FINGERPRINT MODULE: DESIGN, IMPLEMENTATION AND MEASUREMENT

BY

GROUP C MEMBERS

DEPARTMENT OF COMPUTER ENGINEERING

FACULTY OF ENGINEERING

UNIVERSITY OF BENIN

BENIN CITY

APRIL, 2018

# CERTIFICATION

This project work is approved in fulfilment of CPE 471 project in the Department of Computer Engineering, University of Benin, Benin City.

Approved by,

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

Signature

Supervisor : Engr. ODIA O.O

Date : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# DECLARATION

We hereby declare that this project report is based on my original work except for citations and quotations which have been duly acknowledged. We also declare that it has not been previously and concurrently submitted for any other degree or award at UTAR or other institutions.

Signature : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ID No. : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# DEDICATION

Specially dedicated to

Our friends, family members and well-wishers

# ACKNOWLEDGEMENTS

We would like to thank everyone who had contributed to the successful completion of this project. We would like to express our gratitude to our research companion, Our senior colleagues for their invaluable advice, guidance and enormous patience throughout the development of the research.

In addition, we would also like to express my gratitude to our loving parent and friends who had helped and given me encouragement.

# **TABLE OF CONTENTS**

[CERTIFICATION 2](#_Toc512061799)

[DECLARATION 3](#_Toc512061800)

[DEDICATION 4](#_Toc512061801)

[ACKNOWLEDGEMENTS 5](#_Toc512061802)

[TABLE OF CONTENTS 6](#_Toc512061803)

[LIST OF SYMBOLS / ABBREVIATIONS 9](#_Toc512061804)

[LIST OF FIGURES 10](#_Toc512061805)

[CHAPTER 1 11](#_Toc512061806)

[INTRODUCTION 11](#_Toc512061807)

[1.1 HISTORY 11](#_Toc512061808)

[1.2 Matching: Verification and Identification 12](#_Toc512061809)

[1.2.1 Feature Types 12](#_Toc512061810)

[1.2.2 System Issues 14](#_Toc512061811)

[1.3 Problems That the Project Has Been Able to Solve 15](#_Toc512061812)

[1.3.1 Benefits Offered by the Advance Systems Biometric Clock: 15](#_Toc512061813)

[1.3.2 Elimination of “Buddy Punching”: 15](#_Toc512061814)

[1.3.3 An Accurate Option: 15](#_Toc512061815)

[1.3.4 Increased Productivity: 15](#_Toc512061816)

[1.3.5 Increased Return on Investment (ROI): 15](#_Toc512061817)

[1.3.6 Increase Employee Accountability Thanks to Audit Trails: 15](#_Toc512061818)

[1.3.7 Enhanced Job Satisfaction: 16](#_Toc512061819)

[1.3.8 Easy and Safe to Use: 16](#_Toc512061820)

[1.3.9 Convenient Option: 16](#_Toc512061821)

[1.4 Biometric Attendance System Circuit Aim and Objective 16](#_Toc512061822)

[1.5 Scope of this Project 16](#_Toc512061823)

[1.6 Future 17](#_Toc512061824)

[CHAPTER 2 18](#_Toc512061825)

[LITERATURE REVIEW 18](#_Toc512061826)

[2.1 Finger Print Module 18](#_Toc512061827)

[2.1.1 Working Principle 18](#_Toc512061828)

[2.1.2 Hardware interface 19](#_Toc512061829)

[2.2 ARDUINO NANO V3.0 19](#_Toc512061830)

[2.2.1 Communication 20](#_Toc512061831)

[2.2.2 Programming 20](#_Toc512061832)

[2.3 LIQUID CRYSTAL DISPLAY (LCD) 21](#_Toc512061833)

[2.3.1 Blue LCD 1602 21](#_Toc512061834)

[2.3.1.1 Advantages 22](#_Toc512061835)

[2.3.1.2 Disadvantages 22](#_Toc512061836)

[2.4 Pin Headers 23](#_Toc512061837)

[2.5 SD Card Module 24](#_Toc512061838)

[2.6 Jumper Wire 24](#_Toc512061839)

[2.6.1 Types 25](#_Toc512061840)

[2.7 Arduino Nano Expansion Board 25](#_Toc512061841)

[2.8 7805 5 Volts Regulator IC 26](#_Toc512061842)

[CHAPTER 3 27](#_Toc512061843)

[METHODOLGY 27](#_Toc512061844)

[3.1 Pre-Processing 27](#_Toc512061845)

[3.1.1 Center Point Determination 27](#_Toc512061846)

[3.1.2 Minutiae Detection 28](#_Toc512061847)

[3.1.3 IMAGE ORIENTATION 29](#_Toc512061848)

[3.2 Main Process 30](#_Toc512061849)

[3.2.1 Sectorization and Normalization 30](#_Toc512061850)

[3.2.2 Gabor Filtering 30](#_Toc512061851)

[3.2.3 Feature Vector - Variance Calculation 31](#_Toc512061852)

[3.3 POST-PROCESSING 32](#_Toc512061853)

[3.4 ALGORITHM OVERVIEW 32](#_Toc512061854)

[3.5 SIGNAL FLOW 32](#_Toc512061855)

[3.6 RESULTS & CONCLUSION 33](#_Toc512061856)

[3.7 MEMORY PAGING & PROFILE RESULTS 36](#_Toc512061857)

[3.8 Project Units and Segmentation 37](#_Toc512061858)

[3.8.1 Power supply unit 37](#_Toc512061859)

[3.8.1.1 AC Power Adapter Source 37](#_Toc512061860)

[3.8.1.2 9 Volts Battery Power Supply Source 37](#_Toc512061861)

[3.8.2 Central Processing unit 38](#_Toc512061862)

[3.8.3 The Fingerprint Sensor Unit 39](#_Toc512061863)

[3.8.4 Alert Unit 40](#_Toc512061864)

[3.8.4.1 Visual Unit 40](#_Toc512061865)

[3.8.4.2 Audio unit 40](#_Toc512061866)

[3.9 System Design Flowchart 41](#_Toc512061867)

[3.10 Micro Controller Code 41](#_Toc512061868)

[3.11 Circuit Diagram 42](#_Toc512061869)

[CHAPTER 4 43](#_Toc512061870)

[TESTING AND TROUBLESHOOTING 43](#_Toc512061871)

[4.0 Bill of Engineering Measurement and Evaluation 43](#_Toc512061872)

[4.0 Project timeline 43](#_Toc512061873)

[CHAPTER 5 44](#_Toc512061874)

[CONCLUTIONS AND RECOMMMENDATIONS 44](#_Toc512061875)

[REFERENCE 45](#_Toc512061876)

# LIST OF SYMBOLS / ABBREVIATIONS

*cp* specific heat capacity, J/(kg⋅K)

*h* height, m

*Kd* discharge coefficient

*M* mass flow rate, kg/s

*P* pressure, kPa

*Pb* back pressure, kPa

*R* mass flow rate ratio

*T* temperature, K

*v* specific volume, m3

*α* homogeneous void fraction

*η* pressure ratio

*ρ* density, kg/m3

*ω* compressible flow parameter

ID inner diameter, m

MAP maximum allowable pressure, kPa

MAWP maximum allowable working pressure, kPa

OD outer diameter, m

RV relief valve

# LIST OF FIGURES

TITLE PAGE

[Figure 1.0.1 Fingerprint patterns: arch, loop, and whorl. Fingerprint landmarks are also shown: core and delta. (No delta locations fall within the captured area of the whorl here.) 13](#_Toc512061877)

[Figure 2.0.1Finger print Module 18](#_Toc512061878)

[Figure 2.0.2 Hardware interface 19](#_Toc512061879)

[Figure 2.0.3 Arduino NANO 20](#_Toc512061880)

[Figure 2.0.4 Blue LCD 1602 22](#_Toc512061881)

[Figure 2.0.5 Circuit Board of 12c Blue LCD 1602 22](#_Toc512061882)

[Figure 2.0.6 “Pin Header Connectors, Male and Female, On an Arduino Uno Board”. 23](file:///C:\Users\gideON\Desktop\FINALREPORT%202.docx#_Toc512061883)

[Figure 2.0.7 Female Machine Pins Header 24](#_Toc512061884)

[Figure 2.0.8 SD Card Module 24](file:///C:\Users\gideON\Desktop\FINALREPORT%202.docx#_Toc512061885)

[Figure 2.0.9 Jumper Wire 25](#_Toc512061886)

[Figure 2.0.10 Arduino Nano Expansion Board 26](#_Toc512061887)

[Figure 2.0.11 LM7805 Pin out Diagram 26](#_Toc512061888)

[Figure 3.0.1 Center point of Fingerprint 28](#_Toc512061889)

[Figure 3.0.2 Minutiae Types 28](#_Toc512061890)

[Figure 0.3 Angle of Rotation 29](file:///C:\Users\gideON\Desktop\FINALREPORT%202.docx#_Toc512061891)

[Figure 3.0.4 Gabor Filter 31](#_Toc512061892)

[Figure 3.0.5 Result of Center Point Algorithm 34](file:///C:\Users\gideON\Desktop\FINALREPORT%202.docx#_Toc512061893)

[Figure 3.0.6 Fingerprint before and after rotation 34](#_Toc512061894)

[Figure 3.0.7 Results of minutiae detector 35](file:///C:\Users\gideON\Desktop\FINALREPORT%202.docx#_Toc512061895)

[Figure 3.0.8 Results of 6 Gabor Filters 35](file:///C:\Users\gideON\Desktop\FINALREPORT%202.docx#_Toc512061896)

[Figure 3.0.9 LM7805 Pinout Diagram 38](#_Toc512061897)

[Figure 30.10 Power supply from 9Volts schematics 38](#_Toc512061898)

[Figure 0.11 Arduino Nano Pin Out 39](#_Toc512061899)

[Figure 3.0.12Finger print capture 39](#_Toc512061900)

[Figure 3.13 Visual Unit: LED 40](#_Toc512061901)

[Figure 3.14 Visual Unit : LCD 40](#_Toc512061902)

[Figure 3.0.15 Circuit Diagram 42](#_Toc512061903)

# CHAPTER 1

# INTRODUCTION

The use of fingerprints as a biometric is both the oldest mode of computer-aided, personal identification and the most prevalent in use today. However, this widespread use of fingerprints has been and still is largely for law enforcement applications. There is expectation that a recent combination of factors will favor the use of fingerprints for the much larger market of personal authentication.

