

DESIGN AND CONSTRUCTION OF A BIOMETRIC APPLICATION SYSTEM FOR EXAMINATION HALLS.

**OJIMA BENJAMIN UFARUNA
2004/18852EE**

**ELECTRICAL AND COMPUTER ENGINEERING
DEPARTMENT FEDERAL UNIVERSITY OF TECHNOLOGY,
MINNA, NIGER STATE**

DECEMBER 2009.

DESIGN AND CONSTRUCTION OF A BIOMETRIC APPLICATION SYSTEM FOR EXAMINATION HALLS.

**OJIMA BENJAMIN UFARUNA
2004/18852EE**

A THESIS SUBMITTED TO THE DEPARTMENT OF ELECTRICAL AND
COMPUTER ENGINEERING, FEDERAL UNIVERSITY OF
TECHNOLOGY,
MINNA.

DECEMBER 2009.

DEDICATION


This final year project is dedicated to God almighty, the infinite wisdom behind the operations of the earth and to all persons out there who are craving to creatively improve various systems within their environment.

DECLARATION

I hereby declare that this is my work and has not been submitted before any where for the purpose of awarding of degree to the best of my knowledge.

UFARUNA OJIMA BENJAMIN

.....
(Name of student)

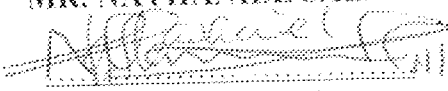

..... 11/07/10
(Signature and date)

ENGR. DR. Y.A ADEDIRAN

.....
(Name of H.O.D)

May 6, 2010
.....
(Signature and date)

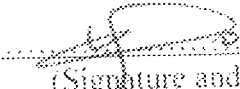
MR. NATHANIEL SALAWU


..... 11/07/10
(Name of Supervisor)

.....
(Signature and date)

DR. (Mrs.) B.A. ADENYI

.....
(Name of External Examiner)


..... 09/03/10
(Signature and date)

ACKNOWLEDGEMENT

First and foremost, I want to thank God almighty for his ever increasing and never failing love that has enabled me to see the ultimate moment and conclusive phase of obtaining a first degree. Without God, this would never have happened. All glory is to him.

Secondly, I want to thank my parents who have really and truly being supportive in all facets of life through out my stay in school. They showed so much love and care. They were always there through the dark days and the bad times. They could always be counted on. I really appreciate your efforts. God bless you.

I also want to thank my siblings for their love and support, their prayers, their advice, their contributions throughout my stay in school. God bless you all.

I want to acknowledge my project supervisor, Mr. Nathaniel Salawu who approved this project topic. He took time out of his busy schedule to make this possible and was always helpful throughout the period. God bless you sir. I also want to thank my project co-supervisor, Mr. Bukola Olawuyi for his help throughout the period of this project. I want to thank all those whose knowledge and skill rubbed off on me all through my stay in school. God bless you all.

I acknowledge the entire lecturers of the Department of Electrical / Computer Engineering for their work throughout these 5years.

I also want to acknowledge all my friends; charles, kingsley, Galaxy, Popsy, Abdulrahman, and all those not mentioned, that made school fun through out these years and were really helpful in one way or the other. Finally I want to thank the members of my

project group and all my class mate for their support and for making it up to this time. To all that died while in school, may your soul rest in peace. Amen.

ABSTRACT

The purpose of this project is to automate the process of verifying student's identity before entry into an examination hall, eliminating every form of human involvement in the process. As we drift towards perfecting various systems within our environment to make them more reliable and credible, minimizing human error is a major step towards this goal. Hence the need to automate processes. The Biometric Application System consists of a software module and a hardware module. The software module provides the functionalities for verifying a student's identity by means of a fingerprint sample. If the student is eligible for the examination, a signal is sent to the door circuit (hardware module) to open the door to the examination hall. After some seconds the door closes and the verification process continues.

Table of Contents

Cover Page	
Title Page	
Dedication.....	i
Declaration.....	ii
Acknowledgement.....	iii
Abstract.....	v
List of figures.....	vi
List of tables.....	vii
CHAPTER ONE: Introduction.....	1
1.1 Preamble.....	1
1.2 Aims and Objectives.....	2
1.3 Methodology.....	2
1.4 Scope of work.....	3
1.5 Sources of materials used.....	3
1.6 Constraints to achievable performance.....	3
1.7 Other Persons involved.....	4
CHAPTER TWO: Literature review.....	5
2.1 Historical Background.....	5
2.2 Types of Biometric.....	6

2.2.1 DNA.....	7
2.2.2 EAR.....	7
2.2.3 FACE.....	8
2.2.4 FINGERPRINT.....	8
2.2.5 GAIT.....	9
2.2.6 IRIS.....	9
2.2.7 KEYSTROKE.....	10
2.2.8 ODOUR.....	10
2.2.9 RETINA.....	11
2.2.1.0 SIGNATURE.....	11
2.2.1.1 VEIN THERMOGRAM.....	12
2.2.1.2 VOICE.....	12
2.3 Types of Biometric Systems.....	13
2.4 Biometric System Model Modules.....	13
2.4.1 Data Collection.....	13
2.4.2 Signal Processing.....	14
2.4.3 Transmission.....	14
2.4.4 Storage.....	14
2.4.5 Decision.....	15

2.5 Biometric Applications Characterizations.....	15
2.5.1 Overt x Covert	15
2.5.2 Optional x Mandatory	16
2.5.3 Fixed Duration x Indefinite Duration	16
2.5.4 Public x Private	16
2.5.5 Open x Closed	16
2.5.6 Habituated x Non-Habituated	17
2.5.7 Standard x Non-standard Environment	17
2.5.8 User Ownership x Institutional Ownership of Biometric Data	17
2.5.9 Template Storage x Identifiable Data Storage	18
2.5.1.0 Supervised x Non-Supervised	18
2.5.1.1 Example of characterizing biometric applications	18
CHAPTER THREE: Design and Analysis	20
3.1 Software Module	20
3.2 Biometric Application Design.....	20
3.3 Fingerprint Capture.....	24
3.4 Fingerprint Image Format.....	24
3.5 Colour Coding Format.....	24
3.6 Contexts.....	24

3.7 Threshold and Rotation Tolerance.....	25
3.8 Hardware Module.....	26
3.8.1 Parallel Port.....	26
3.8.2 Buffers.....	29
3.8.3 Power Supply.....	29
3.8.3.1 Transformer Specification.....	30
3.8.3.2 Rectifier.....	30
3.8.3.3 Filters.....	32
3.8.3.4 Voltage Regulation.....	33
3.9 System Controller Module.....	34
3.1.0 Visual Display Unit.....	35
3.1.1.0 LCD interfacing with System Controller.....	35
CHAPTER FOUR: Tests, Results and Discussion.....	39
4.1 Testing of various units.....	39
4.1.1 The Software Module.....	39
4.1.2 The Parallel Port.....	40
4.1.3 System Controller Module.....	41
CHAPTER FIVE: Conclusion and Recommendations.....	42
5.1 Recommendations for Further Work.....	42

References.....43

Appendix.....44

LIST OF FIGURES

	Page
Fig 3.1 Flow chart showing operation of software module of biometric application.....	22
Fig 3.2 Circuit diagram of external door module.....	23
Fig 3.3 Pin Configuration of parallel port.....	27
Fig 3.4 Pin Configuration of CD4049.....	29
Fig 3.5 Block diagram showing AC signal conversion in the power supply unit.....	29
Fig 3.6 Diagram showing input signal into a bridge rectifier and its output.....	31
Fig 3.7 Diagram showing input and output signal through a capacitor.....	32
Fig 3.8 Diagram of the AT89C52 Microcontroller.....	34
Fig 3.9 Pin Layout of the AT89C52 Microcontroller.....	34
Fig 3.1.0 Diagram of the 16X2 LCD Display.....	35

LIST OF TABLES

	Page
3.1 Pin Assignments of the D-Type 25 pin Parallel Port Connector.....	28
3.2 Pin description of the AT89C52.....	35
3.3 LCD Pins and Their Functions.....	37

CHAPTER ONE

INTRODUCTION

1.1 Preamble

In the course of human existence, there have been several instances of interference with various systems. This interference in most cases has compromised the integrity of such systems and has reduced dependency on such systems.

