Sudan University of Science and Technology

College of Engineering

Electronics Engineering Department

Implementation of Electronic Voting System Using Fingerprint Recognition Technique

A Research Submitted In Partial fulfillment for the Requirements of the Degree of B.Sc. (Honors) in Electronics Engineering

Prepared By:

1. Areej Abdallah Ebrahim Mohammed
2. Ekram Abdallah Abdalrahman Osman
3. Zeinab Elnazeir Mohammed Abdelraheim

Supervised By:

Dr. Ahmed Abdallah Mohammed Ali

October 2016

الآيـــــــــة

قـال تعالـــى :

" وَلَا تقُولَنَ لِشَيءٍ إنِي فـَاعِـلٌ ذَلِكَ غـَدَاً (23) إلآ أن يَشـَآءَ اللهُ وَ اذكُر رَبـَكَ إذَا نَسِيـتَ وَقـُل عـَسَى أن يَهـدِيـنِ رَبَي لِأقـرَبَ مِن هـَذا رَشـــَدَاً(24) " صَدَقَ اللهُ العَظِيم

الكهف

Dedication

To our parents, Brothers, Sisters, and Teachers we present this work.

To those who stands with us by their efforts and time waiting for nothing to return.

ACKNOWLEDGEMENT

Thanks to Allah for his mercy and help without which we could not complete this work.

We express our deepest thanks and gratitude to our supervisor Dr. Ahmed Abdallah Mohammed Ali, who stands beside us by his advices, time, efforts and support to bring out this research.

Our thanks and deep gratitude to our families for encouragement and support during our study period, and also to all those who contributed to this work and encourage us to successfully finish this study.

ABSTRACT

Objective of voting to allow voter to cast his/her votes fairly, efficiently and accurately. This project deals with the design and implementing of an electronic voting system using fingerprint recognition. The aim is to provide security, accuracy and to avoid illegal voting. The proposed system allows voter to scan his fingerprint, then compares it with the pre-saved fingerprints in the database. After the verification is done, voter is allowed to cast his/her vote through a keypad, and the system communicates with the voter through LCD. The casted vote is updated immediately making the system fast and unable to fraud the results which will be viewed on the LCD at the end of voting process.

المستخلص

الهدف من التصويت هو السماح للناخب ان يدلي بصوته بعدل وكفاءة ودقة. هذا المشروع يختص بتصميم و تنفيذ نظام تصويت إلكتروني باستخدام التعرف ببصمة الإصبع. الهدف هوان يكون النظام آمناً و دقيقاً و لتجنب التصويت غير الشرعي. النظام المقترح يسمح للناخب بإدخال بصمته ثم يقوم بمقارنتها مع البصمات المحفوظة مسبقا في قاعدة البيانات. بعد اكتمال عملية التحقق من البصمة, يسمح للناخب بالإدلاء بصوته باستخدام لوحة مفاتيح, وسوف يقوم النظام بالتواصل مع الناخب عبر شاشة عرض. الصوت الذي ادلي يحسب فوراً ما يجعل النظام سريعاً وغير قابل لأن تزور نتائجه, النتائج يمكن أن يتم عرضها على شاشة العرض بعد انتهاء عملية التصويت.

TABLE OF CONTENTS

APPENDIX

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

CHAPTER ONE

INTRODUCTION

1.1 Preface

1.2 Problem statement

1.3 Proposed solution

1.4 Aim

1.5 Research Outlines

1.1 Preface :-

The objective of voting is to allow voters to exercise their right to express their choices regarding specific issues, pieces of legislation, citizen initiatives, constitutional amendments, recalls and/or to choose their government and political representatives. A lot of money has been spent on this to make sure that the elections are rampage free. But, nowadays it has become very usual for some forces to indulge in rigging, which may eventually lead to a result contrary to the actual verdict given by the people. In order to provide inexpensive solutions to this problem, this project will be implemented with electronic voting system using fingerprint recognition. Electronic voting is completing the voting process electronically, without the use of paper and ballot boxes. Voting process includes stalls closed to vote equipped with electronic devices, software, peripherals, processing systems, equipment, tools and screens, networks and means of communication ... etc., and sometimes includes systems, smart cards , or biometric cognitive systems (a standard vital systems that rely on measuring the physical properties that are unique to each person is different from the other by such as fingerprint, retina and DNA)[1]. Fingerprint matching is one of the most popular and reliable biometric techniques used in automatic personal identification. It is used to ensure the security to avoid fake, repeated voting, etc. It also enhances the accuracy and speed of the process. The system uses thumb impression for voter identification as we know that the thumb impression of every human being has a unique pattern. Thus it would have an edge over the present day voting systems.

1.2 problem statement :-

The problem with the existing manual voting system includes the following:

- **Expensive and Time consuming:** The process of collecting data and entering this data into the database takes too much time and is expensive to conduct, for example, time and money is spent in printing data capture forms, in preparing registration stations together with human resources, and there after advertising the days set for registration process including sensitizing voters on the need for registration, as well as time spent on entering this data to the database.
- **Too much paper work:** The process involves too much paper work and paper storage which is difficult as papers become bulky with the population size.
- **Errors during data entry:** Errors are part of all human beings; it is very unlikely for humans to be 100 percent efficient in data entry.
- **Loss of registration forms:** Some times, registration forms get lost after being filled in with voters' details, in most cases these are difficult to follow-up and therefore many remain unregistered even though they are voting age nationals and interested in exercising their right to vote.
- **Short time provided to view the voter register:** This is a very big problem since not all people have free time during the given short period of time to check and update the voter register.

- **Can be fooled:** low level of security; one person may cast his vote several times.
- **Susceptible to fraud.**

1.3 Proposed solution :-

We represent the Electronic voting machine using fingerprint authentication as a solution to the drawbacks of the traditional system. **First:** using an electronic system in voting, counting votes and representing the results is much better in saving time, effort and money .In addition, it matches the requirements in traditional voting process such as:

- Fairness: No person can learn the voting outcomes before the tally.
- Eligibility: Only eligible voters are allowed to cast their vote.
- Uniqueness: No voter is allowed to cast their vote more than once.
- Privacy: No person can access the information about the voters vote.
- Accuracy: All the valid votes should be counted correctly.
- Efficiency: The counting of votes can be performed within a minimum amount of time.

Second: The use of fingerprint authentication can increase the level of security and secrecy that no one can vote twice or manipulate the results.

1.4 Aim and Objectives:-

The main aim of the project is to design and implement an electronic voting machine using fingerprint recognition technology to provide more security in authentication of a candidate contesting in elections by providing a unique identity to every user using the

fingerprint technology provided if we maintain the fingerprints of all the voters in a database.