These factors include: small and inexpensive fingerprint capture devices, fast computing hardware, recognition rate and speed to meet the needs of many applications, the explosive growth of network and Internet transactions, and the heightened awareness of the need for ease-of-use as an essential component of reliable security. This chapter contains an overview of fingerprint verification methods and related issues. We first describe fingerprint history and terminology.

Digital image processing methods are described that take the captured fingerprint from a raw image to match result. Systems issues are discussed including procedures for enrollment, verification, spoof detection, and system security. Recognition statistics are discussed for the purpose of comparing and evaluating different systems. We describe different fingerprint capture device technologies.

We consider fingerprints in combination with other biometrics in a multi-modal system and finally look to the future of fingerprint verification. It is necessary to state at the onset that there are many different approaches used for fingerprint verification. Some of these are published in the scientific literature, some published only as patents, and many are kept as trade secrets. We attempt to cover what is publicly known and used in the field, and cite both the scientific and patent literature. Furthermore, while we attempt to be objective, some material is arguable and can be regarded that way.

## 1.1 HISTORY

There is archaeological evidence that fingerprints as a form of identification have been used at least since 7000 to 6000 BC by the ancient Assyrians and Chinese. Clay pottery from these times sometimes contain fingerprint impressions placed to mark the potter. Chinese documents bore a clay seal marked by the thumbprint of the originator. Bricks used in houses in the ancient city of Jericho were sometimes imprinted by pairs of thumbprints of the bricklayer. However, though fingerprint individuality was recognized, there is no evidence this was used on a universal basis in any of these societies. In the mid-1800's scientific studies were begun that would have established two critical characteristics of fingerprints that are true still to this day: no two fingerprints from different fingers have been found to have the same ridge pattern, and fingerprint ridge patterns are unchanging throughout life. These studies led to the use of fingerprints for criminal identification, first in Argentina in 1896, then at Scotland Yard in 1901, and to other countries in the early 1900's. Computer processing of fingerprints began in the early 1960s with the introduction of computer hardware that could reasonably process these images. Since then, automated fingerprint identification systems (APIS) have been deployed widely among law enforcement agencies throughout the world. In the 1980s, innovations in two technology areas, personal computers and optical scanners, enabled the tools to make fingerprint capture practical in non-criminal applications such as for ID-card programs. Now, in the late 1990s, the introduction of inexpensive fingerprint capture devices and the development of fast, reliable matching algorithms have set the stage for the expansion of fingerprint matching to personal use. Why include a history of fingerprints in this chapter? This history of use is one that other types of biometric do not come close to. Thus there is the experience of a century of forensic use and hundreds of millions of fingerprint matches by which we can say with some authority that fingerprints are unique and their use in matching is extremely reliable.

## 1.2 Matching: Verification and Identification

Matching can be separated into two categories: verification and identification. Verification is the topic of this chapter. It is the comparison of a claimant fingerprint against an enrollee fingerprint, where the intention is that the claimant fingerprint matches the enrollee fingerprint. To prepare for verification, a person initially enrolls his or her fingerprint into the verification system. A representation of that fingerprint is stored in some compressed format along with the person's name or other identity. Subsequently, each access is authenticated by the person identifying him or herself, then applying the fingerprint to the system such that the identity can be verified. Verification is also termed, one-to-one matching. Identification is the traditional domain of criminal fingerprint matching. A fingerprint of unknown ownership is matched against a database of known fingerprints to associate a crime with an identity. Identification is also termed, one-to-many matching.

There is an informal third type of matching that is termed one-to-few matching. This is for the practical application where a fingerprint system is used by "a few" users, such as by family members to enter their house. A number that constitutes "few" is usually accepted to be somewhere between 5 and 20.

### 1.2.1 Feature Types

The lines that flow in various patterns across fingerprints are called ridges and the spaces between ridges are valleys. It is these ridges that are compared between one fingerprint and another when matching. Fingerprints are commonly matched by one (or both) of two approaches. We describe the fingerprint features as associated with these approaches. The more microscopic of the approaches is called minutia matching. The two minutia types that are shown in Figure 1.1 are a ridge ending and bifurcation. An ending is a feature where a ridge terminates. A bifurcation is a feature where a ridge splits from a single path to two paths at a Y-junction. For matching purposes, a minutia is attributed with features. These are type, location (x, y), and direction (and some approaches use additional features).

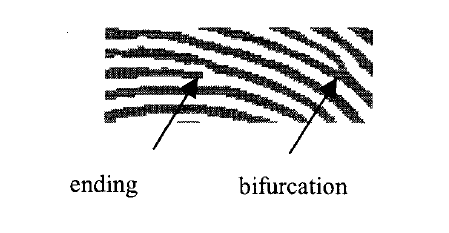


Figure 1.1 Fingerprint minutiae: ending and bifurcation

The more macroscopic approach to matching is called global pattern matching or simply pattern matching. In this approach, the flow of ridges is compared at all locations between a pair of fingerprint images. The ridge flow constitutes a global pattern of the fingerprint. Three fingerprint patterns are shown in Figure 1.2. (Different classification schemes can use up to ten or so pattern classes, but these three are the basic patterns.) Two other features are sometimes used for matching: core and delta, (Figure 1.2.) The core can be thought of as the center of the fingerprint pattern. The delta is a singular point from which three patterns deviate. The core and delta locations can be used as landmark locations by which to orient two fingerprints for subsequent matching - though these features are not present on all fingerprints. There may be other features of the fingerprint that are used in matching. For instance, pores can be resolved by some fingerprint sensors and there is a body of work (mainly research at this time) to use the position of the pores for matching in the same manner that the minutiae are used. Size of the fingerprint, and average ridge and valley widths can be used for matching, however these are changeable over time.

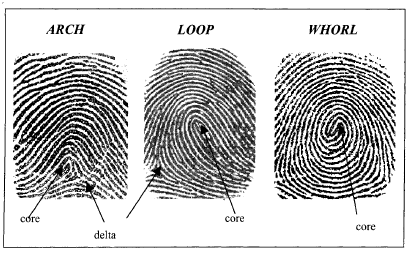


Figure 1.0.1 Fingerprint patterns: arch, loop, and whorl. Fingerprint landmarks are also shown: core and delta. (No delta locations fall within the captured area of the whorl here.)

The positions of scars and creases can also be used, but are usually not used because they can be temporary or artificially introduced.

### 1.2.2 System Issues

The effectiveness of a complete fingerprint verification system depends on more than the verification algorithms just described. There are other, higher level considerations, which we will call systems issues. These include enrollment and verification procedures, speed and ergonomics, user-feedback, anti-spoofing, and security considerations. It is essential to the goal of high recognition rate that the enrollment procedure results in the capture of the highest quality fingerprint image(s) obtainable because enrollment occurs once while verification occurs many times. Therefore, a well-designed verification system will require the user to go through more time and effort for enrollment than for verification. A fingerprint may be captured multiple times and the best taken or some combination of each taken as the enrolled fingerprint. There are options in the design of the verification procedure as well. The fingerprint can be captured once or a few times until a positive match is made. A procedure such as this will decrease false rejections, but increase false acceptances. Verification can be performed on not just one, but two or more fingers. This will enhance the recognition rate; however, it will also cause the user to expend more time. System ergonomics are important. For instance, there are limits to the amount of time that a person is willing to wait in personal authentication applications. That amount of time varies with the particular application and depends on what the person is also doing during processing, for instance swiping a bankcard or entering an identification number. Between 0.5 and 1 second are usually regarded as an acceptable range for processing time. Other user ergonomics considerations include: the number of repeated attempts in case of false rejections, the procedures for enrollment and verification, the design of the capture device, and the recognition setting that determines the trade-off between false acceptance and false rejection. Quality feedback is useful when an image is captured to indicate to the user how to place the finger for the best possible image quality. The type of feedback includes: "finger is placed too high", "finger is not pressed hard enough", etc. Anti-spoofing deterrents must be built into a fingerprint system to prevent use of an artificial fingerprint, a dead finger, or latent fingerprint. A latent fingerprint sometimes remains on a sensor surface due to skin oil residue from the previously applied fingerprint. Countermeasures are built into some sensors, such as the ability to distinguish true skin temperature, resistance, or capacitance. Since the fingerprint system is only as secure as its weakest link, a complete, secure system must be designed. For instance, minutia templates must be secured by some means such as encryption to prevent impostors from inserting their templates into the database in place of properly enrolled users. The end result of fingerprint verification is a "yes" or "no" that is used to gain access. If it is simple just to circumvent the fingerprint system to send a "yes", then the system provides little security. A solution to this problem is to ensure that the host receiving the recognition decision knows that this is from the trusted client, such as by digitally signing the information passed to the host.

## 1.3 Problems That the Project Has Been Able to Solve

### 1.3.1 Benefits Offered by the Advance Systems Biometric Clock:

Modern innovation and technology have led to quite a few advancements that help businesses grow, develop and reach higher levels of productivity. One type of technology many businesses have begun to use is biometric technology. Biometric based attendance and time terminals are becoming more and more popular due to the many benefits they offer. Since the biometrics terminals read each employee’s unique fingerprint, hand shape, iris or face shape, they ensure employees are unable to clock in for one another, preventing cases of employee time theft.

### 1.3.2 Elimination of “Buddy Punching”:

As mentioned above, one of the biggest benefits of biometrics for attendance and time keeping in a business is that employees will be unable to clock in for one another. This type of time theft can cost some companies tens of thousands of dollars (or more) each year. Biometrics characteristics are unable to be duplicated, which prevents employees from punching in another co-worker when they aren’t in the building.

### 1.3.3 An Accurate Option:

Since biometric credentials are unique for everyone and are unable to be duplicated or forged, biometric identification is the most accurate option to identify an employee. This type of technology will help business’s accurately track employee attendance and time. The benefits of biometrics for accuracy don’t stop there. With this technology in place, it will also eliminate cases of leaving early, arriving late or unauthorized overtime.

