive characteristics with both high sink and source capability. As inputs, Port D pins that are externally pulled low will source current if the pull-up resistors are activated. The Port D pins are tri-stated when a reset condition becomes active, even if the clock is not running.

* **AVCC**

AVCC is the supply voltage pin for the A/D Converter, PC[3:0], and PE[3:2]. It should be externally connected to VCC, even if the ADC is not used. If the ADC is used, it should be connected to VCC through a low-pass filter. Note that PC[6:4] use digital supply voltage, VCC.

* **AREF**

AREF is the analog reference pin for the A/D Converter.

* **ADC[7:6] (TQFP and VFQFN Package Only)**

In the TQFP and VFQFN package, ADC[7:6] serve as analog inputs to the A/D converter. These pins are powered from the analog supply and serve as 10-bit ADC channels.

##### 3.2.1.5 HC-O5 BLUETOOTH MODULE

The **HC-05** is a very cool module which can add two-way (full-duplex) wireless functionality to projects. It can be used to communicate between two microcontrollers like Arduino or communicate with any device with Bluetooth functionality like a Phone or Laptop. In this project, it has been employed to communicate with an android device. The module communicates with the help of USART at 9600 baud rate hence it is easy to interface with any microcontroller that supports USART.

**Technical Specifications**

For this module to function adequately, it is required that the supply voltage is between 4 – 6V (typically 5V) and the operating current should be around 30mA. This module works within a distance range of 100m. It follows IEEE802.15.1 standardized protocol and it works with Serial communication (USART) and TTL compatible. It can operate in Master, Slave or Master/Slave mode and it uses Frequency-Hopping Spread spectrum (FHSS). It supports baud rates of 9600,19200,38400,57600,115200,230400,460800.

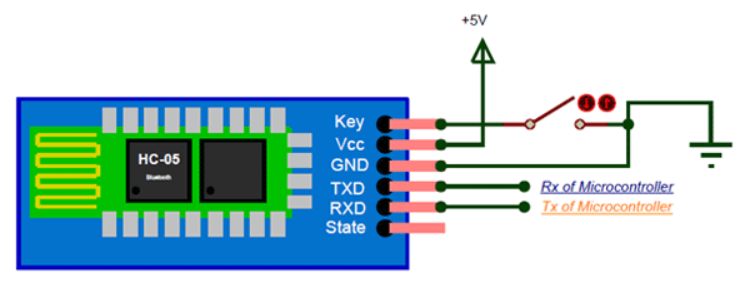
|  |  |  |
| --- | --- | --- |
| **Pin** | **Description** | **Function** |
| VCC | +5V | Connect to +5V |
| GND | Ground | Connect to Ground |
| TXD | UART\_TXD, Bluetooth serial signal sending pin | Connect with the MCU’s (Microcontroller) RXD PIN |
| RXD | UART\_RXD, Bluetooth serial signal receiving pin | Connect with the MCU’s (Microcontroller) TXD PIN |
| KEY | Mode switch input | If it is input low level or connect to the air, the module  Is at paired or communication mode. If it’s input high  Level, the module will enter to AT mode. |

**Table 3.3: Pin description of HC05 Bluetooth module**

**Module Operation**

The **HC-05** has two operating modes, one is the Data mode in which it can send and receive data from other Bluetooth devices and the other is the AT Command mode where the default device settings can be changed. The device can be operated in either of these two modes by using the key pin as explained in the pin description.

It is very easy to pair the HC-05 module with a microcontroller because it operates using the Serial Port Protocol (SPP). We simply power the module with +5V and connected the Rx pin of the module to the Tx of MCU and Tx pin of module to Rx of MCU as shown in the figure below



**Fig 3.13: HC-05 Bluetooth Module pin description**

#### 3.2.2 SOFTWARE DESIGN OF THE SYSTEM

Bulk of the work done in this project is software based, hence a thorough analysis of this part of the system is required. The software system of this project comprises of two parts, viz the C++ code for the ATMEGA 328 microcontroller unit and the JAVA code that was used in building the android mobile application.