1.5 Research Outlines :-

In this research has been organized into five chapters as shown below:

Chapter tow: provides literature review of electronic voting systems with the fingerprint technique projects. Also includes fingerprint recognition, patterns, readers and algorithms.

Chapter three: describes system design, the methodology that followed to implement this project, used tools and analysis of the system flow.

Chapter four: describes the software implementation of the system.

Finally the research has been concluded in Chapter five along with recommendations and future work of this project.

CHAPTER TWO

THEORETICAL PART

Chapter two

Theoretical part

2.1 Background

2.2 Literature Review

2.3 Fingerprint Recognition

2.1 Background :-

Voting is a method for a group such as a meeting or an electorate to make a decision or express an opinion-often following discussions, debates, or election campaigns. It is often found in democracies and republics [2], figure 2-1 shows the traditional voting process.

Past experience of electoral process enforced us to focus on the use of latest technology in electronic voting process. The current voting mechanism has many security problems, and it is very difficult to prove even simple security aspects about them. A voting system that can be demonstrated correct has many considerations. Some of the major concerns for a government regarding electronic voting systems are to expand election activities and to minimize the election expenses. Still there is some opportunity of work in electronic voting system in terms of authenticity of voters and to protect the electronic voting machine from offenders.

Today, identification can be achieved in a few seconds with reasonable accuracy using fingerprint scanners, Another important reason we proposed fingerprint scanners to be used is to provide a quick, easy, efficient, and secure measure through which, an individual with the proper access privileges can authenticate. The fingerprint of a voter for example, is stored in a database that the scanner queries every time it is used searching for a match. The size of these devices is another reason they have become so mainstream recently. For all of that, the use of automated fingerprint identification systems that record, store, search, match and identify finger prints is rapidly expanding. A fingerprint print

identification system can be integrated with a microcontroller and other peripherals to form an embedded system which is a comprehensive electronic voting machine with fingerprint print identification system[3].

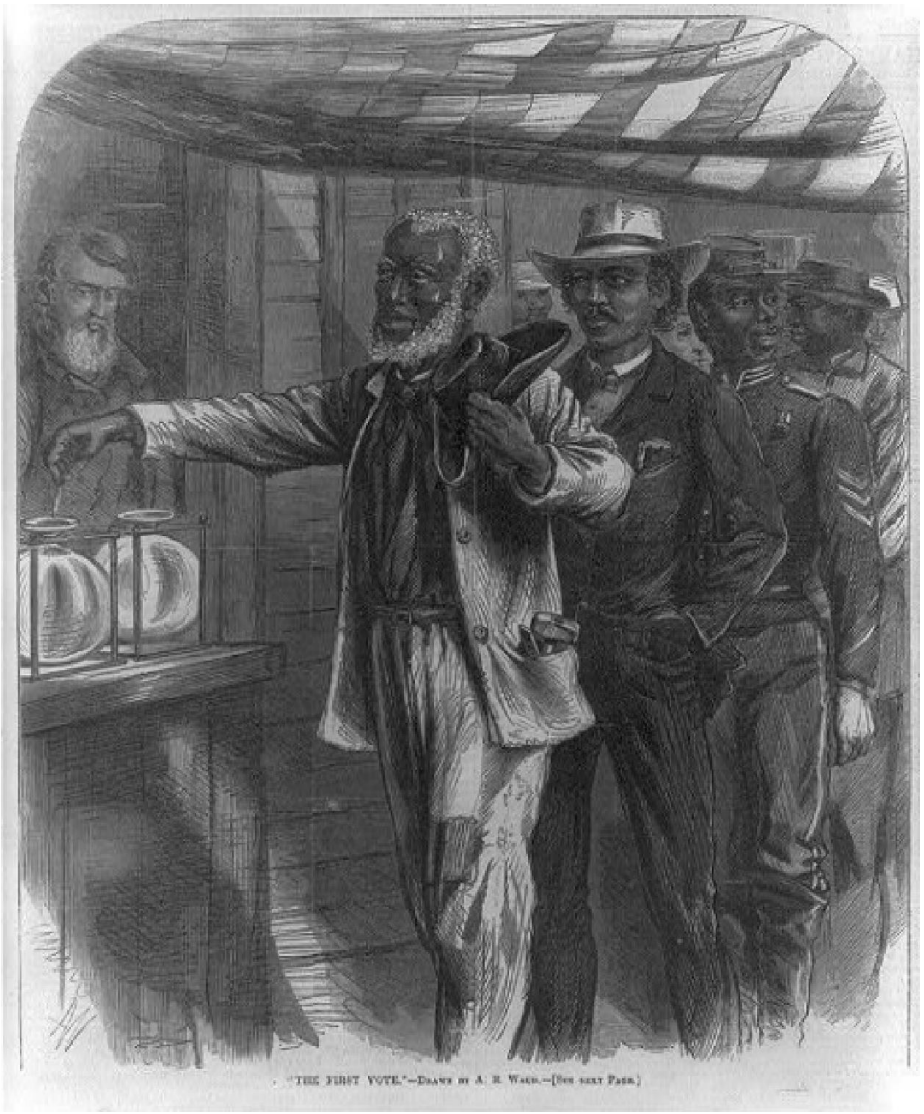


Figure 2-1: (The first vote) A.R. Waud, Wood engraving 1867

2.2 Literature Review :-

F.Hazzaa and S.Kadry, in 2012[4], developed Web-based Voting System using Fingerprint Recognition, the system that they designed suggests an election to choose the president of university, there are 4 candidate for this position, and there are 40 voter register in this election, the admin sponsors for register the voters, each voter can register after attending to the admin, give his name, ID, and scan his fingerprint, then the admin submit this information to store in database, or the admin can get all voter's information with their fingerprints from official office. On the day of election the voters can participate by open the website of election from anywhere and cast their votes. When the voter want to vote, he will asked by the website to identified himself by his fingerprint, he will scan his finger (the same finger who submit before) and submit it to the system, then the system will return the decision for allowed or not allowed him to vote, voter is allowed to vote only for one time, the system can compute and display the results of each candidate. The software is implemented completely as a .net managed code in C#. The system has provided an efficient way to cast votes, free of fraud, and make the system more trustable, economic and fast, they used Minutiae-based fingerprint identification and matching with high accuracy.