### 1.3.4 Increased Productivity:

With biometric clocks in place, the need to keep time manually is eliminated. This saves employees time, reduces staffing overhead and provides an accurate picture of labor data to the payroll department. This helps to effectively manage the overall business operations and will lead to an increase in productivity.

### 1.3.5 Increased Return on Investment (ROI):

When a company implements the use of a biometric time clock, it will help it achieve a positive ROI. This is done by eliminating employee theft, eliminating buddy punching and a number of other problems caused by loopholes and inaccuracies in the older types of attendance and time keeping systems. These old systems cause many businesses to lose quite a bit of money, year after year.

### 1.3.6 Increase Employee Accountability Thanks to Audit Trails:

One of the less known advantages of biometrics for time and attendance tracking is the audit trails they create. With these systems in place, employees are forced to be accountable for the actions they make. Since employees are able to be easily identified and held accountable for taking extended or frequent breaks, unscheduled lunches or other misuses of their time, productivity will be increased significantly.

### 1.3.7 Enhanced Job Satisfaction:

There are some situations where employees must work overtime to address unusual situations. However, putting in hours and hours of overtime, all the time, can wear down even the most dedicated and enthusiastic workers. This is especially true if the employee is unsure whether or not all their hard work is even noticed. When used properly, a quality biometric time clock will allow employers to know of excessive overtime situations and make changes accordingly to balance the workload. As a result, the employees don’t feel as though they are overworked. When overtime is required, they will also have confidence it will be noticed.

### 1.3.8 Easy and Safe to Use:

One of the best things about using biometric time clocks for identification purposes is that modern systems have integrated technology that is safe and easy to use. This provides accurate results with minimal invasiveness for users. Also, the clocks themselves are able to be installed quickly, with minimal training needed to begin using them.

### 1.3.9 Convenient Option:

Biometric time clocks are considered to be a convenient security solution because no passwords have to be remembered, no badges have to be used, nor ID cards, documents, etc. This lets employees quickly get to work, without worrying that they aren’t clocked in because they forgot their access badge.

## 1.4 Biometric Attendance System Circuit Aim and Objective

The main aim of this circuit is to take the attendance and display when requested. Finger print identification is because no two persons will have the same fingerprint in this world. This is because of the peculiar genetic code of DNA in each person. Finger print module differentiates between two fingers based on the ridges and valleys on finger print. When the finger print is given it stores the points where there are changes in the direction of ridges and valleys using some algorithms. Inside the finger, print module a Digital Signal Processor (DSP) is present to implement and analyzed the algorithm. Main heart of the circuit is finger print module. This sends commands to the controller whenever fingerprint is matched. Microcontroller receives these commands from the finger print module and uses the internal EEPROM (Electrically Erasable Programmable Read Only Memory) to store the attendance. Keypad is used to send the requests to the controller to either enroll the new one or to save the attendance or to exit. LCD display displays the messages related to the commands received.

## 1.5 Scope of this Project

Because of the peculiar genetic code of DNA in each person. Finger print module differentiates between two fingers based on the ridges and valleys on finger print. When the finger print is given it stores the points where there are changes in the direction of ridges and valleys using some algorithms. The Golden user path is to have a user enroll his or her finger print pattern into the system and hav the system save it for furture check. When the users access via the fingerprint, the system verifies the fingerprint and compares with all that is in the data base. If found to tally with already stored fingerprint, the system gives access to that user else if buzzes and show visual signals with the aid of an LED to signify that the fingerprint currently trying to access the system isn’t registered or enrolled in the system.

## 1.6 Future

Where is biometric technology going? System price will continue to decrease along with size, while recognition rates will improve (at a slower rate than price and size changes). Recognition rate will be a deciding factor in acceptance for demanding applications such as automatic teller machines (requiring a very low rate of false rejections), and military (requiring a very low rate of false acceptances). For especially demanding applications, multi-modal systems will evolve to combine biometrics to provide an optimum level of security and convenience to users. Alternatively, multiple verifications, such as by using multiple fingers, will be used to enhance recognition reliability. If costs plummet as the industry projects, personal use of biometric systems will grow to replace the current reliance on passwords, PINs, and door keys that are used for computers, home security systems, restricted entry, ATMs, credit cards, internet access, corporate networks, confidential databases, etc. The biometrics promise is to make access much simpler while at the same time providing a higher level of security.

# CHAPTER 2

# LITERATURE REVIEW

In this chapter, the major component used in this project design will be described with a view to understanding their general principles of operation and characteristic.

The major component used in this projects are finger print module, Arduino NANO v3.0, Blue LCD 1602, Headers, Arduino NANO expansion board, SD Card module, jumper wires and so on.

## 2.1 Finger Print Module

Biometric identification from a print made by an impression of the ridges in the skin of a finger is often used as evidence in criminal investigations. Yes, now we can use the same biometric identification technique to build our own projects like a biometric authenticator/access control system with the help of readily-available Fingerprint Identification Modules.

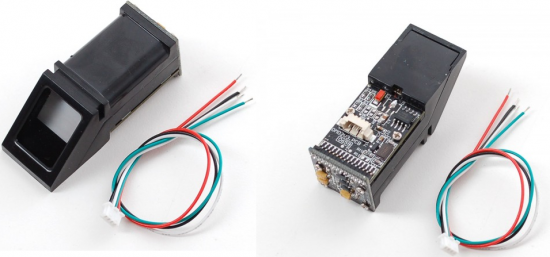


Figure 2.0.1Finger print Module

This is an optical biometric fingerprint reader/sensor (R305) module with TTL UART interface for direct connections to a microcontroller UART. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the 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.

### **2.1.1 Working Principle**

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-time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library.

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.

### 

### **2.1.2 Hardware interface**

The module itself does all complex tasks behind reading and identifying the fingerprints with an on-board optical sensor and fingerprint algorithm. All you need to do is send it simple commands, and the fingerprint scanner can store different fingerprints.

The database of prints can even be downloaded from the unit and distributed to other modules. As well as the fingerprint template, the analyzed version of the print, you can also retrieve the image of a fingerprint and even pull raw images from the optical sensor.

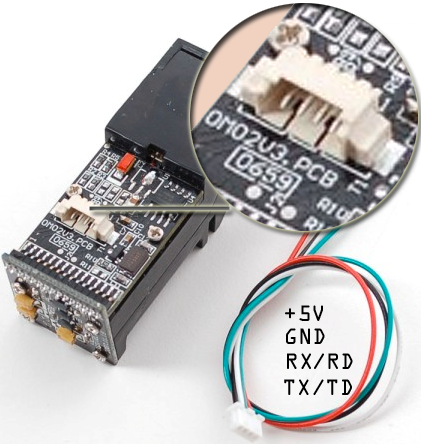
[](https://www.electroschematics.com/wp-content/uploads/2015/05/FPS-2.png)

Figure 2.0.2 Hardware interface

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 (uC) runs on of 3.3V or 5V power supply. TX/TD pin of the module connects with RXD (RX-IN pin of the uC), and RX/RD pin connects with TXD (TX-OUT pin of the uC).

If you are building a personal computer (PC) – based project, remember to add a level converting circuit (for instance, the [MAX232](https://www.datasheets.com/pd/max2320eup-maxim-integrated-18251003.html?utm_medium=PartNumber&utm_source=electroschematics&utm_term=MAX232)) between the module and the personal computer. Serial communication protocol mode is semi-duplex asynchronous serial communication, and user can set the baud rate in 9600 – 115200bps. Recommended working voltage of the module is 3.6 to 6.0 Volt DC, and the typical working current is 90 to 100 mA (150mA peak).

### 

### 2.2 ARDUINO NANO V3.0

Arduino is an open-source platform used for building electronics projects. Arduino consists of both a physical programmable circuit board (often referred to as a microcontroller) and a piece of software, or IDE (Integrated Development Environment) that runs on your computer, used to write and upload computer code to the physical board.

The Arduino platform has become quite popular with people just starting out with electronics, and for good reason. Unlike most previous programmable circuit boards, the Arduino does not need a separate piece of hardware (called a programmer) in order to load new code onto the board – you can simply use a USB cable. Additionally, the Arduino IDE uses a simplified version of C++, making it easier to learn to program. Finally, Arduino provides a standard form factor that breaks out the functions of the micro-controller into a more accessible package.

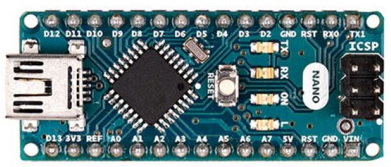


Figure 2.0.3 Arduino NANO

### 2.2.1 Communication

The Arduino Nano has a number of facilities for communicating with a computer, another Arduino, or other microcontrollers. The ATmega168 and ATmega328 provide UART TTL (5V) serial communication, which is available on digital pins 0 (RX) and 1 (TX). An FTDI FT232RL on the board channels this serial communication over USB and the FTDI drivers (included with the Arduino software) provide a virtual com port to software on the computer. The Arduino software includes a serial monitor which allows simple textual data to be sent to and from the Arduino board. The RX and TX LEDs on the board will flash when data is being transmitted via the FTDI chip and USB connection to the computer (but not for serial communication on pins 0 and 1). A Software Serial library allows for serial communication on any of the Nano's digital pins. The ATmega168 and ATmega328 also support I2C (TWI) and SPI communication. The Arduino software includes a Wire library to simplify use of the I2C bus; see the documentation for details. To use the SPI communication, please see the ATmega168 or ATmega328 datasheet.

### 

### 2.2.2 Programming

The Arduino Nano can be programmed with the Arduino software. Examples are Arduino Diecimila, Duemilanove, or Nano w/ ATmega168 or "Arduino Duemilanove or Nano w/ ATmega328" from the Tools > Board menu (according to the microcontroller on your board). The ATmega168 or ATmega328 on the Arduino Nano comes preburned with a bootloader that allows you to upload new code to it without the use of an external hardware programmer. It communicates using the original STK500 protocol (reference, C header files). You can also bypass the bootloader and program the microcontroller through the ICSP (In Circuit Serial Programming) header.