The C++ code is used for communication with the fingerprint module. This communication is serial communication with a baud rate of 57600bps (Hangzhou Grow Technology co, 2011). The system resources of the module used in this communication are:

1. **Buffer:** There are an image buffer and two 512bytes character file buffer within the RAM space of the module. Read and write can be performed on both buffers using instructions. The image buffer serves for image storage and the image format is 256 \* 288 pixel in BMP. When transferring through UART, to quicken speed, only the upper 4 bits of the pixel is transferred (that is 16 grey degrees). When transferring through USB, the image is 8-bit pixel, that’s 256 grey degrees. Character file buffer, CharBuffer1, CharBuffer2, can be used to store both character file and template file. Contents of the above buffers will be lost at power off.
2. **Fingerprint Library:** The system sets aside a certain space within Flash for fingerprint template storage. Contents of the library remain at power off. Capacity of the library changes with the capacity of Flash, system will recognize the latter automatically. Fingerprint template’s storage in Flash is in sequential order. Assume the fingerprint capacity is N, then the serial number of template in library is 0, 1, 2, 3 … N. contents of the Library can only be accessed by template number.
3. **Data package length:** This parameter decides the max length of the transferring data package when communicating with upper computer (microcontroller). Its value is 0, 1, 2, 3, corresponding to 32 bytes, 64 bytes, 128 bytes, 256 bytes respectively.
4. **Module Address:** Each module has an identifying address. When communicating with upper computer, each instruction/data is transferred in data package form, which contains the address item. Module system only responds to data package whose address item value is the same with its identifying address. The address length is 4 bytes, and its default factory value is 0xFFFFFFFF. This address can be modified via instruction *SetAdder.* The new modified address remains at power off.

##### 3.2.2.1 COMMUNICATION PROTOCOL

The protocol defines the data exchanging format when the module communicates with microcontroller. The protocol and instruction sets applies for both UART and USB communication mode. For PC, USB interface is strongly recommended to improve the exchanging speed.

**Data package format**

The general format of data sent to and received from the module is shown below (Hangzhou Grow Technology co, 2011).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Header | Adder  (Address) | Package identifier | Package length | Package content  (instruction/data/parameter) | checksum |

**Definition of data package**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Symbol** | **Length** | **Description** | |
| Header | Start | 2 bytes | Fixed value of 0xEF01; High byte transferred first. | |
| Adder | ADDER | 4 bytes | Default value is 0xFFFFFFFF, which can be modified by command. High byte transferred first and at wrong adder value, module will reject to transfer. | |
| Package identifier | PID | 1 byte | 01H | Command Packet. |
| 02H | Data packet: Data packet shall not appear alone in executing process, must follow command packet or acknowledge packet. |
| 07H | Acknowledge packet; |
| 08H | End of Data packet. |
| Package length | LENGTH | 2 bytes | Refers to the length of package content (command packets and data packets) plus the length of Checksum (2 bytes). Unit is byte. Max length is 256 bytes. And high byte is transferred first. | |
| Package content | DATA |  | It can be commands, data, command’s parameters, acknowledge result, etc. (fingerprint character value, template are all deemed as data) | |
| Checksum | SUM | 2 bytes | The arithmetic sum of package identifier, package length and all package contents. Overflowing bits are omitted. High byte is transferred first. | |

***Table 3.4: Data package definition of fingerprint module.***

##### 3.2.2.2 CHECK AND ACKNOWLEDGEMENT OF DATA PACKAGE.

Commands are sent from microcontroller to the fingerprint module and the module acknowledges the command. Upon receipt of commands, module will report the commands execution status and results to the microcontroller through acknowledge packet. Acknowledge packet has parameters and may also have following data packet. The microcontroller can’t ascertain module’s package receiving status or command execution results unless through acknowledge packet sent from Module. Acknowledge packet includes 1 byte confirmation code and maybe also the returned parameter.