For example, a student writing an examination for another student exemplifies human interference with a system, which in this case is the examination system. A student involved in such an act that goes undetected undermines the credibility of the examination system. There are innumerable instances of such interferences occurring every day. Hence the question of how to reduce interference with systems by humans arises.

In the quest to reduce interference with systems, the idea of automating systems has arrived on the scene. This reduces to a great extent the incidence of interference with systems.

The process of verifying a student's identity before entry into an examination hall constitutes a system which could be negatively influenced by humans and could foster cases of false identity undermining the credibility of the examination process. Officers who are assigned to perform the exercise of verification could be bribed, e.t.c. to allow impersonation. Hence there is a need to automate this process to reduce human involvement to the barest minimum.

This is where the biometric application System for examination halls comes in. It is a drift from the conventional method of verifying a student's identity to a more reliable method that attempts to avoid or reduce human interference to a zero or minimum level by using undisputed characteristics of humans for identification.

1.2 Aims and Objectives

The aims and objectives of this project are enumerated below

- 1 To design and construct a biometric application system for examination halls which would consist of a software module and a hardware module.
- 2 The software module would be completely written and deployed on the java platform and would provide an interface for verification of the students Identity based on fingerprint samples.
- 3 The software module would also provide other functionalities like enrolment of the student's biometric data, extraction of the student's fingerprint data, an interface that displays the student's fingerprint sample along with its minutiae, e.t.c. a database that stores the student's biometric data at the back end, a status bar that displays information about what's currently happening in the software module. On successful verification of the student's identity, the student's bio-data along with his or her picture will be displayed. When not successful, a prompt will be displayed to that effect.
- 4 The hardware module will simulate the opening of a door and would be constructed majorly with a microcontroller.
- 5 The hardware module will interface with the software module through the parallel port of the computer.

- 6 The output will be displayed through an LCD

1.3 Methodology

In the design of this biometric application system, an algorithm was written for the operation of the biometric application system and was implemented using the java programming language. The database used is Mysql. The hardware module was constructed using an AT95C2 micro-controller. Pin 2 and Pin 18 to Pin 25 of the parallel

port were used as the active and ground pins respectively and were connected to the micro-controller.

1.4 Scope of the work

The biometric application system is limited only to the use of fingerprint biometrics in identifying an individual and the opening of a door upon verification of the individual's identity.

1.5 Sources of materials used.

Most of the materials used in carrying out this work were sourced locally here in Minna at affordable prices in various electronic shops found around town.

Other sources of information used in the design and construction of this project work includes the internet, libraries(both school and state libraries), consultation with friends, technicians and other experts in the field

1.6 Constraints to achievable performance

The constraints to achievable performance could have risen as a result of the following factors;

- 1 Power failure was rampant during the period in which this project was carried out, as a result the progress of the work was slowed down.
- 2 Also some of the components due to their high degree of sensitivity to temperature were damaged by the soldering iron.
- 3 Another constraint was the difficulty in getting some of the components used in constructing the hardware module, as a result substitutes were used, which might not function as accurately as the original ones.

1.7 **Other Persons involved**

In the course of this project work, the services of other persons such as professionals in the field, technicians, electronic engineers (inside and outside of the department), and fellow classmates were employed.

CHAPTER TWO

LITERATURE REVIEW

2.1 Historical Background

There are evidences of biometric uses on human history as early as pre-historical age. Estimated 31000 years old, caves were adorned with pre-historical pictures apparently signed by fingerprint stamps of authors. Evidence exists, of the use of fingerprints by Babylonian at 500 B.C. They recorded business transactions on clay tables in which fingerprint stamps were found [1].

The first reported use of biometrics was related by Portuguese explorer João de Barros in the 14th century. He described the practice of Chinese merchants stamping children's palm-prints and footprint to distinguish one from another [2].

The first real biometric system was created in 1870 by French anthropologist Alphonse Bertillon who turned biometrics into a distinguished field of study. He developed an identification system (Bertillonage) based on detailed records of body measurement, physical description and photographs. Despite their imprecise measures and difficulty to apply methodology, the Bertillonage was an important advancement on criminal and people identification. It began to fail when it was discovered that many people share the same anthropologic measures [3].

The first classification method for fingerprints was developed in 1892 by Sir, Francis Galton. The features used by Galton's method were the minutiae that are still used nowadays.

Some years later in 1896, Sir Edward Henry, General Inspector of the Bengal police, began to use Galton's method to replace the anthropometrics system for identification of criminals. Henry created a method to classify and store fingerprint that lets a quick

searching of records. Later, that method was introduced by Henry in London for the first British fingerprint file. Each biometric characteristic has its own advantages and disadvantages, therefore, the question of which biometric characteristic should be used for a given authentication application, depends on the application requirements [4].

2.2 Types of Biometrics

A number of biometric characteristics have been proposed for authentication purposes. Traditionally, they can be categorized into two major groups: physical or behavioral characteristics. Examples of physical characteristics include: DNA, ear, face, fingerprint, hand geometry, iris, and retina. Behavioural characteristics include: gait, signature, and voice [5].

A summary of these characteristics is given below:

1. DNA
2. EAR
3. FACE
4. FINGERPRINT
5. GAIT
6. HAND GEOMETRY
7. IRIS
8. KEYSTROKE
9. ODOUR
10. RETINA
11. SIGNATURE
12. VEIN THERMOGRAM
13. VOICE

2.2.1 DNA

DNA stands for Deoxyribonucleic Acid and is a molecule that contains biological instructions of the living organisms. The DNA is composed of chemical building blocks called nucleotides. A sequence of DNA that contains information for producing a protein is known as gene, whereas the whole DNA instructions of the organisms are called genome. The human genome is shared about 99.5% to 99.9% across the human beings, however, even the small percentage difference are of the order of millions of base pairs. The human genome is unique to each individual; however this affirmation is not valid for identical twins since they share the same DNA patterns. The low degree of popularity of this biometric characteristic is based on three factors:

1. Privacy concerns: some additional information of the individual could be obtained such as diseases.
2. Real-time authentication capabilities: this technique involves high computational resources and is difficult to be automated since it requires some chemical processes.
3. Access availability: it is easy to steal a piece of DNA from an individual and this information could be used for fraudulent purposes [5].

2.2.2 EAR

The topology of the ear has been suggested as an alternative biometric technique. This suggestion is based on the fact that the ear grows proportionally after the first four months of birth and therefore the ear's structure of an individual should remain the same over time. However, it has been studied, that gravity can cause some stretching of the ear in the vertical direction. Therefore, its features are not expected to be very distinctive for authentication purposes. In spite of this observation, ear-based authentication can be used as a supplementary biometric technique. One could, for example, combine face

authentication with ear authentication tasks by taking into advantage that the same device could be used to capture both biometric characteristics [5].

2.2.3 FACE

Face recognition is perhaps the most friendly and acceptable way to conduct human authentication. These facts rely basically on its easy collectability mechanisms and its non-intrusive property, e.g., people generally accept this biometric characteristic as a valid authentication method. The face recognition process often involves three different steps:

- i. Detect whether there exists a face in an image.
- ii. Locate the face(s) if it is case
- iii. Recognize the face(s).

For each of the three mentioned steps, there are some challenges to be considered. First, face images are captured under non-controlled conditions. Therefore, these images may be characterized by the presence of different illumination conditions and backgrounds. Furthermore, changes in the facial expressions and occlusions of some facial features may reduce the overall recognition accuracy. Due to these facts, face recognition is a challenging research field [5].

2.2.4 FINGERPRINT

Fingerprints are considered nowadays as one of the most reliable biometric characteristic for human recognition due to their individuality and persistence. A fingerprint consists basically of a pattern of ridges and valleys in the surface of the fingertips and its formation is related to the earlier fetal months. Maybe its main disadvantage is related to its intrusiveness, since people need to cooperate explicitly when providing their fingerprints to the system. Furthermore, fingerprint-based authentication is traditionally associated with criminal-authentication methods. State-of-the-art

authentication methods have demonstrated adequate accuracies for fingerprint recognition methods, however, for the sake of human identification they are still some open tasks. First, the processing time of the current algorithms should be reduced since the output of such systems should be done in real time. Second, the non-controlled interaction between users and capture devices will produce miss aligned and rotated images [5].