### 

### 2.3 LIQUID CRYSTAL DISPLAY (LCD)

A liquid-crystal display (LCD) is a flat-panel display or other electronically modulated optical device that uses the light-modulating properties of liquid crystals. Liquid crystals do not emit light directly, instead using a backlight or reflector to produce images in colour or monochrome. LCDs are available to display arbitrary images (as in a general-purpose computer display) or fixed images with low information content, which can be displayed or hidden, such as preset words, digits, and 7-segment displays, as in a digital clock. They use the same basic technology, except that arbitrary images are made up of a large number of small pixels, while other displays have larger elements.

LCDs are used in a wide range of applications including LCD televisions, computer monitors, instrument panels, aircraft cockpit displays, and indoor and outdoor signage. Small LCD screens are common in portable consumer devices such as digital cameras, watches, calculators, and mobile telephones, including smartphones. LCD screens are also used on consumer electronics products such as DVD players, video game devices and clocks. LCD screens have replaced heavy, bulky cathode ray tube (CRT) displays in nearly all applications. LCD screens are available in a wider range of screen sizes than CRT and plasma displays, with LCD screens available in sizes ranging from tiny digital watches to huge, big-screen television sets.

Since LCD screens do not use phosphors, they do not suffer image burn-in when a static image is displayed on a screen for a long time (e.g., the table frame for an aircraft schedule on an indoor sign). LCDs are, however, susceptible to image persistence. The LCD screen is more energy-efficient and can be disposed of more safely than a CRT can. Its low electrical power consumption enables it to be used in battery-powered electronic equipment more efficiently than CRTs can be. By 2008, annual sales of televisions with LCD screens exceeded sales of CRT units worldwide, and the CRT became obsolete for most purposes.

### 

### 2.3.1 Blue LCD 1602

This I2C LCD can display 16 characters on 2 lines and it features adjustable contrast and backlight. You’ll only need two wires to control this LCD, making it perfect for our project.

It is also great for your project especially if you have limited pin resources, because it can be controlled by using only two pins.

This module consists into a normal LCD connected to an I2C backpack.

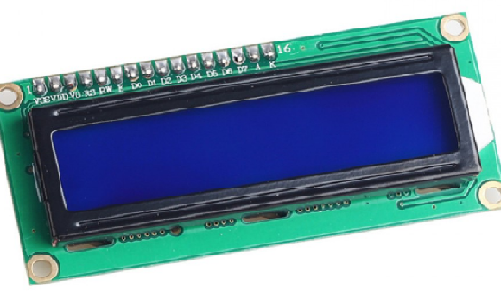


Figure 2.0.4 Blue LCD 1602

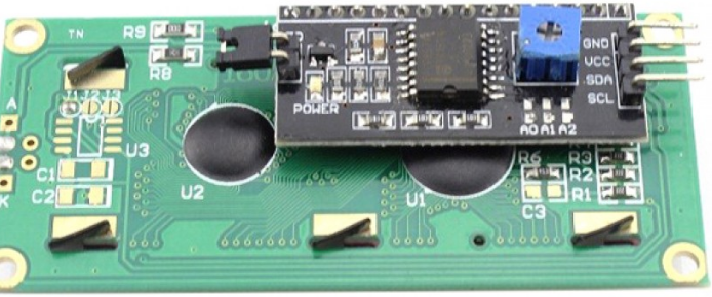


Figure 2.0.5 Circuit Board of 12c Blue LCD 1602

### 2.3.1.1 Advantages

* Very compact, thin and light, especially in comparison with bulky, heavy CRT displays.
* Little heat emitted during operation, due to low power consumption.
* No geometric distortion.
* The possible ability to have little or no flicker depending on backlight technology.
* Unaffected by magnetic fields, including the Earth's.
* Can be made with very narrow frame borders, allowing multiple LCD screens to be arrayed side-by-side to make up what looks like one big screen.

### 2.3.1.2 Disadvantages

* Limited viewing angle in some older or cheaper monitors, causing color, saturation, contrast and brightness to vary with user position, even within the intended viewing angle.
* Uneven backlighting in some monitors (more common in IPS-types and older TNs), causing brightness distortion, especially toward the edges ("backlight bleed").
* Only one native resolution. Displaying any other resolution either requires a video scaler, causing blurriness and jagged edges, or running the display at native resolution using 1:1-pixel mapping, causing the image either not to fill the screen (letterboxed display), or to run off the lower or right edges of the screen.

## 2.4 Pin Headers

Pin headers are often associated with ribbon cable connectors; pin headers often also function as recipients for jumpers. The most common jumper spacing is 2.54 millimeters (0.1 in), though 2.0 millimeters (0.079 in) is sometimes used in smaller products.

Pin header connectors are thus "male" connectors ("female" counterparts do exist, but these are normally just called female header (FH) or header connector, without "pin") and are mostly used inside equipment, rather than being used as a connector on the outside of the device.

Normally pin headers are pin through hole (PTH) devices, but surface-mount technology (SMT) versions of one and two row pin headers also exist. In the latter case the solder sides of the pins are simply bent on a 90-degree angle so as to be soldered to a solder plane. On single row pin headers, the pins are bent alternating to one side or the other, on dual row pin headers the pins are simply bent outwards. If pin headers are optional, the PTH variant is often chosen for ease of manual assembly. Pin headers can be either straight or angled. The latter form is often used to connect two boards together.

Pin headers are cost-effective due to their simplicity. Headers are often sold as long strips (typically 40 or 50 pins for the dual row versions) which can easily be broken off to the right number of pins.

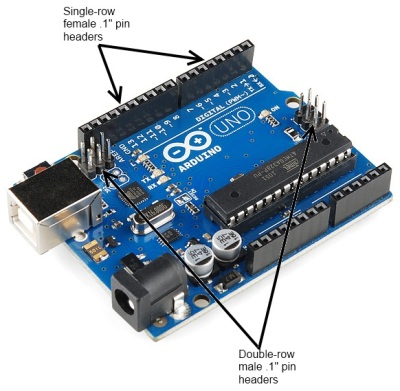


Figure 2.0.6 “Pin Header Connectors, Male and Female, On an Arduino Uno Board”.

A common variation on this part is a “machine pin” version. While the normal version is formed out of stamped and folded sheet metal, machine pin connectors are formed by tooling the metal into the desired shape. The result is a more robust connector, with a better joint and longer life, making it somewhat more expensive.

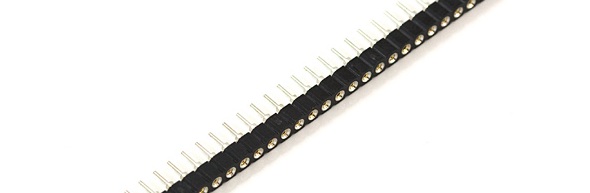
[](https://cdn.sparkfun.com/assets/d/4/8/d/a/5114022cce395f547e000003.jpg)

Figure 2.0.7 Female Machine Pins Header

Note: that these are designed to be snapped apart into smaller sections, while standard .1" female header pin connectors are not. It’s also important to note that not all non-machine pin header connectors will mate with the machine pin variety.

## 2.5 SD Card Module

The micro- SD Card Module is a simple solution for transferring data to and from a standard SD card. The pin out is directly compatible with Arduino, but can also be used with other microcontrollers. It allows you to add mass storage and data logging to your project.

This module has SPI interface which is compatible with any sd card and it use 5V or 3.3V power supply which is compatible with Arduino UNO/Mega.

SD module has various applications such as data logger, audio, video, graphics. This module will greatly expand the capability an Arduino can do with their poor limited memory.

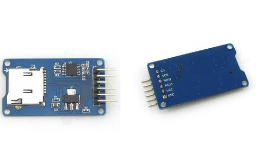


Figure 2.0.8 SD Card Module

## 

## 2.6 Jumper Wire

A jump wire (also known as jumper, jumper wire, jumper cable, DuPont wire, or DuPont cable – named for one manufacturer of them) is an electrical wire, or group of them in a cable, with a connector or pin at each end (or sometimes without them – simply "tinned"), which is normally used to interconnect the components of a breadboard or other prototype or test circuit, internally or with other equipment or components, without soldering.

Individual jump wires are fitted by inserting their "end connectors" into the slots provided in a breadboard, the header connector of a circuit board, or a piece of test equipment.

### 2.6.1 Types

There are different types of jumper wires. Some have the same type of electrical connector at both ends, while others have different connectors. Some common connectors are:

* Solid tips: are used to connect on/with a breadboard or female header connector. The arrangement of the elements and ease of insertion on a breadboard allows increasing the mounting density of both components and jump wires without fear of short-circuits. The jump wires vary in size and colour to distinguish the different working signals.
* Crocodile clips: are used, among other applications, to temporarily bridge sensors, buttons and other elements of prototypes with components or equipment that have arbitrary connectors, wires, screw terminals, etc.
* Banana connectors: are commonly used on test equipment for DC and low-frequency AC signals.
* Registered jack (RJnn): are commonly used in telephone (RJ11) and computer networking (RJ45).
* RCA connectors: are often used for audio, low-resolution composite video signals, or other low-frequency applications requiring a shielded cable.
* RF- Connectors: are used to carry radio frequency signals between circuits, test equipment, and antennas.



Figure 2.0.9 Jumper Wire

## 2.7 Arduino Nano Expansion Board

This Nano Multi-Function expansion board is designed especially for Arduino Nano, solve the problem of wiring confusing when a variety of sensors connected.  
Lead out all digital IO port and analog IO port, each one with standard positive and negative power interface.  
Lead out the I2C interface of mainboard for convenient connection.  
Increasing the DC power supply interface. Nano USB interface supply current is actually only 50MA, to bring high-current devices, such as the steering, is obviously insufficient. So in the DC power connector provide external power supply to ensure the stability of equipment operation.