Confirmation code’s definition is

|  |  |
| --- | --- |
| Code | Meaning |
| 00H | Command execution complete. |
| 01H | Error when receiving data package |
| 02H | No finger on sensor |
| 03H | Fail to enroll the finger |
| 04H | Fail to generate character file due to over-disorderly fingerprint image |
| 05H | Fail to generate character file due the over-wet fingerprint image |
| 06H | Fail to generate character file due to over-disorderly fingerprint image |
| 07H | Fail to generate character file due to absence of character point or over-smallness of fingerprint image |
| 08H | Fingerprint does not match |
| 09H | Fail to find the matching finger |
| 0AH | Fail to combine the character file |
| 0BH | Addressing PageID is beyond the finger library |
| 0CH | Error when reading template from library or the template is invalid |
| 0DH | Error when uploading template |
| 0EH | Module can’t receive the following data packages |
| 0FH | Error when uploading image |
| 10H | Fail to delete the template |
| 11H | Fail to clear finger library |
| 13H | Wrong password |
| 15H | Fail to generate the image due to the absence of valid primary image |
| 18H | Error when writing flash |
| 19H | No definition error |
| 1AH | Invalid register number |
| 1BH | Incorrect configuration of register |
| 1DH | Fail to operate the communication port |
| 41H | No finger on sensor when add finger on second time |
| 42H | Fail to enroll the finger for second fingerprint add |
| 43H | Fail to generate character file due to absence of character point or over-smallness of fingerprint image for second fingerprint add |
| 44H | Fail to generate character file due to the over-disorderly fingerprint image for second fingerprint add |
| 45H | Duplicate fingerprint |

***Table 3.5: confirmation code definition.***

##### 3.2.2.3 MODULE INSTRUCTION SYSTEM

R307 series provide 23 instructions. Through combination of different instructions, application program may realize multi finger authentication functions. All commands/data are transferred in package format.

Instructions used in this project include (Hangzhou Grow Technology co, 2011):

1. **Fingerprint verification (GR\_Auto Search- 32H)**

This instruction matches the captured fingerprint with fingerprint library then return the result. Input parameters to this instruction include capture time, start bit number and search quantity. The returned parameters are the confirmation code, pageID of the match and the match score.

Command (or instruction) package format

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 1 byte | 2 bytes | 2 bytes | 2 bytes |
| Header | Address | Package ID | Package  Length | Instruction code | Time for capture | Start bit number | Search quantity | Checksum |
| 0xEF01 | 0Xffffffff | 01H | 08H | 32H | xxH | xxxxH | xxH | sum |

***Table 3.6: command package format for fingerprint verification.***

Acknowledgement data format

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 2 bytes | 2 bytes | 2 bytes |
| Header | Address | Package ID | Package length | Confirmation code | Page | Score | Checksum |
| 0xEF01 | 0Xffffffff | 07H | 07H | xxH | pageID | MatchScore | Sum |

***Table 3.7: Acknowledgement data format for fingerprint verification.***

Note

* Confirmation code = 00H: read complete
* Confirmation code = 01H: error when receiving package
* Confirmation code = 06H: fail to generate character file due to over-disordely fingerprint image.
* Confirmation code = 07H: fail to generate character file due to absence of character point or over-smallness of fingerprint image.
* Confirmation code = 09H: No matching in the library (both the pageID and matching score are 0).

1. **Collect finger image (GenImg-01H)**

Detects finger image and store the detected finger image in Image buffer while returning successful confirmation code. If there is no fingerprint, returned confirmation code would be “cant detect finger”. No input is passed to this instruction and the returned parameter is confirmation code(1 byte).

Command (or instruction) package format

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 2 bytes |
| Header | Address | Package ID | Package length | Instruction code | Checksum |
| 0xEF01 | 0Xffffffff | 01H | 03H | 01H | 05H |

***Table 3.8: command package format for collecting fingerprint.***

Acknowledgement package format

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 2 bytes |
| Header | Address | Package ID | Package length | confirmation code | Checksum |
| 0xEF01 | 0Xffffffff | 07H | 03H | xxH | sum |

***Table 3.9: Acknowledgement data format for collecting fingerprint.***

Note

* Confirmation code = 00H: finger collection success
* Confirmation code = 01H: error when receiving package
* Confirmation code = 02H: can’t detect finger
* Confirmation code = 03H: fail to collect finger

1. **Generate character file from image (Img2Tz-02H)**

Generates character file from the original finger image in ImageBuffer and store the file in CharBuffer1 or CharBuffer2. The bufferID is an input parameter to this instruction while the confirmation code is the return parameter.