2.2.5 GAIT

Gait is an emergent behavioral characteristic used to authenticate people by the way they walk. The attractiveness of this technique relies in its unobtrusive properties, since individuals are authenticated at certain distances without any need of big co-operation efforts. Furthermore, it has received attention from studies in medicine, psychology, and human body modeling, to create a gait signature: some models are built based on temporal and spatial metrics of the human motion.

Despite all of the benefits of gait, gait is not supposed to be very distinctive across individuals and therefore it is not well suited for high-security scenarios. In addition, since this technique involves video-sequence analysis, it may be computationally expensive [5].

2.2.6 IRIS

Its visual texture information is formed during the fetal period and its formation is extended up to the first two years of life. Iris-based authentication methods take into advantage the fact that the iris information is unique across individuals, and its main characteristics do not change over time, as is the case of fingerprints. Besides its main properties, the texture of the iris is believed to be very difficult to be modified surgically. Although it benefits, its main properties are affected by its intrusiveness, since it needs a high collaboration effort of the individuals [5].

2.2.7 KEYSTROKES

Keystroke dynamics is related to the way people type characters on keyboards. Its attention as an emerging biometric characteristic is supported by psychological studies which demonstrate that human repetitive actions are predictable, and therefore an individual could be characterized by their keystroke dynamics. This kind of systems aims to capture the inter-key and hold times of the user's keyboard interaction in order to provide unique representations for each individual. The inter-key time is referred to as the latency periods between keystrokes, whereas the hold times represents the period of time between the hit and release of a key hold. One of the main benefits of this technique is that it allows "continuous authentication", since the individual can be analyzed over a large periods of time [5].

2.2.8 ODOUR

Given that biological organisms are composed of chemical elements, each organism produces a given odour that is characteristic to that organism. Therefore, odour could be used as a distinctive characteristic across species. Human beings or animals capture odour because of smell receptors connected to the olfactory nerve. The receptors are specialized in specific kinds of odorants. Therefore, they are just activated to the odorant they respond. The excited cells propagate some pulses to a part of the brain known as the olfactory bulb. The olfactory receptor neurons consist in nerve cells that are able to capture specific chemical components in the inhaled air. The combination of the chemical components captured by the receptors determines finally the captured odour. Furthermore, the intensity of the stimulus is determined by the number of activated receptors. On the other hand, the study of odour for human authentication is under investigation both in the academic world and in the industry. Since this is a very complex

task, practical devices are still not available. Furthermore, it is not clear if odour is affected by external factors such as deodorants, perfumes, etc [5].

2.2.9 RETINA

The pattern of veins beneath the back of the eyeball is called Retina. It is believed to be unique to each person as well as the most secure biometric technique. To be captured, a low intensity beam or infrared light is projected into the eye so that a predetermined part of the retinal vasculature can be digitized. The image acquisition process requires cooperation of the subject, since he/she has to gaze into an eye-piece and focus at a specific spot in the visual field. Due to these reasons, as well as the cost of retina scanners, retinal-based techniques have not become yet very popular. However, there are nowadays a large number of highly secure environments, in which retina scan is adopted as a perfect solution [5].

2.2.1.0 SIGNATURE

The handwriting of a given individual can be thought as representing his/her own characteristics. Signatures have been widely used in different areas ranging from government and legal applications to commercial ones. Traditionally, signature authentication may be either static or dynamic. Static signature authentication uses only the geometric features of the signatures, whereas the dynamic authentication uses not only those features, but also some additional information such as velocity, acceleration, pressure, and trajectory of the signatures. Furthermore, although it has proven reasonable authentication accuracy, it is not high enough for large-scale applications. This observation relies basically on the fact, that signatures present some variations due to the physical and emotional state of a person, and at the same time may vary over a period of time. However, such systems may be incorporated transparently since individuals are used to provide their signatures in different environments of their daily life [5].

2.2.1.1 VEIN THERMOGRAM

Vein patterns are believed to be unique across individuals and invariant to time, even in the case of identical twins. Due to these reasons, vein patterns could be used to authenticate individuals. An image of the vascular patterns is obtained by using an infrared sensor that captures the hemoglobin in the blood. Traditionally, the deoxygenated hemoglobin appears as black patterns in the captured image, whilst the hand or fingers have lighter patterns. One of the challenges in capturing the hand vein structure is that the veins usually move and they flex as the blood is pumped through the human body. Some of the actual capture devices appear not only to have solved this shortcoming, but also its size has been reduced so as to make them portable, and therefore making this biometric characteristic feasible in nowadays applications. The main disadvantage of this biometric characteristic is related to the cost of the infrared sensors as well as the changes in the hand [5].

2.2.1.2 VOICE

Voice is a combination of physical and behavioral characteristics that are related to the voice signal patterns of a given individual. The physical characteristics of voice are related to the appendages that form its sound. These characteristics include for example, the vocal tracts, mouth, nasal cavities, and lips. On the other hand, the behavioral characteristics of voice are related to the emotional and physical states of the speaker. Traditionally, voice-based authentication methods can be divided into two major groups: text-dependent and text-independent methods. In text-dependent techniques, the individuals are authenticated by speaking a fixed predetermined phrase, whereas in text-independent techniques no constraints exist about what has to be spoken. Furthermore, text-independent authentication tasks are more complex than text-dependent tasks, but they offer at the same time more reliability. Regardless of their classification type, voice-

based authentication methods have to face some challenges related for example to the room acoustics, misspoken phrases or individuals emotional states. Due to all of this variability, this technique is not adequate for large-scale systems [5].

2.3 Types of Biometric Systems

Basically, there exist two types of biometric authentication systems: verification systems and identification systems [6].

- In a Verification System the input is a claimed identity and a biometric record. The system compares that biometric record with the biometric record stored in database for that identity in order to verify the claimed identity. In that kind of system only a comparison is performed.
- In an Identification System the input is just a biometric record. The system must search a (probably large) database looking for the biometric data most similar with an input query biometric data and must decide if both of them belong to the same person. In that kind of system many comparisons are performed.

One particular case of identification system is the Watch List System. In that kind of system, there exist lists of "wanted" persons and given an input biometric record the system must decide if that record matches with some of the individuals on the watch list.

2.4 Biometric System Model Modules

Different biometric systems share a common general flow. That common model is defined as a set of modules or components: data collection, transmission, Signal processing, storage, matching score and decision [6].

2.4.1 Data Collection

The first step for the use of a biometric system is the capture and acquisition of biometric data from biometric sensor hardware. Usually, it is affected by human factors,

environmental conditions and quality of sensor used. The final result of enrolment process is an image or signal captured directly from individuals. The Failure to Enrol Rate measures the lack of success of enrolment process [6].

2.4.2 Signal Processing

Signal processing methods and algorithms are applied to the enrolled data in order to detect and extract their main features. Ideally, the extracted biometrical features must describe uniquely an individual. The final result of signal processing component is the template creation. A template is a structure for biometric features representation. The algorithms used for extraction are proprietary and are the core intellectual property of biometrics vendors [6].

2.4.3 Transmission

In some biometric systems data collection and processing occurs at different places. In those cases biometric data must be transmitted from data collection to the signal processing components. Generally, that transmission process involves a great amount of data and compression techniques are applied. The compression technique used depends on the biometric type. Some standards have been defined. Wavelet Scalar Quantization (WSQ) is the standard compression format for fingerprints images and JPEG200 standard format for facial images. For voice signal, the Code Excited Linear Prediction (CELP) is defined as standard format [6].

2.4.4 Storage (Template Creation)

Biometric data is never stored on database in its original format, i.e. digital image. The signal processing methods detect features on enrolled data and organize them as a so called characteristic vector. A characteristic vector is a description of the main features detected for Signal Processing component and must be small and easy to process. There exists a proposal of standard format of templates for fingerprint based on minutiae point

found in fingerprint images. Nevertheless, usually the template format and type of information it stores is part of the proprietary core intellectual property. Some of the biometric technology contests as FVC (Fingerprint Vendor Competition) impose limits to the memory size of templates generated by algorithms [6].