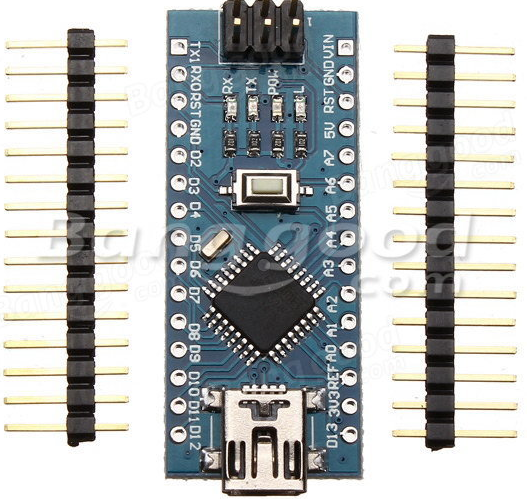


Figure 2.0.10 Arduino Nano Expansion Board

## 2.8 7805 5 Volts Regulator IC

The 7805 is a versatile IC known to provide an average voltage of about 5volts. Which is the needed output for this electronics project.

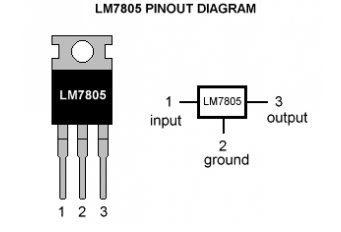


Figure 2.0.11 LM7805 Pin out Diagram

SPECIFICATION:

Voltage regulator:

As we require a 5V we need LM7805 Voltage Regulator IC.

7805 IC Rating:

* Input voltage range 7V- 35V
* Current rating Ic =1A
* Output voltage range   VMax=5.2V ,VMin=4.8V

## 2.7 5-Volts AC Power Adapter

SPECIFICATION:

Input: 100-240V AC 50/60Hz

Output: 5V, 2.0A (2000mA)

# 

# CHAPTER 3

# METHODOLGY

## 3.1Pre**-**Processing

### 3.1.1 Center Point Determination

Initially, a reference point, or center point, must be determined. The following steps in the process will all be referenced around this point. The center point is found at the point of maximum curvature of ridge lines.

1. apply Wiener filter to the image. This filter performs 2-D adaptive noise-removal. It uses a pixel-wise adaptive Wiener method based on statistics estimated from a local neighborhood of each pixel. The size of these neighborhoods are 5x5 pixels.
2. determine the numerical gradient of the image in the x and y directions.
3. apply the Wiener filter on the x and y gradients to enhance them further.
4. divide input fingerprint image into blocks of 10x10 pixels.
5. compute the slope perpendicular to the local orientation of each block using the following formula:



1. for blocks with slopes ranging from 0 to π/2, trace a path down until slope that is not ranging from 0 to π/2 is found and mark it.
2. compute the slope in the negative y direction and output an x and y position which will be the center point of the fingerprint for block that has the highest number of marks.



Figure 3.0.1 Center point of Fingerprint

### 3.1.2 Minutiae Detection

A minutia is a pattern of the flow of the ridges or valleys. A fingerprint can have number of minutiae. The minutiae can be distinguished and classified into many different types. See the diagram below:

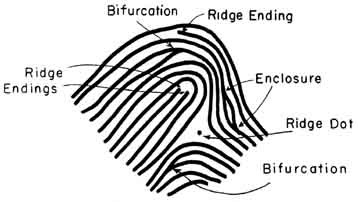


Figure 3.0.2 Minutiae Types

Since each fingerprint has its unique sets of minutiae, many automatic fingerprint matching systems are based on minutiae matching. The traditional way is to use neural networks, which often requires lots of computing power. The quality of images also becomes very critical to minutiae detection because most programs are written to trace down the ridge lines. For example, a short noise line along a ridge can likely be mistaken for a bifurcation minutia. Therefore, we took noises into consideration, and we tried to have more flexibility on the image quality by just searching one minutiae point near the center point of the fingerprint[[1]](#footnote-1).

We first create a binary image from the scanned image. The threshold is set so that the noise on the image is not as apparent. Since we only need to find one minutiae point within a small area near center, we have used a different approach in our minutiae detection. One difference is that we only look for ‘bifurcations’ and ‘dots’. Before we start the minutiae search, those two patterns are predefined. During the search process, we use the predefined patterns to scan through the image from 4 different directions. Once we find a minutia, the process is stopped and the location of the minutiae is recorded along with the type. (bifurcation or dot)

### 3.1.3 IMAGE ORIENTATION

A major obstacle in fingerprint recognition is that the images obtained are not usually perfectly aligned. Usually rotation and displacement of some sort is evident. Attempting to compare two fingerprints with different orientations will affect the result significantly. To adjust for this, rotation of the input image is performed.

To rotate an image both the angle of rotation and the origin point are needed. To find the angle of rotation, 4 points are needed: center point of image in database and input image, and location of the same minutiae point for both images. Then the angle is calculated using the following equation:

Angle of rotation = tan-1(y2-center\_y2 / x2-center\_x2)

– tan-1(y1-center\_y1 / x1-center\_x1);

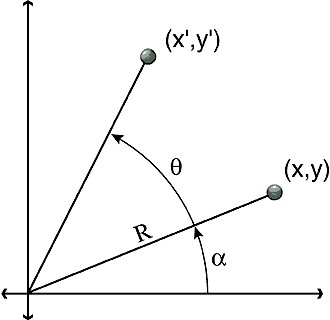
The origin point to rotate around will be the center point of the input image. The initial technique was to go through each pixel of the input image, and use the rotation equations below to find the corresponding rotated position (x’, y’). This technique has problems though, when the corresponding coordinates are found they are not usually integer values. This implies that the resulting rotated image will only have pixels at integer values, and that certain output pixels will not get mapped by any input pixels. The resulting output would be completely inaccurate.

Figure 0.3 Angle of Rotation

x = R \* Cos(a) y = R \* Sin(a) x' = R \* Cos (a + q) y' = R \* Sin (a + q)

The method used to solve this problem is to do the reverse. For every pixel in the rotated image, calculate which pixel in the input maps to it. Doing this is simple because the negative of the angle of rotation can be used. When mapping back though the coordinates will also probably not be integers, though the closest neighboring pixel can be used. This implies that some output pixels will map to the same input, but this is acceptable as it is very difficult to observe and is significantly better than unmapped pixels.

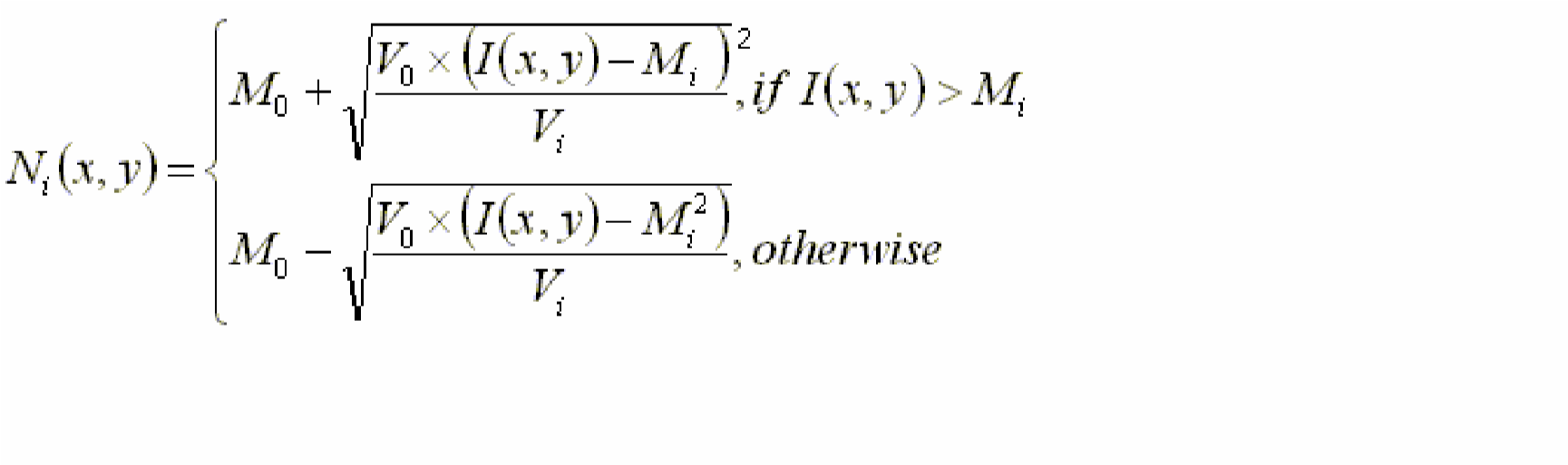
## 3.2 Main Process

### 3.2.1 Sectorization and Normalization

The fingerprint image needs to be normalized in order to that no differences in brightness or contrast exist throughout the image. These differences occur when acquiring the image from a scanner or other digitizing device as well as the pressure applied by the person.

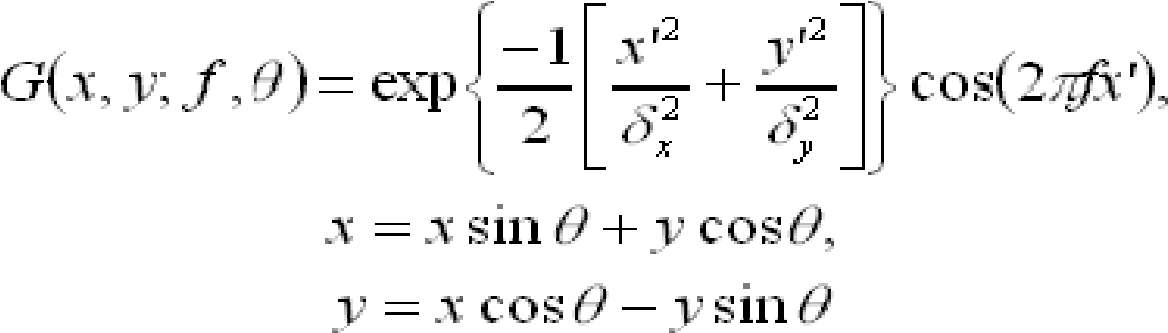
Furthermore, sectorization is used in the next step in the process –feature extraction. The 6 Gabor Filters used are lined up with 12 sectors in each band.

The image is divided into 5 concentric bands, each with a radius of 20 pixels, laid over the center point. The center band has a radius of 12 pixels. The total diameter is (20\*5+12) \*2-1 = 223 pixels. The five bands each contain 12 wedges. Therefore, there are 60 sectors for the image. The center band is omitted, as its area is small relative to the other bands. The radius values are specifically chosen so as to avoid the effects of circular convolution.