S.Baig et.al, in 2011[5], developed Electronic Voting System using Fingerprint Recognition, they have devised a user interface that includes an LCD and a Keypad interfaced with microcontroller in serial communication with a computer, a fingerprint scanner is also interfaced with the computer through USB port. The scanned fingerprint image is

transferred to the computer and the image is further processed for verification and authentication using MATLAB. A database containing the information of the voters and the candidates will be updated accordingly, as the users cast their votes. Therefore, system will facilitate automatic counting of votes against a candidate. The system has provided an efficient way to cast votes, free of fraud. They used Gabor Filter based fingerprint identification and matching with high accuracy.

D.Kumar and T.Begum, in 2011[2], successfully implemented and evaluated a PC based electronic voting system; they have conducted the pilot election using a personal computer with four fingerprint scanners for selecting class representative. For that, they have created the database which consists of the fingerprint of the computer science department students with the number of 80 (45 males and 35 females). The database is created based on the digital personal scanner. This primary process is done during the registration process. After that, the chosen finger can be live scan. The fingerprint template is then processed and extracted. It will subsequently match the scanned fingerprint against the stored template. Upon verification, they will have the access to vote for their desired candidates. Mismatched fingerprint certainly would indicate denial from the access. During the voting, the voter first places his thumb on the touch sensitive region. If the fingerprint matches he is allowed to vote. In case the print is not stored before, a single beep is given, so the person cannot vote, or if the same person votes again, the system should give a double beep, so that the security can be alerted. The system is programmed to recognize a fingerprint twice, but to give a beep for more than once. After the completion of voting, one can know

the status of the nominees by clicking the count button. The results were significant and more comparable. It proved the fact that the fingerprint image enhancement step will certainly improve the verification performance of the fingerprint based recognition system. The best enhancement technique Gabor is used to enhance the fingerprints for electronic voting.

S.Kumar and M.Singh, in 2013[3], developed a simple, small and easy to use voting machine based on fingerprint recognition with the objective of eliminating bogus voting and vote repetition, less election expenditure, more transparency and fast results. The machine comprises of a key pad, graphical LCD, microcontroller (Arduin-Mega 2560) and a fingerprint module. First, voter should inter the password, then he scans his fingerprint which is compared to a database then the LCD will display the list of candidates that voter should choose one of them. The result is shown immediately and the machine waits for another voter.

A.Nalluri, B.Teja and A.Balakrishna, in 2014[6], developed a voting system project based on fingerprint recognition to improve the security performance in the voting machine. In the project, RFID (Radio Frequency Identification) is used as vote ID card, each user is provided a voter's ID in the form of RFID Tag. The hardware design has a Finger print scanning sensor which is used to compare the finger print of the user with the pre-stored finger print of the user. During voting, both the finger prints are checked for matching and if it does not match, then an alert is given using buzzer. Keypad is used for selecting the voting preferences. LCD is used to display the corresponding data for each key to the user. Thus, illegal voting cannot be done since finger print is unique for each person. The voting process is carried out only if the

finger print matches with the stored value. The use of fingerprint improves the security performance and avoids forgery vote because naturally one human finger print is different from other humans.

J.Kumari, S.Pal, Arthi R and P.Michael, in 2014[7], developed an Electronic Voting Machine using ZIGBEE communication system for sorting out the wired electronic voting problems, fingerprint technique is also used to design a secure electronic voting system. The design is based on the (ATMEGA328p) microcontroller, RS232 cable which is used for interfacing between ZIGBEE and the microcontroller, LCD (16X2) for displaying the instruction, fingerprint sensor for scanning voter's fingerprint before voting, ZIGBEE transmitter, ZIGBEE receive, security alarm and visual basic for creating display page in computer. Simulation is done using Proteus software, coding and the .hex file is generated for microcontroller using Arduino software. Each voter can vote only once thus protecting the identity of the voter in making the process unbiased and fair. Database comprising details of all voters with their personal details and fingerprint are stored in microcontroller for comparing and verification during polling. This design of electronic voting machine will save considerable amount of time and manpower. Thus, the proposed system is more reliable and fast as compared to existing electronic voting system. At the end of the polling, just by pressing a button the results can be obtained. The system afforded additional security by allowing voter to vote only once by imparting unique identification.

2.3 Fingerprint Recognition :-

Finger print recognition refers to the automated method of identifying or confirming the identity of an individual based on the comparison of two finger prints. Fingerprint recognition is one of the most well-known biometrics, and it is by far the most used biometric solution for authentication on computerized systems. The reasons for fingerprint recognition being so popular are the ease of acquisition, established use and acceptance when compared to other biometrics, and the fact that there are numerous (ten) sources of this biometric on each individual[8].

2.3.1 Fingerprint Patterns :-

The three basic patterns of fingerprint ridges are the arch, the loop, and the whorl as shown in figure 2-2.

a) **Arch:** an arch is a pattern where the ridge enters one side of the finger, then rises in the center forming an arch, and exits on the other side of the finger, 5% of people have his type of fingerprint.
b) **Loop:** with a loop the ridge enters one side of the finger, then forms a curve, and exits on the same side of the finger from which it entered. Loops are the most common pattern in fingerprints, 60% of people have his type of fingerprint.
c) **Whorl:** a whorl is the pattern you have when ridges form circularly around a central point, 35% of people have his type of fingerprint[8].

Figure 2-2: The six fingerprint major patterns: (a) arch, (b) tented arch, (c) left loop, (d) right loop, (e)whorl, and (f) twin-loop.

2.3.2 Fingerprint Readers:-

A fingerprint reader's job is to take the place of a human analyst by collecting a print sample and comparing it to other samples on record. There exist four main types of fingerprint readers hardware:

Optical Readers:

Those are the most common type of fingerprint readers; the type of sensor in an optical reader is a digital camera that acquires a visual image of the fingerprint. Advantages are that optical readers start at very cheap prices, disadvantages are that readings are impacted by dirty or marked fingers, and this type of fingerprint reader is easier to fool than others[9].

Capacitive Readers:

Also referred to as CMOS readers, they do not read the fingerprint using light. Instead a CMOS reader uses capacitors and thus electrical current to form an image of the fingerprint. CMOS readers are more expensive than optical readers, although they still come relatively cheap, an important advantage of capacitive readers over optical readers is that a capacitive reader requires a real fingerprint shape rather than only a visual image, this makes CMOS readers harder to trick[9].

Ultrasound Readers:

Ultrasonic readers are the most recent type of fingerprint readers, they use high frequency sound waves to penetrate the epidermal (outer) layer of the skin, and they read the fingerprint on the dermal skin layer, which eliminates the need for a clean, unscarred surface. All other types of fingerprint readers acquire an image of the outer surface, thus requiring hands to be cleaned and free of scars before read-out. This type of fingerprint reader is far more expensive than the first two, however due to their accuracy and the fact that they are difficult to fool the ultra sound readers are already very popular[9].