2.4.5 Decision (Matching)

The final component of a biometric system is the decision or matching component. Decision component compares a query biometric template with the stored template of claimed person and assigns to them a similarity score. That score is used for making decisions about the matching of the templates. In Verification Systems, if the similarity scores are greater than a fixed threshold, the system decides if that template belongs to the same person. In Identification System, the database templates are compared to the query template and higher similarity score templates are selected to decide if some person was identified in the database [6].

2.5 Biometric Applications Characterization

Depending on how a biometric application is deployed it can be classified as:

2.5.1 Overt x Covert

A biometric application is considered overt if the users are aware that their biometric data is being captured and used. As opposed to overt, the covert systems capture and use the biometric data without consent or knowledge of the user. An example of an overt system is the iris and fingerprint recognition system, where the user's cooperation is very important. While the facial and voice recognition don't necessary need the users consent, therefore it is possible to develop a covert application using these technologies [6].

2.5.2 Optional x Mandatory

A biometric system that obligates (imposes) the users to provide their biometric data is considered Mandatory. In such applications, if a user refuses to give their biometric data, they may suffer some punishment. If a biometric system is optional, the user may decide whether to use their biometric data for their identification, in this case their identity can be verified in other ways, such as by presentation of a passport or driver's license [6].

2.5.3 Fixed Duration x Indefinite Duration

This characteristic refers to how long the captured biometric data will be used. This is more related to the privacy of the biometric data. When the biometric captured data are used for a long period, it has a more privacy risk than a short period of use [6].

2.5.4 Public x Private

This category describes the relationship of the user to the system management. Examples of users of public applications include customers. Users of private applications include employees of business or government. Depending on whether the application is public or private, the user's attitude towards biometric devices may vary, which will directly affect the performance of the biometric system [6].

2.5.5 Open x Closed

This category refers to whether the biometrics collected within the system will be shared (open) or remain internal (closed). For example, a fingerprint recognition system used to control the access of the employees to a building and logon to their computer network, may be considered closed if the data aren't shared with other external systems. Other examples are state driver's licenses and entitlement programs. A state may want to communicate with other states or other programs within the same state to eliminate fraud.

This would be an open system, in which standard formats of data and compression would be required to exchange and compare information [6].

2.5.6 Habituated x Non-Habituated

This characteristic describes the frequency of users using the system. In habituated systems, the users tend to use the system periodically, whereas in the non-habituated environment users may enter and leave the system sporadically. This category influences the design of the user interface. In non-habituated environments the user interface must be intuitive and simple because the users do not necessarily spend much time in the system and therefore may not have incentive to spend much time learning the interface. As examples, the use of fingerprints for computer or network access is a habituated use, while the use of fingerprints on a driver's license, which is updated once for several years, is a non-habituated use [6].

2.5.7 Standard x Non-standard Environment

This categorization describes the setting of the system with respect to the temperature, humidity, and other physical conditions of the environment in which the system is installed. The standard environment system tends to operate in an indoor and more controlled environment whereas the non-standard tend to operate in outdoor or less controlled conditions [6].

2.5.8 User Ownership x Institutional Ownership of Biometric Data

In a user ownership system, the user maintains ownership over his or her biometric information, whereas in other case the public or private institution owns the users biometric data. This characteristic has to do much with privacy of the biometric data. User control over collection, usage, and disposal of biometric information is not possible in every deployment, especially in entitlement programs or other public sector uses [6].

2.5.9 Template Storage x Identifiable Data Storage

The biometric data may be stored as a mathematical model (template) or as identifiable by human sample (images, audio, etc). Biometric templates are generally only of value when processed through a vendor algorithm, and cannot be linked with a specific biometric characteristic without dedicated processing. Biometric images are generally identifiable, and can be associated with a specific individual based on visual or aural inspection. As example, in a fingerprint system only the fingerprint image or the minutiae information can be stored [6].

2.5.1.0 Supervised x Non-Supervised

This category refers to whether the use of the biometric device during operation will be observed and guided by system management. Non-cooperative applications will generally require supervised operation, while cooperative operation may or may not. Nearly all systems supervise the enrolment process.

2.5.1.1 Example of characterizing biometric applications

The following example shows, how a real application can be described using the above characteristics. The Immigration and Naturalization Service's Passenger Accelerated Service System (INSPASS) is a biometric system used since 1990 at many airports of USA and Canada, with the aim to reduce the inspection processing time for authorized travellers. The INSPASS system uses the hand geometry biometric for the verification of the travellers. In order to use this system the traveller must obtain an INSPASS card in the enrolment centre before travelling, there the hand geometry template is captured and stored in the card. When the travellers next arrive at the airport, they go directly to the INSPASS terminal which is able to read the INSPASS card and allow the person to key in their flight details. The terminal is connected to a remote computer which checks the validity of the card and the traveller must then place their

hands on the hand geometry reader to give a new sample for comparison with the template printed on their INSPASS card. This system can be classified as an overt, optional, fixed duration, public, closed, non-habituated, standard environment, and institutional ownership of biometric data, template storage and non-supervised application.

- It is overt because the travelers are aware that they are required to give a biometric measure as a condition of enrollment into this system.
- It is optional because the passengers can choose the normal inspection control if they do not want to use the INSPASS system.
- It is of fixed duration because the validity of the enrolled data is normally one year.
- The system is public because enrollment is open to any frequent traveler into the United States.
- It is closed because INSPASS does not exchange biometric information with any other system.
- It is non-habituated because most international travelers use the system less than once per month.
- It is of institutional ownership of biometric data, because the hand geometry templates are also stored on a central computer of INSPASS, each time when a person is verified, the template is updated.
- It is template storage because only the geometric information of the hand is stored, the template has 14 bytes of size.
- It is non-supervised and in a standard environment because collection of the biometric data will occur near the passport inspection counter inside the airports, but not under the direct observation of an INSPASS employee [6].

CHAPTER THREE

DESIGN AND ANALYSIS

3.1 Software Module

The Software module was developed using the following Application Programming Interfaces (API's):

- Java API
- Griaffe Fingerprint SDK (software development kit)
- RXTX Comm API
- L2FProd API

3.2 Biometric Application Design

The Operation of the biometric application involves four basic steps:

- i Initializing the Finger Print based SDK library
- ii Start Capturing images from a Fingerprint reader or loading them from files
- iii Extract a template for each image
- iv Choose among enrolling a template or matching it against other templates in a database. Usually the Capturing, extracting, enrolling, Identifying or matching steps are repeated until the application is finished.

The auto - identify and auto - extract check box options of the biometric application are checked by default. It is designed as such so that the user of the application can operate the application with minimal instructions. Since the main purpose of the application is to identify candidates with the help of their fingerprint samples before entry into an examination hall, it makes sense that the auto identify and auto extract option be checked by default. This is also to enable the application to be user friendly.

When a fingerprint sample is loaded from a file and extracted, the application compares the given fingerprint (query) with all the recorded fingerprints (references) in the system to find a match. When a match is found, some bio-data, information and passport of the identified individual is displayed on the interface of the application along with the extracted fingerprint sample. An active low digital signal is sent to pin 2 of the parallel port for six seconds and then an active high signal is sent subsequently to pin 2 of the parallel port. An active low digital signal is first sent because an inverter (CD4049) interfaces between the parallel port and the door. To get an inverted output at the door circuit that is active High, then an active low signal must be sent from the application. This activates the external door circuit for some seconds. It is designed as such to proof that an individual has being identified. When a match is not found, an appropriate prompt is displayed to that effect to notify the user of the application that such an individual does not exist in the school's database. A text pane at the bottom of the application's interface displays information about the current activity going on in the application.