### 3.2.2 Gabor Filtering

After we finish normalization, we will then pass the normalized image through a bank of 6 different angles of Gabor filters. Each filter is created by producing a 33x33 filter image with angles 0, π/6, π/3, π/2, 2π/3 and 5π/6. By applying Gabor filters, we are able to remove noises, preserve ridge and furrow structures, and provide information contained in certain direction of the image.



The Gabor filter has a height and width (33\*33) to maintain its peak center point. The parameters, δx and δy, the space constants of the Gaussian envelope along x and y axis, were set to be 4.0. The frequency is determined by the inverse of the average inter ridge distance. Too large a value of f will create spurious ridges, and close ridges will merge into one if the value of f is too small. We found that the average distance to be about 10 pixels.

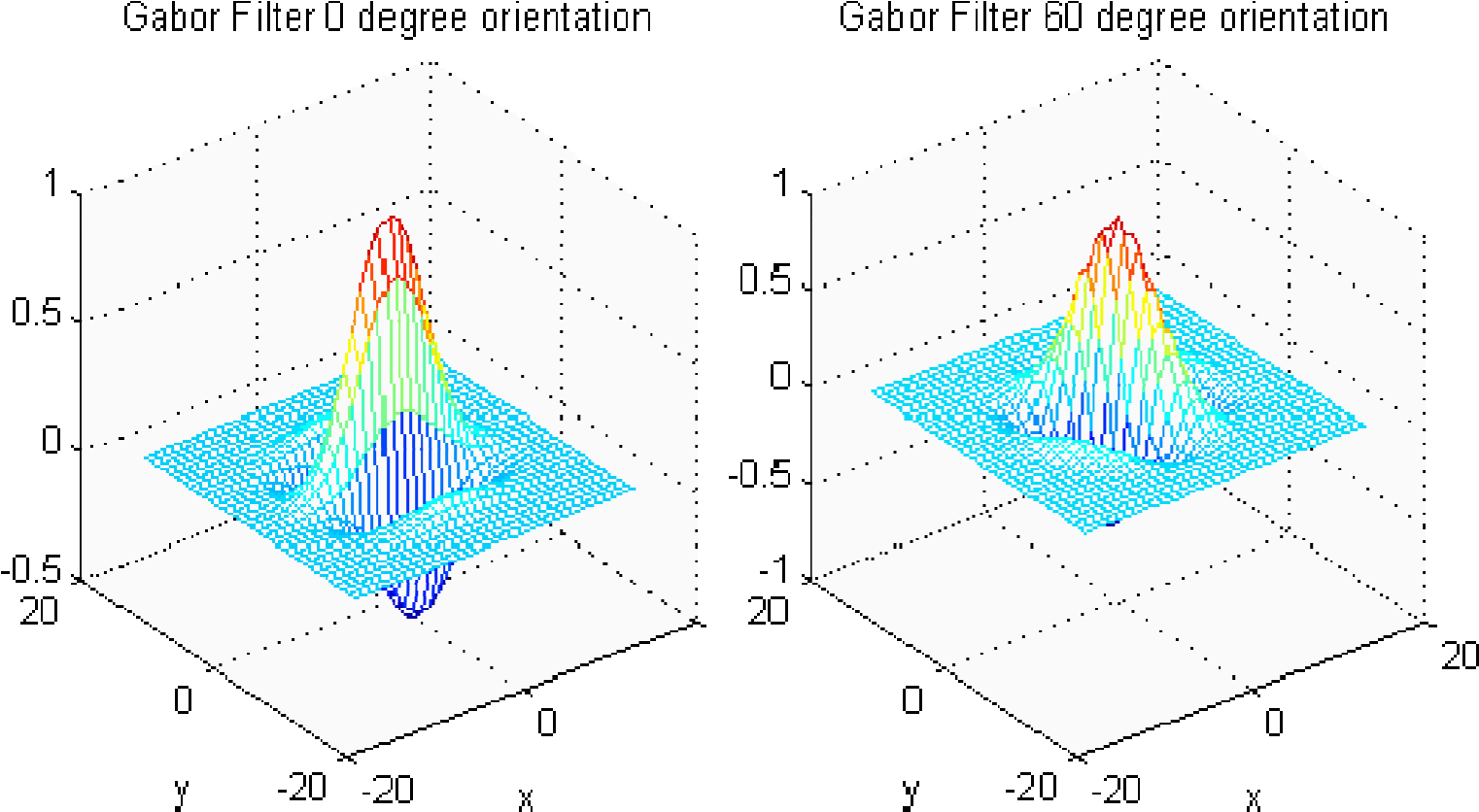
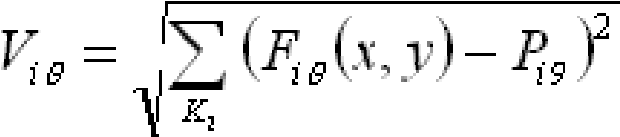


Figure 3.0.4 Gabor Filter

We have considered applying FFT to the normalized image and the filter, so that we can speed up the filtering by using only multiplication. However, applying FFT takes extra steps, and it also requires more memory space for coefficient storage. As a result, we simply have the convolution done in space. The sectorization is then used to detect the presence of ridges in the direction of the corresponding Gabor filter.

### 3.2.3 Feature Vector - Variance Calculation

After obtaining the 6 Gabor filtered images, the variance of pixel values in each sector is calculated. This variance gives an idea of the concentration of ridges in each direction in that sector. Higher variance values imply that the ridges in the sector were in a more similar direction to that angle of the Gabor filter, while lower variance values imply that the ridges were in other directions and were thus filtered out. A variance value was obtained for each sector and for 6 of the filtered images. Therefore, a total of 60 variance values are obtained and they represent the feature vector of the fingerprint. The following equation is used to calculate the variance for each sector:



Fiθ - pixel values in ith sector for Gabor filter with angle θ

Piθ - mean of pixel values

Ki – number of pixels in ith sector

## 3.3 POST-PROCESSING

Mean Nearest Neighbor

We choose mean nearest neighbor as our classifier. One feature vector from each individual person is calculated from the training set and then saved in our database for future matching. The feature vectors in the database are gathered from better quality images. For a given fingerprint, we find that the Euclidean distance between the target feature vector and feature vector of each person in our database. The person that yields the lowest distance is chosen and matched. As we have looked into many classification schemes, the mean nearest neighbor requires the least calculations to yield a result. It also consumes the least storage space since it takes only one feature vector from each person. Although this classifier does not take into account the variations of fingerprints of the same person, it is sufficient enough for our project.

## 3.4 ALGORITHM OVERVIEW

## 3.5 SIGNAL FLOW

“scanned” input

Image

Minutiae locator.

PC side

EVM

Image rotation

and transformation

n

Image centering

Sectorization and

Normalization

Gabor Filters

Feature Vector

Comparison

## 3.6 RESULTS & CONCLUSION

Overall, the center point determination algorithm did not give precise results. It was applied to the following 3 fingerprint images. The corresponding center points are shown for each image respectively. It is evident that the algorithm is not very accurate. Noise and low image resolution are important factors that these images possess. Better quality images may result in improved center points. However, the algorithm used is not accurate in general.

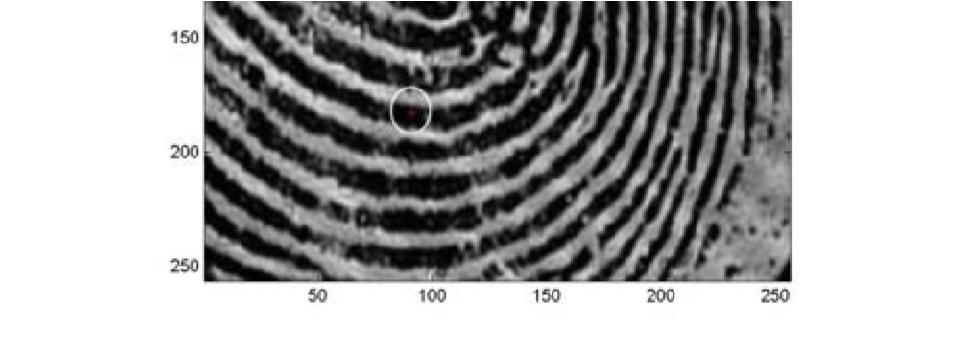
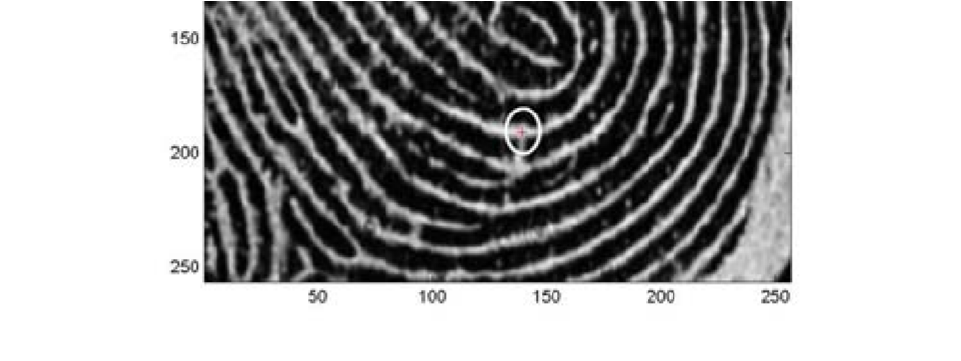
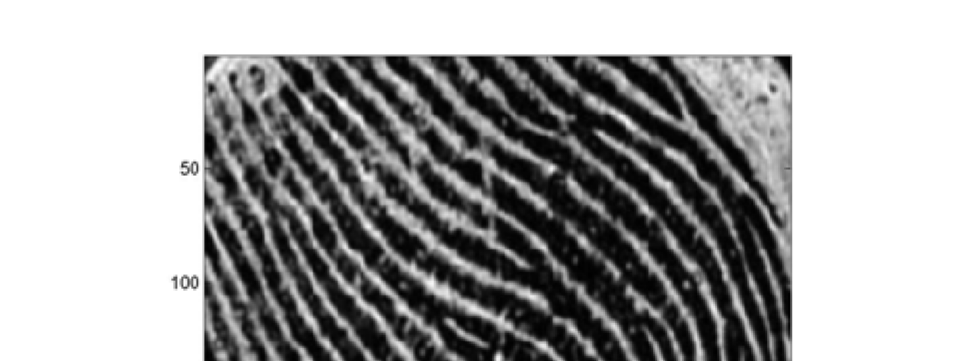
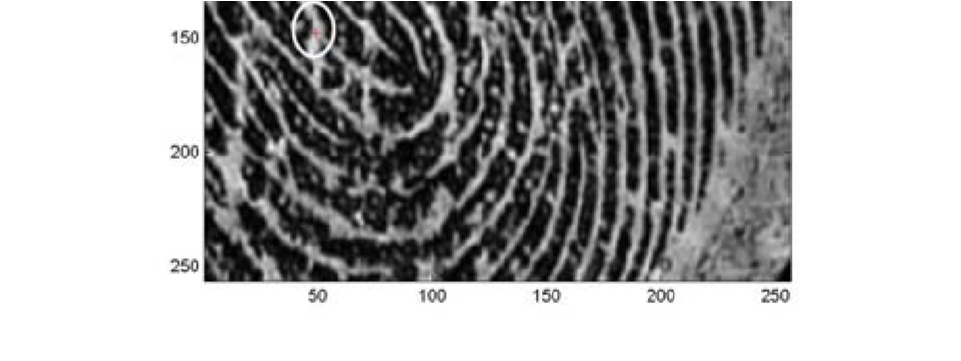