Command (or instruction) package format:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 1 byte | 2 bytes |
| Header | Address | Package ID | Package length | Instruction code | Buffer number | Checksum |
| 0xEF01 | 0Xffffffff | 01H | 04H | 02H | BufferID | sum |

***Table 3.10: command package format for generating character file.***

BufferID of CharBuffer1 and CharBuffer2 are 1h and 2h respectively. Other values would be processed as CharBuffer2.

Acknowledge package format:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 2 bytes |
| Header | Address | Package ID | Package length | confirmation code | Checksum |
| 0xEF01 | 0Xffffffff | 07H | 03H | xxH | sum |

***Table 3.11: Acknowledgement data format for generating character file.***

Note

* Confirmation code = 00H: generate character file complete
* Confirmation code = 01H: error when receiving package
* Confirmation code = 06H: fail to generate character file due to the over-disorderly fingerprint image
* Confirmation code = 07H: fail to generate character file due to absence of character point or over-smallness of fingerprint image.
* Confirmation code = 15H: fail to generate the image due to absence of valid primary image.

1. **Generate template (RegModel-05H)**

This instruction combines information of character files from CharBuffer1 and CharBuffer2 and generate a template which is stored back in both CharBuffer1 and CharBuffer2. No input parameter is passed to this instruction and the confirmation code is the returned parameter.

Command (or instruction) package format

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 2 bytes |
| Header | Address | Package ID | Package length | Instruction code | Checksum |
| 0xEF01 | 0Xffffffff | 01H | 03H | 05H | 09H |

***Table 3.12: command package format for generating template.***

Acknowledge package format

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 2 bytes |
| Header | Address | Package ID | Package length | confirmation code | Checksum |
| 0xEF01 | 0Xffffffff | 07H | 03H | xxH | sum |

***Table 3.13: Acknowledgement data format for generating template.***

Note

* Confirmation code = 00H: operation success
* Confirmation code = 01H: error when receiving package
* Confirmation code = 0AH: fail to combine the character files. The character files don’t belong to one finger.

1. **Store the template (Store-06H)**

This instruction stores the template of the specified buffer (Buffer1/Buffer2) at the designated location of flash library. Input parameters to this instruction are the BufferID, PageID (flash location of the template, two bytes with high byte front and low byte behind) while the return parameter is the confirmation code.

Command (or instruction) package format

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 1 bytes | 2 bytes | 2 bytes |
| Header | Address | Package ID | Package length | Instruction code | Buffer number | Location number | Checksum |
| 0xEF01 | 0Xffffffff | 01H | 06H | 06H | BufferID | PageID | sum |

***Table 3.14: command package format for storing template.***

BufferID of CharBuffer1 and CharBuffer2 are 1h and 2h respectively.

Acknowledge package format

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 2 bytes |
| Header | Address | Package ID | Package length | confirmation code | Checksum |
| 0xEF01 | 0Xffffffff | 07H | 03H | xxH | sum |

***Table 3.15: Acknowledgement data format for storing template.***

Note

* Confirmation code = 00H: storage success.
* Confirmation code = 01H: error when receiving package
* Confirmation code = 0BH: addressing PageID is beyond the finger library
* Confirmation code = 18H: error when writing Flash.

1. **Empty finger library (Empty-0DH)**

This instruction deletes all templates in the flash library. It takes no input parameter and returns the confirmation code

Command (or instruction) package format

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 2 bytes |
| Header | Address | Package ID | Package length | Instruction code | Checksum |
| 0xEF01 | 0Xffffffff | 01H | 03H | 0DH | 0011H |

***Table 3.16: command package format for clearing the finger library.***

Acknowledge package format

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 2 bytes |
| Header | Address | Package ID | Package length | confirmation code | Checksum |
| 0xEF01 | 0Xffffffff | 07H | 03H | xxH | sum |

***Table 3.17: Acknowledgement data format for clearing the finger library.***

Note

* Confirmation code = 00H: empty success
* Confirmation code = 01H: error when receiving package
* Confirmation code = 11H: fail to clear finger library.

1. **Search the finger library (Search-04H)**

Searches the whole finger library for template that matches the one in the CharBuffer1 or CharBuffer2. When found, PageID will be returned. Input to this instruction are BufferID, StartPage (searching start address), PageNum (searching numbers) while the PageID (matching templates location) and confirmation code are return parameters.