The flow chart for the operation of the software module of the biometric application is shown in fig. 3.1;

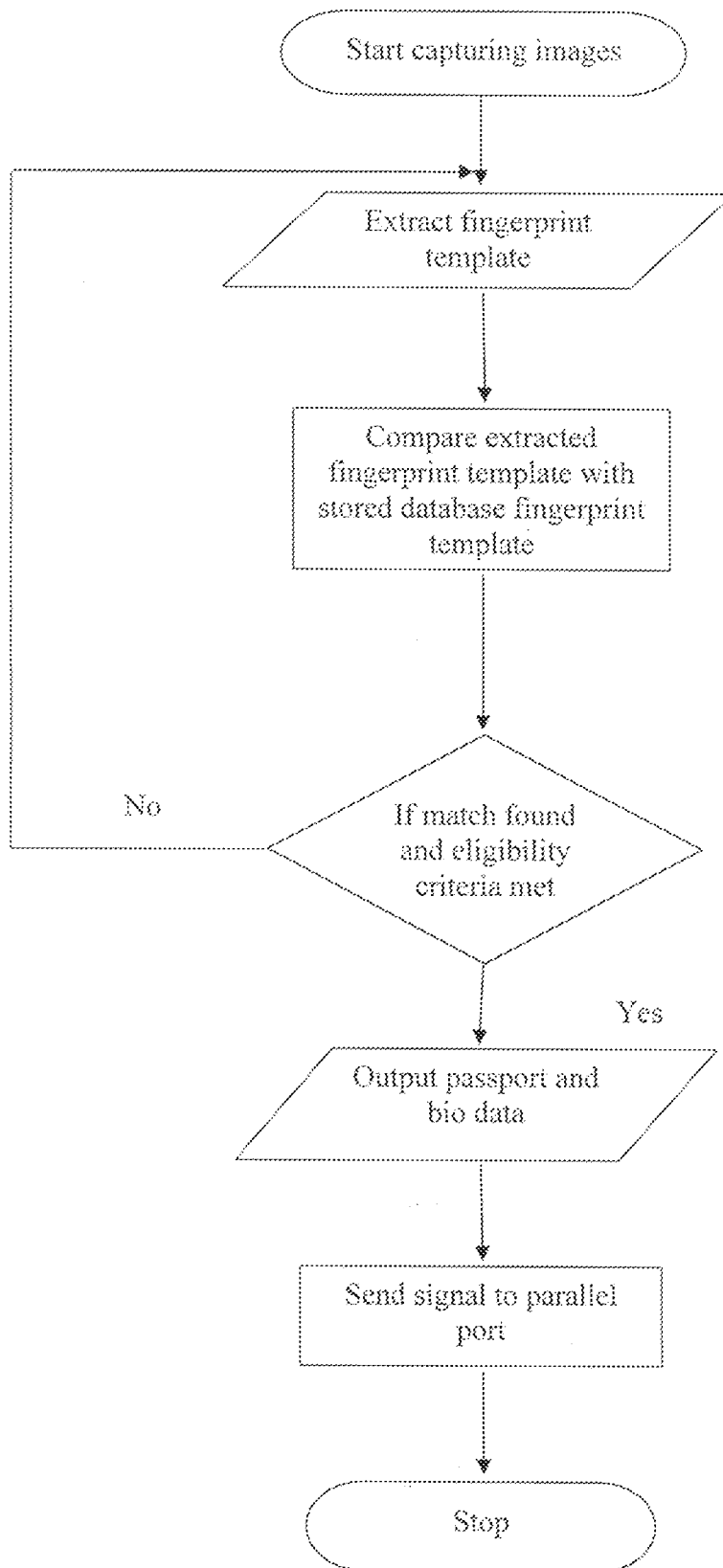


Fig. 3.1: flow chart showing operation of software module of the biometric application

The circuit diagram for the operation of the door module is shown in fig. 3.2:

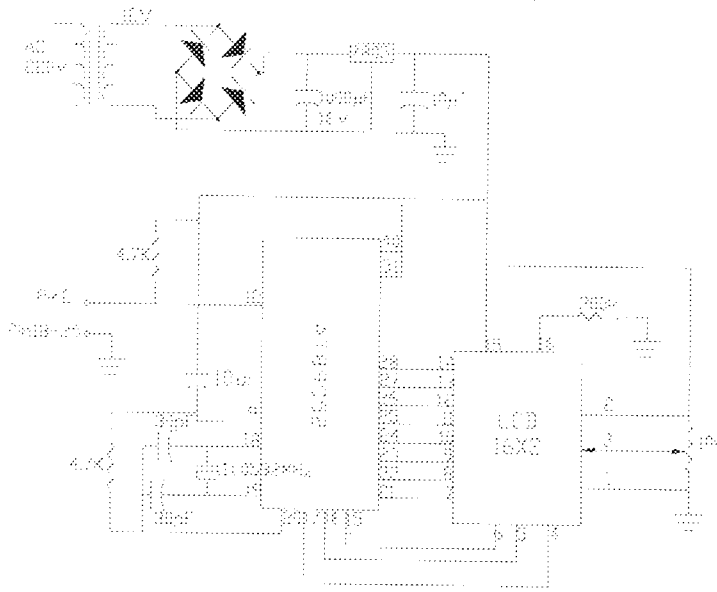


Fig. 3.2: circuit diagram of external door module

3.3 Fingerprint Capture

Once the capture module is initialized, whenever a fingerprint sample is loaded into the application either from a file or from a fingerprint reader, a corresponding event is fired. When the capture module is initialized, a special sensor is automatically plugged, firing the corresponding plugging event: the "File" sensor. Enabling image capture on this special sensor is required in order to load fingerprint images from picture files.

3.4 Fingerprint Image Format

The fingerprint image format used in the Fingerprint SDK library is an array of width * height unsigned bytes. Each byte represents a single pixel of the image. The array is arranged in left to right, top to bottom order. There's no padding, each line immediately follows the previous one. Each pixel has a grayscale value ranging from 0 (pure black) to 255 (pure white). This format does not store information about the resolution or size (width and height) of the image.

3.5 Color Coding Format

The color coding format used by the Fingerprint SDK library is the BGR 24-bits format. Each color channel has 256 levels (0 to 255) and the color is coded as the integer number composed by the three channels values in the strict order blue-green-red (most significant byte to least significant byte), or, $\text{blue} \times 65536 + \text{green} \times 256 + \text{red}$.

Some examples:

- 255 (decimal) or 0000FF (hex) means pure red;
- 65280 (decimal) or 00FF00 (hex) means pure green;

3.6 Contexts

Contexts are an advanced feature used to:

- allow two or more biometric operations to be executed at the same time

- create different ready-to-use identification or verification environments

Most biometric applications are interactive and don't execute more than one biometric operation at a time, using just the default context. But, for example, to perform two fingerprint identifications simultaneously on a multithreaded server, each identification must be executed on its own context. Two operations must not be called simultaneously in the same context because they are not guaranteed to be thread-safe. Creating a new context for each operation that will be executed simultaneously guarantees the thread safety.

Furthermore, each context has its own matching parameters, making it possible to create different identification or verification environments. For example, in a two-level security biometric application, instead of tightening or lowering the matching parameters depending on the security level before performing a matching, two contexts, each one with the appropriate matching parameters, may be created; any fingerprint matching is then performed in a context corresponding to the right security level.

3.7 Thresholds and Rotation Tolerance

The identification and verification functions in Fingerprint SDK library are governed by two important parameters: threshold and rotation tolerance.

The threshold is the minimum score needed to state that two fingerprints do match. The default value is 45 for the identification process and 25 for the verification process, ensuring a 1% FRR. The default values were used in the development of this biometric application

The rotation tolerance defines the maximum acceptable angle variation (in degrees) between two fingerprints being compared that will result in a match. This value is valid in

both clockwise and counter-clockwise directions, so the maximum value that can be set is 180.

3.8 Hardware Module

The software module is interfaced with the hardware module through the parallel port of the computer. The hardware module which is the door module consist of the following components

- Power Supply Unit
- The System controller module
- The visual display unit

3.8.1 Parallel Port

The Parallel Port is the most commonly used port for interfacing homemade projects or small scale projects. This port will allow the input of up to 9 bits or the output of 12 bits at any one given time, thus requiring minimal external circuitry to implement many simpler tasks. The port is composed of 4 control lines, 5 status lines and 8 data lines. It is found commonly on the back of a PC as a D-Type 25 Pin female connector. For the purpose of this project pin 2 and pins 18 - 25 of the data port of the parallel port were used for communication with the door module.