Thermal Readers:

Sense on a contact surface, the difference of temperature in between finger print ridges and valleys. Thermal fingerprint readers have a number of disadvantages such as higher power consumption and a performance that depends on the environment temperature[9].

- Next to these four types, fingerprint readers are divided in between touch and swipe readers. A **swipe** reader has a small contact surface over which you swipe your fingerprint, this type usually used in smart phones; figure 2-3 shows a swipe fingerprint reader. On a **touch** reader you just have to press and release your finger; figure 2-4 shows a touch reader. In general touch readers are more easy to use, swipe readers require a bit of practice the first time the device is used[10].

Figure 2-3: Fingerprint swipe reader

Figure 2-4: Fingerprint touch reader

In practice, whatever the type of fingerprint reader used, there are factors that affect the quality of a fingerprint image:

1. Wetness or dryness of the skin.
2. Noise of the sensor.
3. Temporary or permanent cuts and bruises in the skin.
4. Variability in the pressure against the sensor.

Figure 2-5 shows fingerprint images with different quality.

Figure 2-5: Fingerprint images with different quality. From left to right: high, medium and low quality, respectively.

2.3.3 Fingerprint Matching Algorithms :

2.3.3.1 Pre-processing:

Pre-processing helped enhancing the quality of an image by filtering and removing unnecessary noises. The minutiae based algorithm only worked effectively in 8-bit gray scale fingerprint image. A reason was that an 8-bit gray fingerprint image was a fundamental base to convert the image to 1-bit image with value 0 for ridges and value 1 for furrows; as a result, the ridges were highlighted with black color while the furrows were highlighted with white color. This process partly

removed some noises in an image and helped enhance the edge detection. Furthermore, there are two more steps to improve the best quality for the input image: minutiae extraction and false minutiae removal. The minutiae extraction was carried out by applying ridge thinning algorithm which was to remove redundant pixels of ridges, as a result, the thinned ridges of the fingerprint image are marked with a unique ID so that further operation can be conducted. After the minutiae extraction step, the false minutiae removal was also necessary. The lack of the amount of ink and the cross link among the ridges could cause false minutiae that led to inaccuracy in fingerprint recognition process[11].

2.3.3.2 Pattern based (image based) algorithm:

Pattern based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a previously stored template and a candidate fingerprint this requires that the images can be aligned in the same orientation, to do this, the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The voter fingerprint image is graphically compared with the template to determine the degree to which they match[11].

2.3.4 Strengths and weaknesses of fingerprint recognition :

Finger-scan technology is the most widely deployed biometric technology, with a number of different vendors offering a wide range of solutions. Among the most remarkable strengths of fingerprint recognition, we can mention the following:

- Fingerprint recognition based systems are usually simple to use and install.
- It requires inexpensive equipment which usually have low power intake.
- A fingerprint pattern has individually distinctive composition and characteristic remains the same with time.
- Finger prints are largely universal. Only, of the 2% of human population cannot use finger prints due to skin damage or hereditary factors.
- Fingerprints are the most preferred biometric.
- One should not have to remember passwords, you simply swipe your finger on scanner and done it.
- Biometric fingerprint scanner presents a method to record an identity point which is very hard to be fake, making the technology incredibly secure.
- It is easy to use along with the high verification process speed and accuracy.
- Its maturity, providing a high level of recognition accuracy.

On the other hand, a number of weaknesses may in influence the effectiveness of fingerprint recognition in certain cases:

- Because fingerprint scanner only scans one section of a person's finger, it may susceptible to error.
- Many scanning system could be cheat employing artificial fingers or perhaps showing another person’s finger.
- Sometimes it may take many swipe of fingerprint to register.
- Fingerprints of people working in chemical sectors often affected.

- Cuts, marks transform fingerprints which often has negatively effect on performance.
- Small-area sensors embedded in portable devices may result in less information available from a fingerprint and/or little overlap between different acquisitions[8].

CHAPTER THREE

METHODOLOGY

Chapter Three

Methodology

3.1 Research Activities

3.2 Project Design

3.3 Hardware Implementation

3.1 Research Activities :-

In order to accomplish the desired fingerprint voting system, this project has gone through the following steps:

- **Step1 :**
  - ✓ Review the work that had been done in the electronic voting using fingerprint recognition.
  - ✓ Do an analysis requirement for a fingerprint recognition system.
- **Step2 :**
  - ✓ Design the system circuit.
  - ✓ Design the algorithm.
  - ✓ Implement the algorithm with Micro C PRO for AVR.
  - ✓ Do the hardwiring.
  - ✓ Integrate hardware with software.
- **Step3 :**
  - ✓ Test and troubleshoot.
  - ✓ Analyze the results.
- **Step4 :**
  - ✓ Write the research document.

3.2 Project Design :-

The implementation of the project design can be divided in two parts.

- ➢ Hardware implementation
- ➢ Software implementation

Hardware implementation deals in drawing the schematic on the plane paper according to the application, testing the schematic design over the breadboard using the various IC's to find if the design meets the objective, Then preparing the board and testing the designed hardware.

The software part deals in programming the microcontroller so that it can control the operation of the IC's used in the implementation.

The project design and principle are explained in this chapter using the block diagram and circuit diagram. The block diagram discusses about the required components of the design and working condition is explained using circuit diagram and system wiring diagram (schematic).

3.3 Hardware Implementation :-

This section briefly explains about the Hardware Implementation of the project. It discusses the design and working of the design with the help of block diagram and circuit diagram and explanation of circuit diagram in detail. It explains the features, serial communication, of ATMEGA16 microcontroller. It also explains the various modules used in this project.

3.3.1 Block Diagram :-

Figure 3-1 describes the block diagram of the system.