Command (or instruction) package format

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 1 bytes | 2 bytes | 2 bytes | 2 bytes |
| Header | Address | Package ID | Package length | Instruction code | Buffer number | Parameter | Parameter | Checksum |
| 0xEF01 | 0Xffffffff | 01H | 08H | 04H | BufferID | StartPage | PageNum | sum |

***Table 3.18: command package format for searching the finger library.***

BufferID of CharBuffer1 and CharBuffer2 are 1h and 2h respectively. Other values would be processed as CharBuffer2.

Acknowledge package format

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 2 bytes | 4 bytes | 1 byte | 2 bytes | 1 byte | 2 bytes | 2 bytes | 2 bytes |
| Header | Address | Package ID | Package length | Confirmation code |  |  | Checksum |
| 0xEF01 | 0Xffffffff | 07H | 07H | xxH | PageID | MatchScore | sum |

***Table 3.19: Acknowledgement data format for searching the finger library.***

Note

* Confirmation code = 00H: found the matching finer.
* Confirmation code = 01H: error when receiving package
* Confirmation code = 09H: No matching in the library ( both the PageID and matching score are 0)

##### 3.2.3.4 Implementation of module instructions

The above instructions are implemented in the C++ code. It consists of two files. One header file and one cpp file. The header file holds the declaration of classes, methods and properties used in the project. In this file, *Arduino.h* and *SoftwareSerial.h* are included to enable us get access to the core Arduino library and also implement a SoftwareSerial communication between the modules. In the main C++ file the Fingerprint class defined in the header file is implemented. The Constructor of this class creates a new *SoftwareSerial* instance and stores it in a member variable declared as a pointer of *SoftwareSerial*. This instance is used to set the baud rate of the communication to that of the module (57600 bps) using the *begin* method on the *SoftwareSerial* instance. Other methods of the class are implemented as shown in the appendix of the project. This class is included in the main Arduino code (FP\_PROJECT.ino). The ino file has two main methods *setup* and *loop. Setup* is used to set the baud rate of the Bluetooth module to 9600 bps using the hardware *Serial* class of the Arduino library. A new FingerPrint object is created as a global variable in the ino file from which access to the FingerPrint class is derived. With this object, methods in the FingerPrint class implementing the fingerprint module instructions are called. *Loop* which runs continuously as long as power is available to the microcontroller checks if data is available from the Hardware Serial (Bluetooth in this case). If data is available, it reads the first character of the data using the *read()* method and stores it in a character variable. The value of this character determines what operation is to be performed. The following table gives the available operations depending of the value of this character.

|  |  |
| --- | --- |
| **Character Received** | **Operation** |
| R | Register |
| V | Verify |
| D | Upload character file to microcontroller |
| E | Empty the finger library |

***Table 3.20: Characters received and operations performed by module.***

Data from the Hardware Serial (Bluetooth module) is gotten from the mobile app (Java code). Also response from the module is sent to the mobile app via the Bluetooth module for users to carry out appropriate action depending on the response code gotten.

##### 3.2.3.5 ANDROID JAVA CODE

Data from the Hardware Serial (Bluetooth module) is gotten from the mobile app (Java code). Also response from the module is sent to the mobile app via the Bluetooth module for users to carry out appropriate action depending on the response code gotten.

The mobile app is targeted and compiled at android API level 22 but has support for lower API levels down to 15. These settings can be done in the *build.gradle* file of the app package. Also, all dependencies used in the development of the app are compiled in the same file. Android app development using Java is based on some Java classes called *ACTIVITIES*. These are the classes where views (user interface) are rendered, menu items are set, event listeners are declared and all other major processes within the app takes place.