The Data Port or Data Register is simply used for outputting data on the Parallel Port's data lines (Pins 2-9). This register is normally a write only port. If you read from the port, you should get the last byte sent. However if the port is bi-directional, you can receive data on this address.

The pin configuration of a parallel port is shown in fig 3.3;

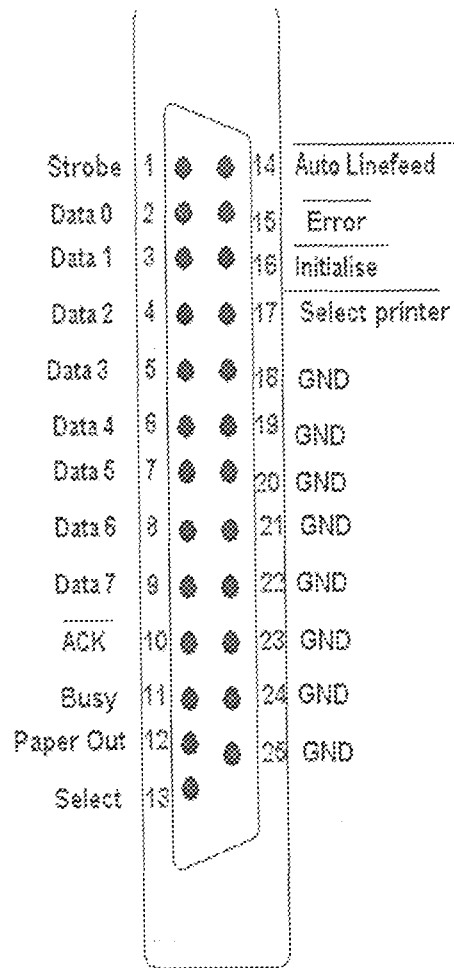


Fig. 3.3: Pin configuration of parallel port

Table 3.1 shows the Pin Assignments of a D-Type 25 pin Parallel Port Connector.

Table 3.1: Pin Assignments of the D-Type 25 pin Parallel Port Connector

Pin No (D-Type 25)	Pin No (Centronics)	SPP Signal	Direction In/out	Register	Hardware Inverted
1	1	nStrobe	In/Out	Control	Yes
2	2	Data 0	Out	Data	
3	3	Data 1	Out	Data	
4	4	Data 2	Out	Data	
5	5	Data 3	Out	Data	
6	6	Data 4	Out	Data	
7	7	Data 5	Out	Data	
8	8	Data 6	Out	Data	
9	9	Data 7	Out	Data	
10	10	nAck	In	Status	
11	11	Busy	In	Status	Yes
12	12	Paper-Out / Paper-End	In	Status	
13	13	Select	In	Status	
14	14	nAuto-Linefeed	In/Out	Control	Yes
15	32	nError / nFault	In	Status	
16	31	nInitialize	In/Out	Control	
17	36	nSelect-Printer / nSelect-In	In/Out	Control	Yes
18 – 25	19-30	Ground	Gnd		

3.8.2 Buffers

Buffers are normally used for the purpose of load isolation. They are also used for digital interfacing. In this project, the CD4049 inverter was used because it was readily available in the market. The pin configuration is shown in Fig 3.4;

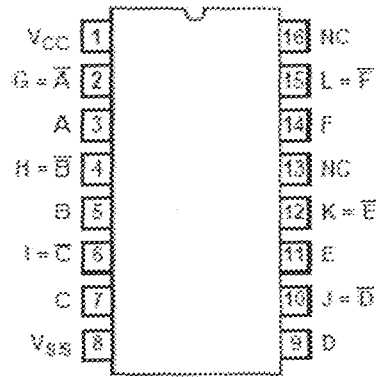


Fig. 3.4: Pin configuration of CD4049

3.8.3 POWER SUPPLY

The integrated circuits used in this project require maximum and minimum electrical power needed for it to function properly. This electrical power is meant to be in form of direct current. Meanwhile, batteries that generate direct current cannot be used simply because they have limited life span and most of them cannot be recharged

However, for effective and efficient transmission of power, the Alternating current source should be converted to a Direct current source; this is achieved as illustrated by the block diagram in fig. 3.5;

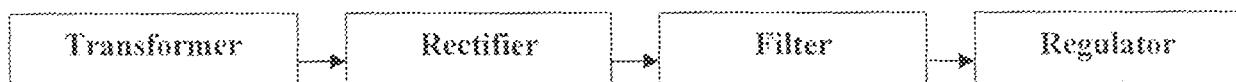


Fig. 3.5: Block diagram showing the conversion of an AC signal to DC signal

3.8.3.1 Transformer specification

The Transformer used for this project is a 12V, 500mA Voltage Transformer. This transformer was not rewound since it was readily available in the market.

3.8.3.2 Rectifier

Rectifier diodes connected in a bridge are used in the circuit convert AC to a pulsating DC. For typical low current rectifiers, the Diode drops about 0.7V, this is the value that will be used for the purpose of analysis.

For a full wave bridge rectifier, two diodes are always conducting while the other two will be in the off state.

D2 and D4 conducts during the period $t=0$ to $t=T/2$ while D1 and D3 are in the non-conducting state. And during the period $t=T/2$ to T , D1 and D3 will conduct while D2 and D4 will be in the off state. The diagram showing the input and output signal through a rectifier is shown in fig. 3.6;

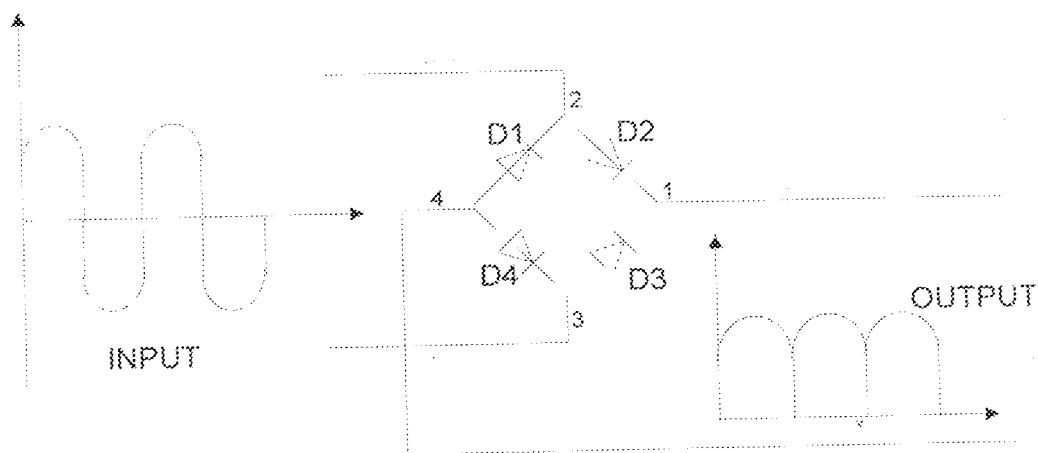


Fig. 3.6: Diagram showing input signal into a bridge rectifier and its corresponding output signal

The output of a bridge rectifier is given as:

V_p = peak value of the AC voltage being rectified

$$V_{p.out} = V_{p.sec} - 2V$$

(3.1)

Where $V_{p,out}$ = peak output voltage

$V_{p,sec}$ = peak of the secondary voltage

$$V_{p,sec} = V_m \sqrt{2}$$

V_m = maximum input voltage

V_d = diode voltage drop (0.7V)

From the parameters given above, it can be deduced that;

$$V_{p,out} = V_m \sqrt{2} - 2 \times 0.7 \quad (3.2)$$

Recall that the output of the transformer is 12Volts,

This implies that $V_{p,out} = 12\sqrt{2} - 2 \times 0.7 = 15.571$ Volts

Rectifier diodes are rated by the maximum current they can pass and the maximum RMS voltage they can withstand. IN5392 rectifier diode is used for this project.