Figure 3.0.5 Result of Center Point Algorithm

After performing a rotation on the image on the left, the resulting image has a better orientation. However, since the input is 256x256 the quality of the rotated image is not as good as the input. Higher resolutions would make the resulting image much smoother. Due to the mapping of the pixels of such a low resolution image, the result is not the same quality as the input. Nevertheless, the resulting image is still acceptable and can be processed for fingerprint matching. It would have been much better if higher quality images were available.

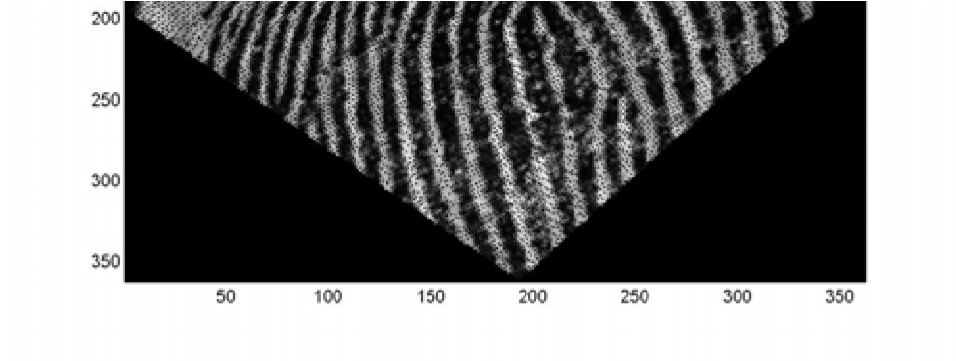


Figure 3.0.6 Fingerprint before and after rotation

As for the minutiae detection algorithm, it did not function very effectively. The main reason for this was the presence of noise in the fingerprint images. The process takes in a threshold value and binaries the image. Therefore, noise values are attributed to a 0 or 1 and affect the results greatly. Minutiae detection is not a simple task and requires extremely high quality images. If restrictions can be placed on the quality of the input images, then minutiae detection could work. The lighter stroked circle on the fingerprint image indicates a true minutiae point, while the thicker stroked circle indicates a result of the minutiae detector. This result is incorrect due to the presence of noise in the image.

After performing, sectorization and normalization, the brightness and contrast throughout the images became constant. There were no variations apparent. The results of the 6 different Gabor filters are shown in the figure below. By applying these filters, noise was reduced, and the ridges in a similar direction to each filter were preserved. A previous group performed Gabor filtering by using the FFT and then the IFFT to obtain the result. By performing the filtering in the time domain we were able to reduce the time and memory requirements significantly.



Figure 3.0.7 Results of minutiae detector

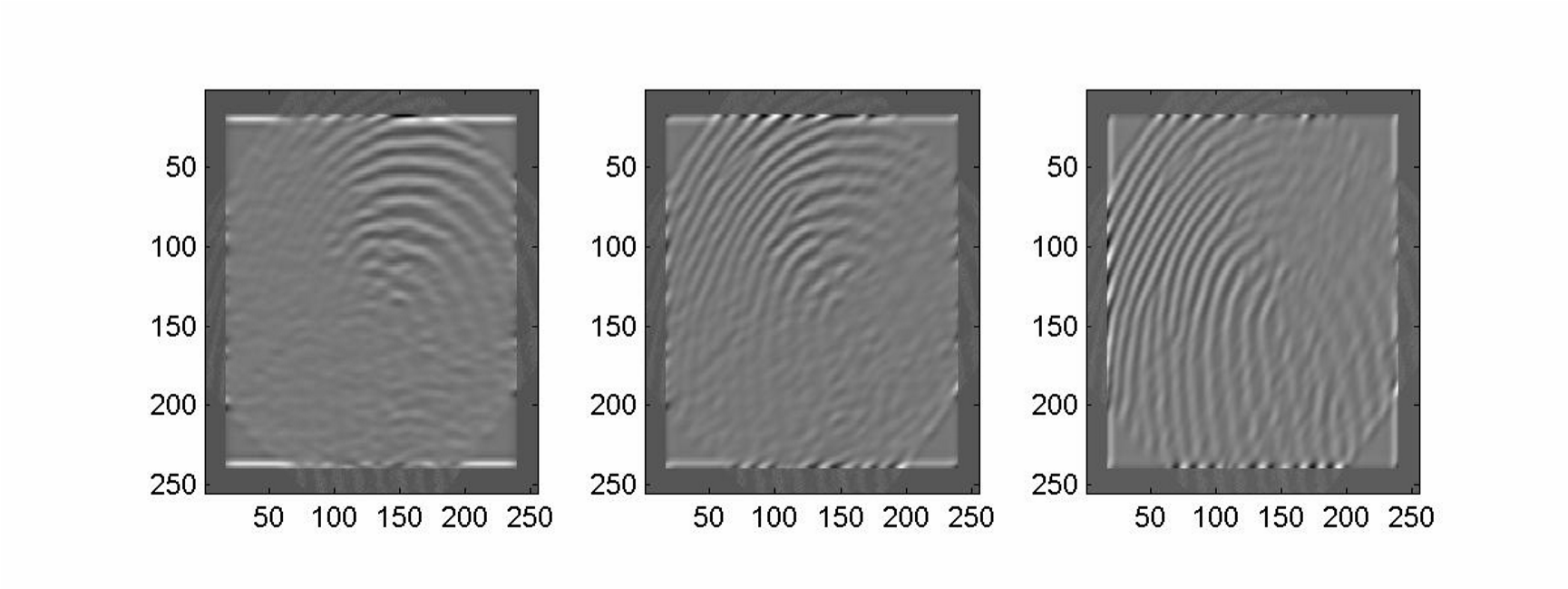
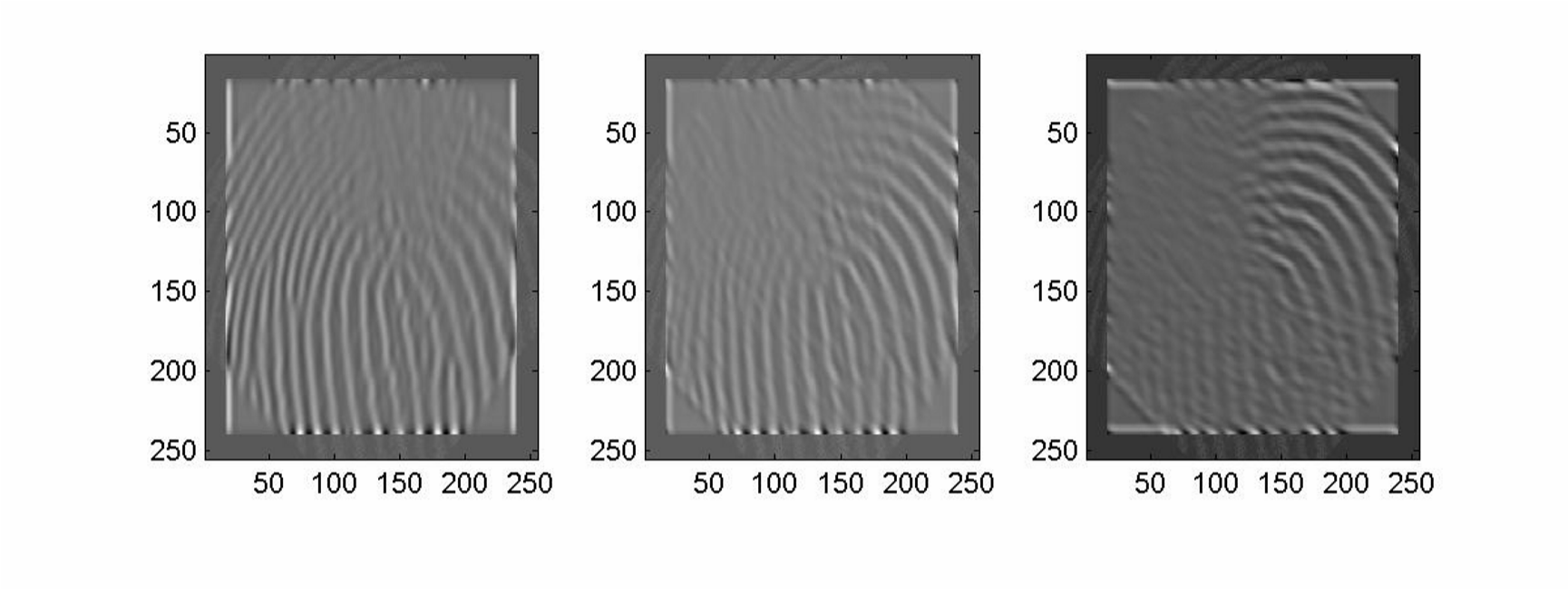


Figure 3.0.8 Results of 6 Gabor Filters

Since we had a database of 5 individuals and 60 fingerprints each, we partitioned these prints into a training set and a testing set. The 5 individuals all had the same type of fingerprint – loop. This made it more challenging to do verification among the prints. The training set consists of 15 prints that make up the database. They are also used to determine the threshold for rejection. A few of the remaining prints, many of which were of bad quality, were used as the testing set.