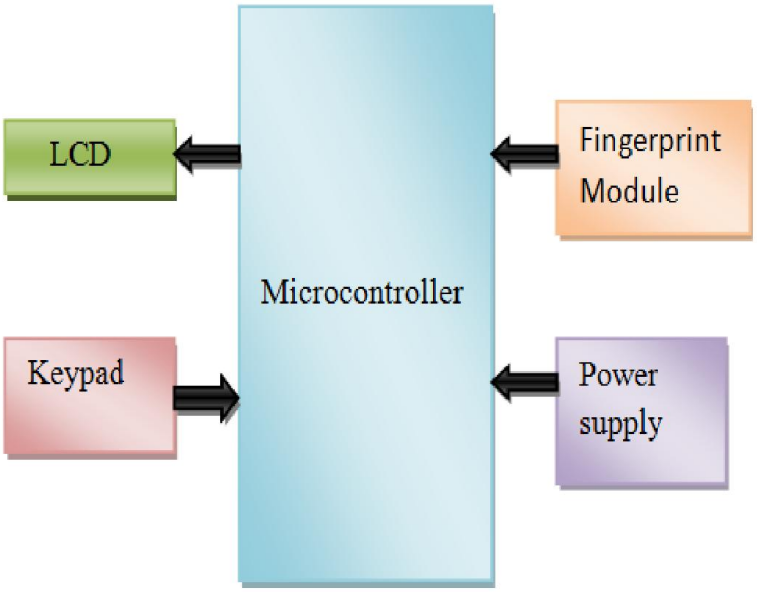


Figure 3-1: Block diagram of the system

3.3.2 System Components:

3.3.2.1 ATMEGA16 Microcontroller:

ATMEGA16 microcontroller is used for controlling. It controls LCD, keypad and fingerprint module by receiving input commands from keypad, controlling fingerprint module and sending commands to the LCD that display messages that direct the user to how to use the system properly. Figure 3-2 shows the ATMEGA16 microcontroller used in this project.

Figure 3-2 : Atmega16 microcontroller

3.3.2.2 Fingerprint Module R305:

Fingerprint module's processing, shown in figure 3-2 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.

Figure 3-3: R305 Fingerprint module

❖ **Features :**

- Power DC: 3.6V-6.0V
- Interface UART: (TTL logical level)/ USB 1.1
- Working current Typical: 100mA /Peak: 150mA
- Matching Mode 1:1 and 1:N.
- Baud rate: (9600*N)bps, N=1～12 (default N=6)
- Character file size: 256 byte.
- Image acquiring time:<0.5s
- Template size: 512 bytes
- Storage capacity: 256
- Security level :5 (1, 2, 3, 4, 5(highest))

❖ **Pin Description :**

It has six pins, their function description is shown on table 3-1 bellow.

Table 3-1: R305 pin description

Pin NO.	Name	Type	Function Description
1	Vin	In	Power input
2	TD	In	Data output. TTL logical level
3	RD	Out	Data output. TTL logical level
4	NC	-	Not connected
5	NC	-	Not connected
6	GND	-	Signal ground

3.3.2.3. LCD 16*2:

LCD stands for Liquid Crystal Display. LCD screen functions as an interface between the user and the microcontroller, which displays messages that facilitates the user to know when to register and when to vote, also whether their vote is valid or not and finally displays the results. Figure 3-4 shows the LCD used in this project.

Figure 3-4: LCD (16*2)

❖ **Features :**

- Type : Character.
- 16 characters * 2 lines.
- Display mode & backlight variation.
- 4-bit or 8-bit microcontroller interface.

❖ **Contrast Control:**

To have a clear view of the characters on the LCD, contrast should be adjusted. To adjust the contrast, the voltage should be varied. For this, a variable resistor is used which can behave like a variable voltage device. As the voltage of this variable resistor is varied, the contrast of the LCD can be adjusted.

3.3.2.4. Keypad (4*4):

Matrix keypads use a combination of four rows and four columns to provide button states to the host device, typically a microcontroller. They have an ultra-thin design, adhesive backing, excellent price and performance ratio; also they are easy to interface to any microcontroller. The keypad here is used to activate the controller for registration during enrollment and selecting the candidate while casting the vote. Figure 3-5 shows the keypad used in this project.

Figure 3-5: Keypad (4*4)

3.3.3 Connection of Circuit:

The voting machine R305 consists of six keys, two are not connected (4&5). Pin1 is connected to the power supply Vcc, pin 2(Tx) is connected to serial receive input of microcontroller which is nothing but PD.0 pin. Similarly pin 3(Rx) is connected to serial transmit pin of microcontroller PD.1. Finally pin 6 is connected to the ground. The display section uses port B of the microcontroller, only four of data pins in the LCD (DB–DB7) are connected to the microcontroller through PB.4–PB.7 respectively for more efficiency. The contrast of this LCD display is adjusted by changing the value of a resistor which is grounded at the other end. The keypad consists of 8 pins connected to the microcontroller through port A. For the microcontroller, pin 10 (Vcc) is connected to the power supply and pin 11 (GND) is connected to the

ground. Figure 3-6 shows how the components of the system are connected together.

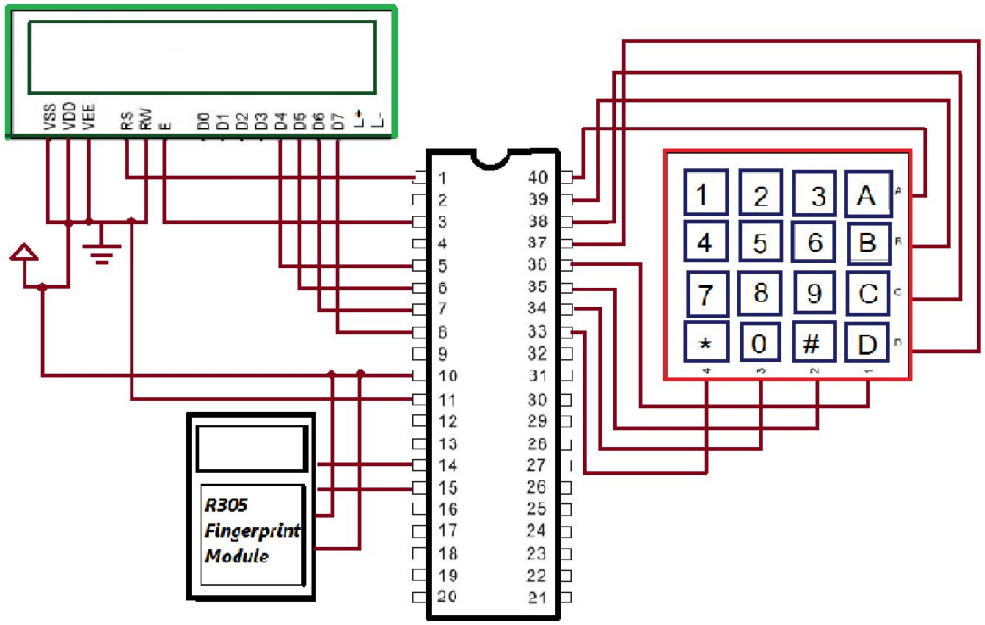


Figure 3-6: Circuit diagram

CHAPTER FOUR

SOFTWARE IMPLEMENTATION

Chapter Four

Software Implementation

4.1 Software Implementation

4.2 Algorithm

4.3 Process Flow

4.1 Software Implementation :-

The software programmed in ATmega16 is designed to communicate with fingerprint module and operate according the commands received from the keypad.