3.8.3.3 Filters

Full wave rectified voltage is filtered by a capacitor. Electrolytic capacitors are used as a ripple filter in a power supply circuit. They have polarity; that is to say they have positive and negative electrodes. It is therefore important to note the particular way they are connected. When using electrolytic capacitor one must pay attention to the maximum voltage, which can be used. This is the breakdown voltage. The breakdown voltage is the voltage that when exceeded will cause the dielectric (insulator) inside the capacitor to breakdown and conduct. Electrolytic capacitor which is connected in parallel to the output of the rectifier to perform smoothing; this reduces the ripple, smoothing is not perfect due to the capacitor voltage falls a little as it discharges given a small ripple voltage. The output of a filter capacitor is as shown in Fig. 3.7;

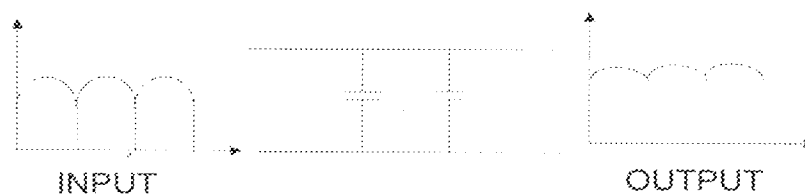


Fig. 3.7: diagram showing input and output signal through a capacitor

One of the important ratings of a power circuit is the ripple factor.

Ripple factor is defined as:

$$r_f = \frac{V_{rip}}{V_{dc}} \times 100\% \quad (3.3)$$

So ripple voltage can be calculated in terms of the circuit parameters shown below:

$$V_{rip} = \frac{I_{dc}}{2fC} \quad (3.4)$$

Where I_{dc} = load current in Ampere

f = frequency in Hertz

C = Capacitor value in farad

From ripple factor equation

$$V_{rip} = r_f \times V_{dc} = \frac{I_{dc}}{2fC} \quad (3.5)$$

By making C the subject of the formular;

$$C = \frac{I_{dc}}{2frfV_{dc}} \quad (3.6)$$

For most electronics circuit a ripple factor of 10% of supply is satisfactory;

$$r_f = 10\%$$

$$\frac{V_{rip}}{V_{dc}} = 0.1$$

$$V_{rip} = 0.1V_{dc}$$

From the ripple diagram

$$V_{dc} = V_m - \frac{V_{rip}}{2} \quad (3.7)$$

Comparing the above equations, it implied that;

$$V_{ac} = V_m / 1.05 \quad (3.8)$$

$$\text{Thus, } C = \frac{I_{ac}}{2f \times 0.1 \times V_m / 1.05}$$

$$C = \frac{5I_{ac}}{fV_m} \quad (3.9)$$

This equation therefore gives the required value for the smoothening capacitor. A larger capacitor will give fewer ripples.

For this circuit each part is expected to be fed with a current of approximately 1Amps and the supply voltage is 15.571Volts.

3.8.3.4 Voltage Regulation

After filtering the DC voltage there are still some AC variation which is called the ripple voltage, this along with the DC value. The smaller the AC variations with respect to the DC level, the better circuit operation. Voltage regulator is a device that receives variable inputs and provides a fixed voltage value. Voltage regulators are available in integrated circuit packages with fixed or variable output voltages. A 5Volt (7805IC) voltage regulator was used in the case of my design.

3.9 SYSTEM CONTROLLER MODULE

The system controller is an AT89C52 with the following characteristics: It is a low power, high performance 40-pin DIP, 8 bit microcontroller with 4Kilobytes of in-system reprogrammable flash memory, 128 bytes of SRAM and 32 programmable I/O lines. It also has a fully static operation of 0Hz to 24MHz. The diagram and pin layout of the AT89C52 is shown in Fig. 3.8 and Fig. 3.9 respectively;

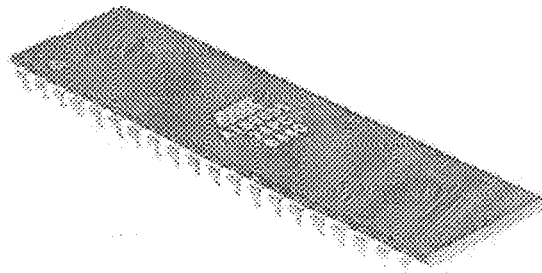


Fig. 3.8: Diagram of the AT89C52 Microcontroller

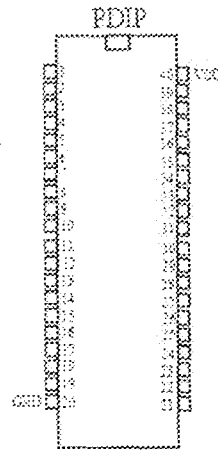


Fig. 3.9: Pin layout of the AT89C52 Microcontroller

Table 3.2 shows the pin description of the AT89C52 microcontroller;

Table 3.2: Pin description of the AT89C52

PIN	DESCRIPTION
1-8	P1.0-P1.7, Port 1
9	RST- Reset
10-17	P3.0-P3.7, Port 3
18	XTAL2-Crystal
19	XTAL1-Crystal
20	GND-Ground
21-28	P2.0-P2.7, Port 2
29	PSEN-Program Store Enable
30	ALE-Address Latch Enable
32-39	P0.7-P0.1, Port 0
40	Vcc-Positive Power Supply

3.1.0 VISUAL DISPLAY UNIT

The visual unit used was a 16-character-by-2-line dot matrix alphanumeric LCD.

This is shown in fig. 3.10;

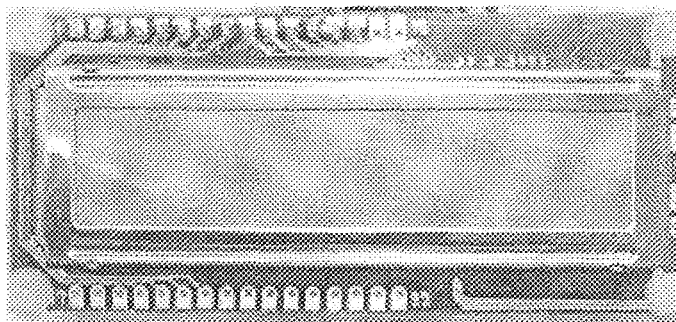


Fig. 3.10: Diagram of the 16X2 LCD Display

3.1.1.0 LCD Interfacing with System Controller

The LCD Character standard requires 3 control lines as well as either 4 or 8 I/O lines for the data bus. If the LCD operates in the 4-bit data bus mode, this requires a total of 7 data lines (3 control lines plus the 4 lines for the data bus). However, for this project, the 8-bit data bus is used and the LCD will require a total of 11 data lines (3 control lines plus the 8 lines for the data bus). This 8-bit mode realizes the desired operational

functionalities with the least software overhead. The three control lines are referred to as EN, RS, and RW.

The EN line is called "Enable". This control line is used to tell the LCD that you are sending it data. To send data to the LCD, your program should make sure this line is low (0) and then set the other two control lines and/or put data on the data bus.

The RS line is the "Register Select" line. When RS is low (0), the data is to be treated as a command or special instruction (such as clear screen, position cursor, etc.). When RS is high (1), the data being sent is text data which should be displayed on the screen. For example, to display the letter "T" on the screen you would set RS high.

The RW line is the "Read/Write" control line. When RW is low (0), the information on the data bus is being written to the LCD. When RW is high (1), the program is effectively querying (or reading) the LCD. Only one instruction ("Get LCD status") is a read command. All others are write commands, so RW will almost always be low.

Table 3.3 shows LCD Pins and their functions;

Table 3.3: LCD Pins and Their Functions

PIN	NAME	FUNCTION
1	V _{ss}	Ground Voltage
2	V _{cc}	+5V
3	V _{ce}	Contrast Voltage
4	RS	Register select 0 = write mode 1 = read mode
5	R/W	Read/Write, to choose read or write mode 0 = write mode 1 = read mode
6	E	Enable 0 = start latch data to LCD character 1 = disable
7	DB0	LSB
8	DB1	-
9	DB2	-
10	DB3	-
11	DB4	-
12	DB5	-
13	DB6	-
14	DB7	MSB
15	BPL	Black Plane Light
16	GND	Ground Voltage

The display was interfaced to Port 0 (P0) of the microcontroller with P2.7 and P2.6 implementing the RS (Register Select) and EN (Enable) functions. Since the display was not read back during the course of system operation, read/write was made permanently low.