In order to determine a threshold value for our verification process, it was necessary to compare a fingerprint from one class to one in each of the five classes. By looking at the Euclidean distance values, it should be obvious to determine which class the fingerprint belongs. Then after repeating the process a few more times, a threshold can be estimated.

Many obstacles make fingerprint verification difficult such as incorrect orientation, displacement, missing sections, and poor quality. Orientation and displacement issues arise as differences each time a fingerprint is digitized from the person. Perfect alignment while scanning is not possible each time. When verifying a fingerprint, it is rejected if its quality is poor causing the classifier to give a Euclidean distance that is much greater than threshold. Here is a sample of the results from the classifier when verifying a fingerprint from Class 1:

|  |  |
| --- | --- |
| Class | Euclidean Distance |
| 1 | 52195 |
| 2 | 95817 |
| 3 | 125299 |
| 4 | 86804 |
| 5 | 83989 |

As you can see the minimum distance among the results is for Class 1. This implies that the fingerprint most closely matched Class 1, which is correct. A thorough testing of the classifier was not performed due to limitations in time. However, from the results obtained the verification system seemed to perform extremely well considering the fingerprints were all the same type.

This research project permitted us to learn topics discussed in class as well as new topics. These include Gabor Filters, interpolation methods (rotation), and classification techniques. For the future, an improved center point determination algorithm that is more accurate should be considered. The project turned out to be an interesting experience in which team work and time management were important.

## 3.7 MEMORY PAGING & PROFILE RESULTS

The following table shows the results of profiling the code on the EVM:

|  |  |  |
| --- | --- | --- |
| Code |  | No of cycles |
| Rotation |  | 191887842 |
| Sectorization/Gabor extraction | Filtering/Feature | 1.022 x 1010 |

Rotation – Internal Memory:

N/A

Rotation – External Memory:

|  |  |
| --- | --- |
| Variable | Size |
| Frame | 256x256x4 |
| Result | 362x362x4 |
| Points | 8 |
| Total | 786328 bytes |

Gabor – Internal Memory:

62x3x4 = 744 bytes

Gabor – External Memory:

|  |  |
| --- | --- |
| Variable | Size |
| Frame | 255x255x4 |
| Result | 255x255x4 |
| Gabor | 33x33x4 |
| Total | 524,556 bytes |

Due to the time limitation, not much optimization of the EVM code was performed. Simple optimizations such as using a common index for an array were done, but not DMA transfers. Further optimization of both the rotation and the Sectorization/Gabor Filtering code are definitely possible.

## 3.8 Project Units and Segmentation

This section show what unit makes up the whole system in the project

### 3.8.1 Power supply unit

The system is dual powered. The AC and DC source. The system runs on 5v. The AC supply uses a 5v charger module to power our circuit via a USB port.

### 3.8.1.1 AC Power Adapter Source

This ai

### 3.8.1.2 9 Volts Battery Power Supply Source

The DC is from a 9v which is regulated and filtered down to a smooth 5v suitable for the circuit.

A power supply is an electrical device that supplies electric power to an electrical load. The primary function of a power supply is to convert electric current from a source to the correct voltage, current, and frequency to power the load. As a result, power supplies are sometimes referred to as electric power converters

Component List:

1. Voltage regulator
2. Capacitors
3. Diodes

Component Rating

Voltage regulator:

As we require a 5V we need LM7805 Voltage Regulator IC.

7805 IC Rating:

* Input voltage range 7V- 35V
* Current rating Ic =1A
* Output voltage range   VMax=5.2V ,VMin=4.8V

Figure 3.0.9 LM7805 Pinout Diagram



Figure 30.10 Power supply from 9Volts schematics



### 3.8.2 Central Processing unit

The processing unit used is that in the Arduino nana. It’s the Atmel 238p micro controller. It is embedded in the Arduino Nano module



Figure 0.11 Arduino Nano Pin Out

### 3.8.3 The Fingerprint Sensor Unit



Figure 3.0.12Finger print capture

Supply voltage: 3.6 - 6.0VDC  
Operating current: 120mA max  
Fingerprint imaging time: <1.0 seconds  
Window area: 14mm x 18mm  
Signature file: 256 bytes  
Template file: 512 bytes  
Storage capacity: 162 templates  
False Acceptance Rate: <0.001% (Security level 3)  
False Reject Rate: <1.0% (Security level 3)  
Interface: TTL Serial  
Baud rate: 9600, 19200, 28800, 38400, 57600 (default is 57600)  
Full Dimensions: 56 x 20 x 21.5mm

### 3.8.4 Alert Unit

### 3.8.4.1 Visual Unit

This is simply the LCD Module and LEDS

This unit alerts and updates the user about what is going in the sytem.

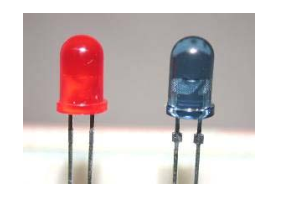


Figure 3.13 Visual Unit: LED

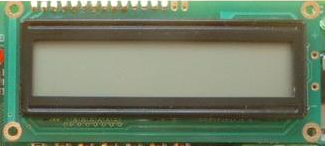


Figure 3.14 Visual Unit : LCD

### 3.8.4.2 Audio unit

This is the buzzer

## 3.9 System Design Flowchart



### 3.10 Micro Controller Code

## 3.11 Circuit Diagram

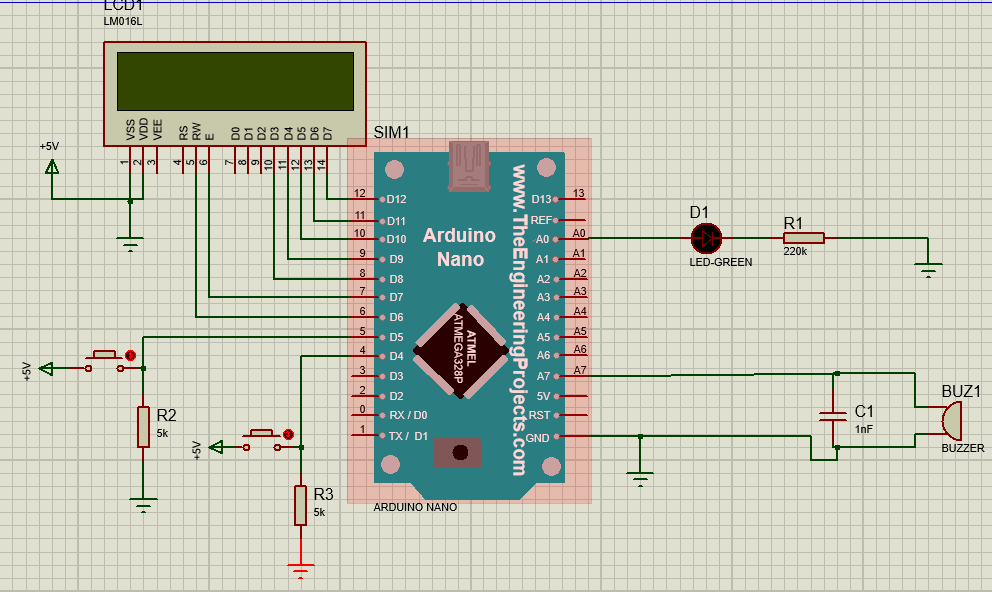


Figure 3.0.15 Circuit Diagram

# CHAPTER 4

# TESTING AND TROUBLESHOOTING

## 4.0 Bill of Engineering Measurement and Evaluation

|  |  |  |  |
| --- | --- | --- | --- |
| COMPONENT | PRICE | QUANTITY | TOTAL |
| Finger Print Module (FPM 10A) | #15,000 | 1 | #15,000 |
| ARDUINO NANO | #2,000 | 1 | #2,000 |
| BLUE LCD 1602 | #800 | 1 | #800 |
| Female Header | #100 | 1 | #100 |
| Male Header | #50 | 1 | #50 |
| Arduino Nano Expansion Board | #1,000 | 1 | #1,000 |
| SD Card Module | #500 | 1 | #500 |
| Jumper wire | #1,500 | 1 | #1,500 |
| Power supply Unit | #2,000 | 1 | #2,000 |
| Project casing | #1,500 | 1 | #1,500 |
| SD card 2GB | #1,000 | 1 | #1,000 |
| Battery Clip | #50 | 1 | #50 |
| Battery (9volts) | #100 | 1 | #100 |
| 7805 Voltage regulator | #100 | 1 | #100 |
| Resistor | #10 | 5 | #50 |
| Sound Buzzer | #200 | 1 | #200 |
| Capacitor | #30 | 3 | #90 |
| Shipping fee | #2,000 | 1 | #2,000 |
| TOTAL | | | #28,040 |

## 4.0 Project timeline

* Coming up with project content and task sharing.
* Get working circuit diagram. | Getting pre-Chapters ready.
* Simulation working circuit diagram | Chapter 1 and 2 typed and reviewed.
* Order components online.
* Get component and breadboard a working prototype.
* Complete the working model. | Chapter 3 and 4 typed and review.
* Clean up Project Hardware connections.
* Clean up project physical appearance and the external power supply unit.
* Chapter 5 typed and reviewed.

# CHAPTER 5

# CONCLUTIONS AND RECOMMMENDATIONS

# REFERENCE

Adafruits :

https://*adafruits.com/products/751* posted 4 May 2014

Nick Koumaris :

<https://create.arduino.cc> posted May 27, 2017

Open source librry:

<https://github.com/adafruit/Adafruit-Fingerprint-Sensor-Library>

LM78XX/LM78XXA Rev. 1.0 Datasheet:

https://www.fairchildsemi.com

1. The reason will be discussed later in the rotation section. [↑](#footnote-ref-1)