Micro C PRO for AVR :-

The Micro C PRO for AVR –shown in figure 3-7- is a powerful, feature-rich development tool for AVR microcontrollers. It is designed to provide the programmer with the easiest possible solution to developing applications for embedded systems, without compressing performance or control.

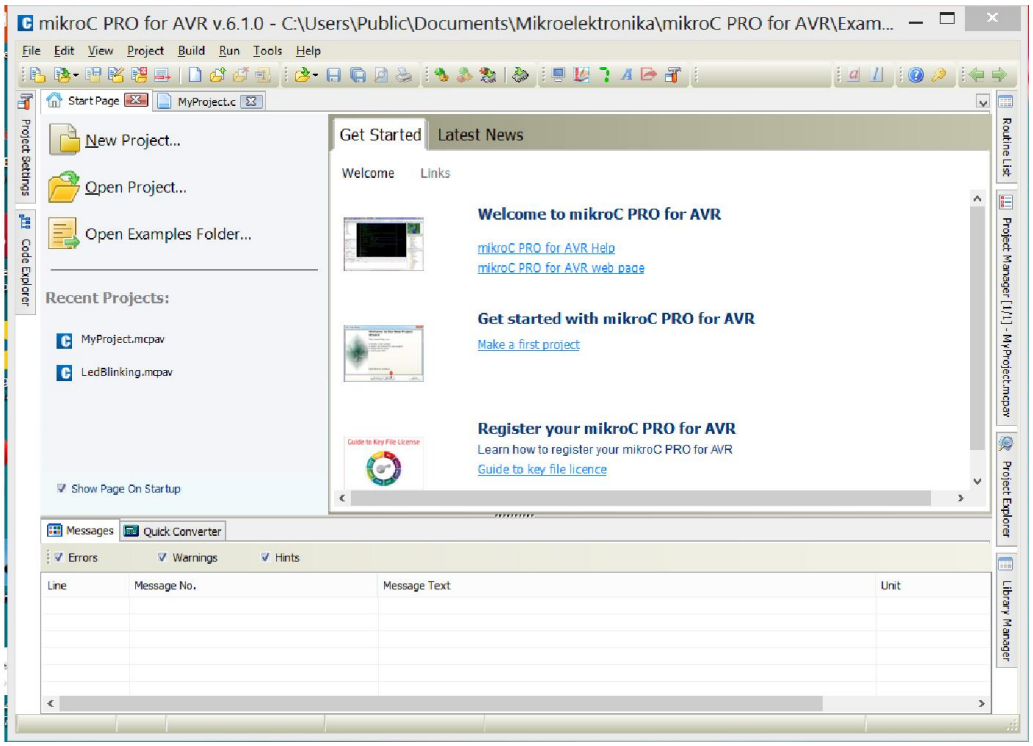


Figure 4-1: Micro C PRO for AVR

❖ **Features :**

Micro C PRO for AVR allows programmer to quickly develop and deploy complex applications:

- Write C source code using built-in Code Editor (code and parameter assistants, code folding, syntax highlighting, auto correct, code templates, and more).
- Use included micro C PRO for AVR libraries to dramatically speed up the development: data acquisition, memory, displays, conversions, communication, etc.
- Monitor program structure, variables, and functions in the Code Explorer.
- Generate commented, human readable assembly, and standard HEX compatible with all programs.
- Inspect program flow and debug executable logic with integrated software.
- Micro C PRO for AVR provides plenty of examples to expand, develop, and use as building bricks in projects.

4.2 Algorithm :-

The algorithm of code consist of three main functions, that will be called according to what process is needed wither to create the **database**, to **search** for a match or to show the **results**.

Database Function :-

This function is concerned with creating a database for the system. It sends a packet to the fingerprint module telling it to first let the voter scan his/her fingerprint, and then store the scanned fingerprint in the module flash memory.

Search Function :-

This function is concerned with searching for matching scanned fingerprint with the pre-saved database. It sends a packet to the fingerprint module telling it to first let the voter scan his/her fingerprint, and then search the database to find a match for the scanned fingerprint.

Results Function :-

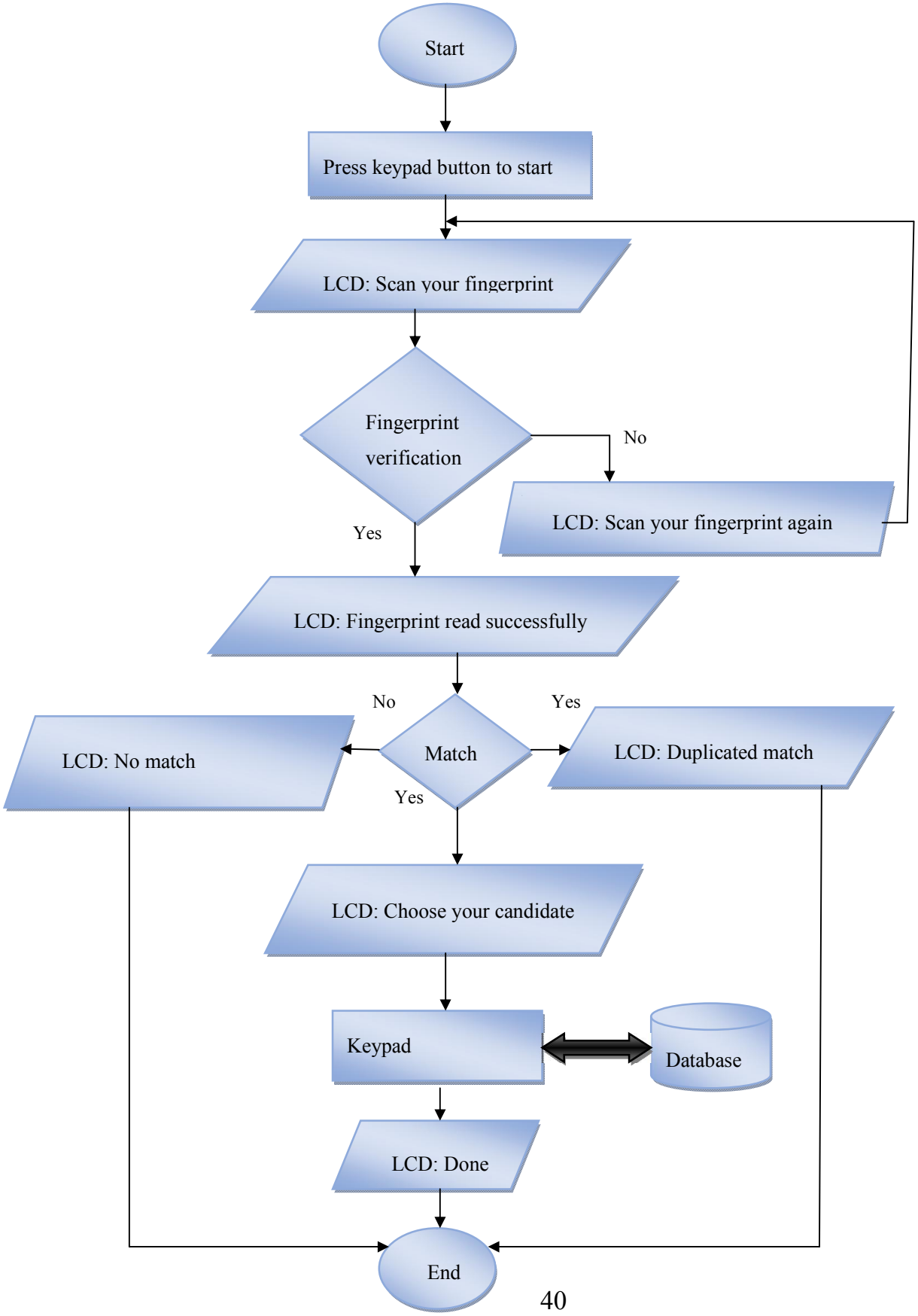
This function is concerned with calculating the voting process and viewing it on the LCD.