From reset, instructions are written to the LCD using the specified set of routines outlined in the system controller subsection, and data likewise. Backlights are provided on the display for night use.

CHAPTER FOUR

TESTS, RESULTS AND DISCUSSION

The purpose of this project is to automate the verification of a student's identity before entry into an examination hall.

Upon completion of the construction, the workability of the biometric application and the door module was confirmed by subjecting it to a series of test procedures. These procedures helped in the test of each of the units. This chapter gives an overview of various test procedures. Testing of individual blocks was conducted in order to aid the debugging of system errors at individual unit level.

4.1 TESTING OF VARIOUS UNITS

4.1.1 The Software Module

The code for the implementation of the software module was written using Netbeans IDE (Integrated development Environment). Under proper operating conditions, the application is meant to connect with a remote central database to compare and fetch the various data. For the purpose of demonstration, another application was created using the Netbeans IDE (Integrated development Environment) for enrollment of some data before testing with the biometric application. That is not meant to be the work of the biometric application. The biometric application is meant to connect with pre-stored data in a database somewhere.

The code for the options and menus in the biometric application was written and tested independently.

The software module for the biometric application was developed from the flow chart shown in fig. 3.1. The third party API's (Application Programming Interface) used in this project are open source API's. Most of them are free except the grFinger library.

You need a license to get the full version of the library. The version of the library used is the trial version which is meant for this kind of purpose which is to show the possibility of biometric use in an application.

The programming approach used for the development of the project was strictly object oriented programming and the programming language used was Java.

The database used at the back end for storage of various data was mysql. The fingerprint sample stored in the database for the purpose of comparison was stored in binary form. Sql queries were written to enable communication with the database from the application.

4.1.2 The Parallel Port

Upon authentication of an individual's identity, the external circuit which is the door module is supposed to receive an active high signal at its input. An active low signal was sent from the application because an inverter (CD4049) interfaces between the application and the external circuit (door module).

During testing of the voltage output at the parallel port, the signal sent was not received at the port. After deeply studying the specification of both the parallel port and the API (Application Programming Interface) used for communication with the ports, I discovered that some pins of the parallel port were meant to receive some signal levels before an output could be received through the data pins of the parallel port. It wasn't explicitly stated hence the difficulty in initially finding out the problem. After connecting some particular pins to the appropriate signal level, the sent signal was received.

4.1.3 Microcontroller

The Microcontroller block, possessing so many routines, was tested using the LCD display. Captions were placed at the various execution points, so as control was passed

from one routine to the other, care was taken to ensure that the appropriate captions were indicated, thus verifying the correct operation of the microcontroller.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

This project exposed the student to various aspects of programming application software, hardware and electronics.

The Project achieved its set goal. It showed the possibility of the use of biometrics in automating verification of candidate's identity before entry into an examination hall. The hardware built (door module) was a prototype which simulates the opening and closing of a real door.

5.1 RECOMMENDATIONS FOR FURTHER WORK

For further work on this project, I recommend that the time for the opening and closing of the door should be an option that should be set from the application's interface. The application should also explore the use of other forms of biometrics aside fingerprint so that an individual could have options. Also in cases where an individual is deformed, his or her identity should still be verifiable by means of other forms of biometrics.

REFERENCES

- [1] <http://www.grialebiometrics.com/page/en-us/book/understanding-biometrics> (accessed on 28th February 2009)
- [2] <http://www.hardwaresecrets.com/article/233/2> (accessed on 28th February 2009)
- [3] http://www.beyondlogic.org/parallel_ect.php (accessed on 28th Feb 2009)
- [4] http://www.electricworks.com/serial_ect.php(accessed on 30th march 2009)
- [5] <http://En.wikipedia.org/wiki/Biometrics>(accessed on 26th may 2009)
- [6] <http://www.britanica.org/Biometrics>(accessed on 26th may 2009)

APPENDIX

Programme code for Software module of the Biometric Application

```
/*
 * FormMain.java
 *
 * Created on Aug 16, 2009, 7:06:50 AM
 */

package biometricapplication;
import java.awt.image.ImageProducer;
import java.awt.Image;
/**
 *
 * @author Benjay
 */
public class FormMain extends javax.swing.JFrame {
    private Util util ;
    public Image image;
    FormOptions pane = null;
    /** Creates new form FormMain */
    public FormMain(Util util) {
        this.util = util;
        initComponents();

    }
    public void showImage(ImageProducer producer) {
        image = fingerPrintPanel.createImage(producer);

        fingerPrintPanel.getGraphics().drawImage(image,0,0,fingerPrintPanel.getWidth(),fingerPrintPanel
        getHeight(),null);
    }
    public void writeLog(String text) {
        jTextArea1.append(text + "\n");

        Runnable autoscroll = new Runnable() {
            public void run() {
                javax.swing.JScrollBar vbar = jScrollPane1.getVerticalScrollBar();
                vbar.setValue(vbar.getMaximum());
            }
        };
        javax.swing.SwingUtilities.invokeLater(autoscroll);
    }
    public void enableTemplate() {
        // jButton.setEnabled(true);
        jButton1.setEnabled(true);
        jButton2.setEnabled(true);
    }
    /** This method is called from within the constructor to
     * initialize the form.
     * WARNING: Do NOT modify this code. The content of this method is
     * always regenerated by the Form Editor.
     */
    @SuppressWarnings("unchecked")
    // <editor-fold defaultstate="collapsed" desc="Generated Code"> //GEN-BEGIN initComponents
```

```

private void initComponents() {

    jButton4 = new javax.swing.JButton();
    jPanel9 = new javax.swing.JPanel();
    jLabel11 = new javax.swing.JLabel();
    jPanel11 = new javax.swing.JPanel();
    jOutlookBar1 = new com.I2fprod.common.swing.JOutlookBar();
    jPanel13 = new javax.swing.JPanel();
    jButton1 = new javax.swing.JButton();
    jPanel2 = new javax.swing.JPanel();
    jButton2 = new javax.swing.JButton();
    jPanel4 = new javax.swing.JPanel();
    jButton3 = new javax.swing.JButton();
    jPanel5 = new javax.swing.JPanel();
    jButton5 = new javax.swing.JButton();
    jPanel6 = new javax.swing.JPanel();
    jCheckBox1 = new javax.swing.JCheckBox();
    jCheckBox2 = new javax.swing.JCheckBox();
    jPanel10 = new javax.swing.JPanel();
    jScrollPane1 = new javax.swing.JScrollPane();
    jTextArea1 = new javax.swing.JTextArea();
    jPanel11 = new javax.swing.JPanel();
    picLabel = new javax.swing.JLabel();
    jPanel7 = new javax.swing.JPanel();
    lblLbl = new javax.swing.JLabel();
    deptLbl = new javax.swing.JLabel();
    skoolLbl = new javax.swing.JLabel();
    nameLbl = new javax.swing.JLabel();
    deptLbl1 = new javax.swing.JLabel();
    fingerpanel = new javax.swing.JPanel();
    fingerPrintPanel = fingerPrintPanel = new javax.swing.JPanel() {
        public void paint(java.awt.Graphics gg) {
            if(image != null) {
                gg.drawImage(image,0,0, fingerPrintPanel.getHeight(), fingerPrintPanel.getWidth(), null);
            }
        }
    };
    jPanel8 = new javax.swing.JPanel();
    deptRst = new javax.swing.JLabel();
    levLRst = new javax.swing.JLabel();
    nameRst = new javax.swing.JLabel();
    skoolRst = new javax.swing.JLabel();
    levLRst1 = new javax.swing.JLabel();
    jMenuBar1 = new javax.swing.JMenuBar();
    jMenu1 = new javax.swing.JMenu();
    jMenuItem1 = new javax.swing.JMenuItem();
    jMenuItem2 = new javax.swing.JMenuItem();
    jMenu3 = new javax.swing.JMenu();
    jMenu2 = new javax.swing.JMenu();
    jMenuItem4 = new javax.swing.JMenuItem();
    jMenuItem3 = new javax.swing.JMenuItem();

    jButton4.setText("jButton4");

    javax.swing.GroupLayout jPanel9Layout = new javax.swing.GroupLayout(jPanel9);

```