The main file where communication is made with the Bluetooth module for registration and verification is the *TakeFingerprintFragment* class. This class has two methods: *onCreateView* and the compulsory method from implementing the *View.onClickListener* interface, *onClick.* The first method is where the Bluetooth connection view (user interface) is inflated and rendered. Also, an event listener is set on the **Start** button. Clicking on this button sends the command to the module to take fingerprint. The *onClick* method is where the main logic of taking fingerprint is done when the start button is clicked. First, a check is done to determine if record is being updated or inserted to determine the template ID where the fingerprint is to be stored in the module. If record is being updated, the old template ID is used, thereby replacing the old template in the module otherwise the next ID is generated by the *TemplateManager* class. Next a check is done to determine if the phone is connected to the module. If it is connected, the start button is disabled to prevent sending the command twice otherwise the user is prompted to hit the connect button. Thereafter the template ID with the required instruction is sent to the module to carry out the appropriate action. When feedback from the module is received, it is processed to determine if the required operation was carried out successfully. If an error occurs during the processing of the request, a toast is displayed telling the user what went wrong and the appropriate action to take in correcting the error.

# CHAPTER FOUR

## CONSTRUCTION, TESTING AND RESULTS

### 4.0 INTRODUCTION

This chapter highlights the procedures involved in the construction of this project. A careful step by step process of construction is enumerated as well as costing of various components is presented. Necessary testing and precautionary steps taken are also highlighted. Lastly, the result of this project is also discussed.

### 4.1 CONSTRUCTION

The crucial components – R307 Fingerprint Module, ATMEGA 328 Microcontroller and HC-05 Bluetooth Module were ordered from Ali Express Online Shop. They arrived two weeks later. The other components and tools such as the resistors, capacitors, crystal oscillator and Veroboard were ordered from a local electronic shop in Benin City. During the time of waiting for the arrival of the components from Ali Express, the User Interface of the android mobile app was designed. After acquiring all the required components, the complete circuit was first assembled on a bread board and tested to ensure proper functioning. Thereafter, the components were assembled on a Veroboard and soldered and then tested again.

#### 4.1.1 Soldering

Soldering is the process of joining two or more electronic parts together by melting solder around the connection. To ensure a good soldered joint, the components were first arranged on Veroboard. The soldering iron is then heated to a sufficiently high temperature. The hot soldering iron is then placed on the joint to be soldered for about 4 seconds to enable it heat up. Thereafter, solder lead is then run across the joint. The soldering iron is removed and the solder is allowed to cool down naturally. Care must be taken not to blow the solder, as this will result in a bad joint.

#### 4.1.2 Casing

After the construction and testing stage, the complete circuit was then enclosed in a small square box casing made of plastic. An opening was made on the casing for the fingerprint scanner. The casing is such that it can be easily opened for accessibility of the other components. Factors affecting the choice of casing were cost, availability, durability, resistance to external environmental conditions which may be cause damage to the circuit if exposed otherwise.

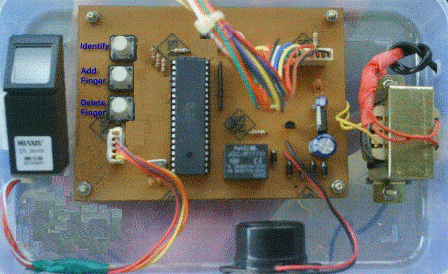


Figure 4.2: Completed Project with Casing

Figure 4.3: Casing opened showing enclosed components

#### 4.1.3 BILL OF ENGINEERING MEASUREMENT AND EVALUATION

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S/N** | **COMPONENT** | **QUANTITY** | **UNIT PRICE ( # )** | **TOTAL PRICE ( # )** |
| 1 | R307 Fingerprint Module | 1 | 2500 | 2500 |
| 2 | ATMega328 Microcontroller | 1 | 3000 | 3000 |
| 3 | HC-05 Bluetooth Module | 1 | 2000 | 2000 |
| 4 | Crystal Oscillator | 1 | 1000 | 1000 |
| 5 | Jumper Wires (set) | 3 | 600 | 1800 |
| 6 | 2.2kohms Resistor | 4 | 50 | 200 |
| 7 | Capacitor | 3 | 200 | 600 |
| 8 | Veroboard | 1 | 200 | 200 |
| 9 | Soldering Iron | 1 | 700 | 700 |
| 10 | Soldering Lead (Roll) | 1 | 500 | 500 |
| 11 | Box Casing | 1 | 600 | 600 |
| 12 | Mulitmeter | 1 | 2500 | 2500 |
| 13 | IC Holder | 1 | 200 | 200 |
| 14 | Miscellaneous |  |  | 6000 |
|  | **TOTAL COST** |  |  | **#40,000** |

***Table 4.1: Cost of components used.***

### 4.2 TESTING

Testing is a process used to identify the correctness, completeness, and quality of a developed system. It includes a set of activities conducted with the intent of finding errors in the system so that it could be corrected before the project is ascertained complete. The following tests were performed for this project.