4.3 Process Flow :-

When a voter wants to cast his/her vote, first he must press the start button on the keypad, here the system displays a message tells the voter to scan his/her fingerprint, after scanning; the fingerprint module transfers the scanned fingerprint to the microcontroller, the latest compares it with the pre-saved database searching for a match, if the microcontroller didn't find a match; the system displays a message telling the voter that he/she is not allowed to vote. When the microcontroller finds a match; it can be one of two: **Case 1**a duplicated match, that means the voter has already casted his/her vote once and the system doesn't allow a voter to vote more than one time, here system displays a message clarifying the case. **Case 2**a first time match, which

indicates that this person didn't vote before, in this case system displays a message telling the voter to cast. The voter chooses his/her candidate by pressing the candidate's number on keypad, here the role of voter is finished.

After that the microcontroller updates the database so that if the voter tried to vote again the system will prevent him/her, and then counts the votes against candidates. The whole process is shown in the following flow chart.


Start
Press keypad button to start
LCD: Scan your fingerprint
Fingerprint verification
No
LCD: Scan your fingerprint again
Yes
LCD: Fingerprint read successfully
No
Yes
LCD: No match
Match
LCD: Duplicated match
Yes
LCD: Choose your candidate
Keypad
Database
LCD: Done
End

CHAPTER FIVE

CONCLUSION

Chapter Five

Conclusion

5.1 Conclusion

5.2 Future Work

5.1 Conclusion :-

This project can be used for voting since it overcome all the drawbacks of ordinary voting mechanism and provided additional security. Since fingerprint of every person is unique, thus this system reduced the chance of illegal personating votes. The system can be manufactured simply as well as cheap. It can be concluded that the design implemented in the project provided portability, flexibility and the data transmission is also done with low power consumption.

5.2 Future Work :-

It is very difficult to design ideal electronic voting system which can allow security and privacy on the high level with no compromise. Future enhancements can be concerned to design a system that connects the electronic voting machine with the computer using a wireless technique (ex. Wi-Fi) in order to provide additional services. Another modification is to introduce a networking mechanism to link all the voting machines with a central server, so the result on the server could be relayed on the network to various offices of the election conducting authority, thus the system will make the results available at any corner of the world in a matter of seconds.

REFERENCES :-

1. Agrawal, S., P. Majhi, and V. Yadav. *Fingerprint Recognition Based Electronic Voting Machine*. in *National Conference on Synergetic Trends in engineering and Technology (STET-2014) International Journal of Engineering and Technical Research ISSN*.

2. Kumar, D.A. and T.U.S. Begum, *A novel design of electronic voting system using fingerprint.* International Journal of Innovative Technology & Creative Engineering, 2011. **1**(1): p. 12-19.

3. Kumar, S. and M. Singh, *Design a secure electronic voting system using fingerprint technique.* IJCSI International Journal of Computer Science Issues, 2013. **10**(4): p. 1694-0814.

4. Hazzaa, F. and S. Kadry, *New system of E-voting using fingerprint.* International Journal of Emerging Technology and Advanced Engineering, 2012. **2**: p. 355-363.

5. Baig, S., et al., *Electronic Voting System Using Fingerprint Matching with Gabor Filter.* proc. IBCAST, 2011.

6. Nalluri, A., B.B. Teja, and A. Balakrishna. *RFID and Fingerprint Recognition based Electronic Voting System for Real Time Application*. in *International Journal of Engineering Development and Research*. 2014. IJEDR.

7. Kumari, J., et al., *ELECTRONIC VOTING MACHINE USING ZIGBEE.*

8. Fierrez, H.F., K. Kollreider, and J. Ortega-Garcia, *Fingerprint Recognition.*

9. Harris, T., *How fingerprint scanners work.* HowStuffWorks. com, 2002.

10. http://www.biometric-solution.com/devices/index.php?story=fingerprint_reader

11. http://en.m.wikipedia.org/wiki/Fingerprint_recognition.