#### 4.2.1 Circuit Connection Test

Several steps were taken to ensure the connection integrity of the circuit. Using a digital multimeter, open circuit test was carried out to check for continuity or otherwise.

Also, using the multimeter, short circuit test was carried out to determine if there was any bridge between board tracts or wires.

Lastly, also using a multimeter, the battery was tested to ensure its voltage was sufficient enough to deliver the 5V required by the components.

#### 4.2.2 Performance Test

This test was done to check the performance and reliability of the project. The system was tested with 17 student subjects. The students’ details and fingerprints were registered into the system under normal condition - clean finger, and thereafter authentication was tested under various conditions – wet finger, dirty finger and oily finger.

### 4.3 RESULT

#### 4.3.1 Circuit Connection Test Result

After testing various parts of the circuit, it was found that there was no open circuit connection in the circuit.

Similarly, there were no short-circuited components that needed to be addressed.

Lastly, after testing, the battery emf was found to be at 7.3V. Whilst this voltage level was sufficiently enough to supply the circuit component parts at the time of testing (which typically required just 5V), we replaced the battery with a new 9V battery from a brand with a good durability review.

#### 4.3.2 Performance Test Result

Below is a table showing the result of testing the system on the 17 students during verification for the different finger conditions.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S/N | CLEAN | WET | DIRTY | OILY |
| 1 | Success | Failure | Failure | Failure |
| 2 | Success | Failure | Success | Failure |
| 3 | Success | Failure | Failure | Failure |
| 4 | Success | Failure | Failure | Success |
| 5 | Success | Failure | Failure | Failure |
| 6 | Success | Failure | Success | Failure |
| 7 | Success | Failure | Failure | Failure |
| 8 | Success | Failure | Failure | Failure |
| 9 | Success | Success | Failure | Failure |
| 10 | Success | Failure | Failure | Failure |
| 11 | Success | Failure | Failure | Failure |
| 12 | Failure | Failure | Failure | Failure |
| 13 | Success | Success | Failure | Failure |
| 14 | Success | Failure | Failure | Failure |
| 15 | Success | Failure | Success | Failure |
| 16 | Success | Failure | Failure | Failure |
| 17 | Success | Failure | Failure | Failure |

***Table 4.2: Performance test result.***

### 4.4 SYSTEM PERFORMANCE AND EVALUATION

In evaluating the system’s performance, two parameters are used – False Acceptance Rate (FAR) and False Rejection Rate (FRR).

#### 4.4.1 False Acceptance Rate (FAR)

False Acceptance refers to an instance or scenario in which a security system incorrectly authenticates or verifies an unauthorized person. This is the most important of all biometric security errors since it gives access to an unauthorized user.

*False Acceptance Rate (FAR)* is the probability of a biometric system incorrectly matches the input pattern to a non-matching template in the system’s database. This is possible if the impostor’s matching score is higher than the threshold set for the matching of the system. For the determination of FAR, the candidates were registered and after that, three different candidates were asked to impersonate a registered candidate. This was done by trying to break through the system by impressing their fingerprints and then comparing it with the template in the database of the system. This is shown mathematically as:

**Where:** FA = Number of false accept,

N = Total number of verifications

|  |  |  |
| --- | --- | --- |
| **Total number of samples, N** | **Number of false accepts, FA** | **FAR (%)** |
| 17 | 0 | 0 |

Table 4.3: Summary of the FAR test

#### 4.4.2 False Rejection Rate (FRR)

False rejection is defined as the scenario or instance in which a biometric system is unable or denies authentication of an authorized person. This depends on the image acquired and the threshold value set for the matching of the template pattern and the input pattern.

The False Rejection Rate (FRR) is the probability or the measure of the possibility that the fingerprint security system will wrongly or incorrectly reject an attempt to access the system by an authorized user. This is shown mathematically as;

It does not denote a flaw in the biometric system; rather, it shows convenience since it a function of the threshold value set for the matching of the images. In testing for the false rejection, candidates were selected and registered and were then authenticated to check if FR may occur. We shall only consider the case of clean dry fingers.

|  |  |  |
| --- | --- | --- |
| **Total number of samples, N** | **Number of false accepts, FA** | **FAR (%)** |
| 17 | 1 | 5.88 |

Table 4.4: Summary of the FRR test

#### 4.4.3 Convenience

The convenience shows how conducive it is to use the fingerprint system i.e. how the security system analyses the template and the input pattern. The fingerprint system may be designed to have a very high threshold value thus, making the matching score of the pattern (template and input) to be very high for authorized users to authenticate and also, reducing the threshold will also make the matching score so low for authentication.

The convenience of a biometric system depends on the False Rejection Rate (FRR). This is mathematically shown as;

***Convenience = 1 – FRR***

Thus, from table 4.3,

***Convenience = 100 – 5.88***

***= 94.12%***

#### 4.4.4 Security

This shows how reliable and secured the fingerprint system. This depends on the False Acceptance Rate (FAR) that may occur during the testing of the system. This is shown mathematically as;

***Security = 1 – FAR***

Thus, from table 4.2,

***Security = 100 – 0***

***= 100%***

Since no FAR occur while testing the system, then, it may be concluded that the system 100% is secured and accurate.

# CHAPTER FIVE

## CONCLUSION AND RECOMMENDATION

### 5.0 CONCLUSION

The fingerprint biometric system is arguably one of the most efficient biometric systems available today. In this project, we have been able apply engineering techniques to make this biometric system useful in our environments.

At the end of the project, a fingerprint authentication system was designed to enroll students during registration stage, and thereafter authenticate/verify students before entry into the examination hall.

Results show that the aim and objectives of this project was successfully achieved. It was found that, to improve the efficiency of verification, and to reduce the false rejection rate, students had to ensure a clean dry finger before scanning. Other finger conditions such as dirty, wet and oily failed to deliver a match even with the student with the right finger.

This system is highly efficient and reliable as can be seen from its performance evaluation using parameters such as FAR and FRR.

In all, this project is one that actively improves the quality and credibility of the educational system that chooses to implement it. Taking strict measures to ensure that the students that take an examination are those that the examination was meant for will inherently increase the credibility and veracity of the certification that comes from it.

### 5.1 RECOMMENDATION

This authentication system was not designed with re-usability as the main focus in that, the point at which the battery voltage drops below the required value for the components, the system is brought to a halt. Battery replacement would therefore be required to continue usage. This would in turn require opening the circuit casing, of which frequent case opening might subsequently lead to circuit fault or damage. Therefore, this project could be improved upon by providing avenue for battery charging without requiring unboxing. Another approach would be to abstract the battery section outside the circuit to avoid interaction with the main circuit in times of battery replacement.

# 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.
5. MAIO D., MALTONI D (1997). Direct Gray-Scale Minutiae Detection In Fingerprints, IEEE Trans. Pattern Anal. Machine. Intell., vol 19, pp. 27-40, USA.
6. BIGUN J., NILSSON K. (2001) Using linear symmetry features as a pre-processing step for fingerprint images, Conf. Audio and Video Based Biometric Person Authentication, pp.247–252, Sweden.
7. Sandeep K. P & Sailendra S. P., (2014). Fingerprint Recognition Project. *APEX Institute of Technology and Management.*
8. [Peer Reviewed Glossary of the Scientific Working Group on Friction Ridge Analysis, Study and Technology (SWGFAST)](http://www.swgfast.org/documents/glossary/090508_Glossary_2.0.pdf), 2012.
9. Lukasz WieClaw, (2009). A Minutiae-based Matching Algorithms in Fingerprint Recognition System. *Journal of Medical Informatics & Technologies Vol. 13/2009, ISSN 1642-6037*
10. Saferstein Richard. (2007). Criminalistics: An Introduction to Forensic Science, Pearson Education, Inc., Upper Saddle River, NJ.
11. Hangzhou Grow Technology co. (Feb 2011), Ltd, R307 Fingerprint module user manual.