APPENDIX

CODE

```
void database();

void search() ;

void result();

unsigned char control[13]=

{0xEF,0x01,0xFF,0xFF,0xFF,0xFF,0x01,0x00,0x04,0x17,0x01,0x00,0x1D
} ;

Unsigned char Gen_img[12]=

{0xEF,0x01,0xFF,0xFF,0xFF,0xFF,0x01,0x00,0x03,0x01,0x00,0x05} ;

unsigned char Img2Tz1[13]=

{0xEF,0x01,0xFF,0xFF,0xFF,0xFF,0x01,0x00,0x04,0x02,0x01,0x00,0x08
} ;

Unsigned char Img2Tz2[13]=

{0xEF,0x01,0xFF,0xFF,0xFF,0xFF,0x01,0x00,0x04,0x02,0x02,0x00,0x09
} ;

Unsigned char Reg_mod[12]=

{0xEF,0x01,0xFF,0xFF,0xFF,0xFF,0x01,0x00,0x03,0x05,0x00,0x09} ;

Unsigned char Store[13]=

{0xEF,0x01,0xFF,0xFF,0xFF,0xFF,0x01,0x00,0x06,0x06,0x01,0x00,0x05
} ;

Unsigned char Match[17]=
```

```
{0xEF,0x01,0xFF,0xFF,0xFF,0xFF,0x01,0x00,0x08,0x04,0x01,0x00,0x01,
0x00,0x01,0x00,0x10} ;

int cnt, Areej, Ekram, zeinab;

unsigned char recive,kp;

// LCD module connections

sbit LCD_RS at PORTB0_bit;

sbit LCD_EN at PORTB2_bit;

sbit LCD_D4 at PORTB4_bit;

sbit LCD_D5 at PORTB5_bit;

sbit LCD_D6 at PORTB6_bit;

sbit LCD_D7 at PORTB7_bit;

sbit LCD_RS_Direction at DDB0_bit;

sbit LCD_EN_Direction at DDB2_bit;

sbit LCD_D4_Direction at DDB4_bit;

sbit LCD_D5_Direction at DDB5_bit;

sbit LCD_D6_Direction at DDB6_bit;

sbit LCD_D7_Direction at DDB7_bit;

// End LCD module connections

//keypad module connections
```

```
sfr char keypadport at PORTA;

sfr char keypadport_Direction at DDRA;

//End keypad module connections

char txt1[] = "scan your";

char txt8[] = "fingerprint";

char txt2[] = "no match";

char txt3[] = "choose your";

char txt4[] = "candidate";

char txt5[] = "1:Areej  2:Ekram";

char txt6[] = "3:Zeinab";

char txt7[] = "Done";

char txt9[] = "well scanned";

char txt10[] = "Error";

char txt11[] = "scan again";

char txt12[] = "stored";

char txt13[] = "Areej=";

char txt14[] = "Ekram=";

char txt15[] = "Zeinab=" ;

char txt16[] = "Wellcome";
```

```
void main(){
  keypad_init();
  Lcd_Init();                    // Initialize LCD
  Lcd_Cmd(_LCD_CLEAR);           // Clear display
  Lcd_Cmd(_LCD_CURSOR_OFF);      // Cursor off
  Lcd_out(1,6,txt16);            // Write text in first row
  Delay_ms(200);
  Lcd_Cmd(_LCD_CLEAR);           // Clear display
    do
      {
      kp=0;
      do
     kp=keypad_key_press();
     while(!kp);
      switch(kp){
      case 1:kp =49;break;  //1
      case 2:kp =50;break;  //2
      case 3:kp =51;break;  //3
      case 4:kp =65;break;  //A
```

```
    case 5:kp =52;break;  //4
    case 6:kp =53;break;  //5
    case 7:kp =54;break;  //6
    case 8:kp =66;break;  //B
    case 9:kp =55;break;  //7
    case 10:kp =56;break; //8
    case 11:kp =57;break; //9
    case 12:kp =67;break;  //c
    case 13:kp =42;break;  //*
    case 14:kp =48;break;  //0
    case 15:kp =35;break;  //#
    case 16:kp =68;break;  //D
    }
UART1_init(9600);
Delay_ms(500);
UART1_write(control);
if(kp=65)
database();
else if(kp=66)
```

```
 search();
 else if(kp=67)
 result();
 else
 LCD_out(1,5,txt10) ;
    }
while(1);


}


void database()
{
 UART1_write(Gen_img);
 delay_ms(50);
  cnt=0;
 while(cnt<10)
  {if(UART1_Data_ready())
 recive=UART1_Read();
 cnt++;}
```

```
 if(recive=0x00)
  {LCD_out(1,3,txt8) ;
 LCD_out(2,3,txt9) ;
 UART1_write(Img2Tz1);
 //UART1_write(Img2Tz2);
// UART1_write(Reg_mod);
 UART1_write(store);
 cnt=0;
  while(cnt<10)
{if(UART1_Data_ready())
 recive=UART1_Read();
 cnt++;
 }
 if(cnt=0x00)
 LCD_out(1,3,txt12) ;
 else
{ LCD_out(1,3,txt10) ;
}
 }
```

```
 }
void search()
{

UART1_write(Gen_img);
delay_ms(50);
   cnt=0;
 while(cnt<10)
   {{if(UART1_Data_ready())
 recive=UART1_Read();}
 cnt++;}
 if(recive=0x01)
 { LCD_out(1,5,txt7) ; }
 else if(recive=0x02)
   {LCD_out(1,5,txt7) ;}
  else if(recive=0x03)
   { LCD_out(1,5,txt7) ;}
 else if(recive=0x00)
 {LCD_out(1,3,txt8) ;
```

```
 LCD_out(2,3,txt9) ;
 UART1_write(Img2Tz1);
 //UART1_write(Img2Tz2);
// UART1_write(Reg_mod);
 UART1_write(Match);
 cnt=0;
 while(cnt<10)
   {{if(UART1_Data_ready())
 recive=UART1_Read();}
 cnt++;}
 if(recive=0x09)
 {LCD_out(1,3,txt2);
 delay_ms(200);
 Lcd_Cmd(_LCD_CLEAR);


 }
 if(recive=0x00)
 {LCD_out(1,2,txt3);
  LCD_out(2,4,txt4);
```

```
 delay_ms(200);
 Lcd_Cmd(_LCD_CLEAR);
 LCD_out(1,2,txt5);
 LCD_out(2,4,txt6);
 delay_ms(200);
 Lcd_Cmd(_LCD_CLEAR);
  do
     kp=keypad_key_press();
      while(!kp);
      switch(kp){
      case 1:kp =49;break;  //1
      case 2:kp =50;break;  //2
      case 3:kp =51;break;  //3
      }
     Areej=EEPROM_read(5) ;
Ekram=EEPROM_read(6) ;
zeinab=EEPROM_read(7) ;
 if(kp=49)
 Areej=Areej+1;
```

```
 if(kp=50)
 Ekram=Ekram+1;
 if(kp=51)
 zeinab=zeinab+1;
 EEPROM_write(5,Areej);
 EEPROM_write(5,Ekram);
 EEPROM_write(5,zeinab);
 LCD_out(1,5,txt7); }
 else
 LCD_out(1,5,txt10); }


   }
 void result()
 {
Areej= EEPROM_read(5) ;
Ekram= EEPROM_read(6) ;
zeinab= EEPROM_read(7) ;
 LCD_out(1,3,txt13);
  LCD_chr(1,11,Areej);
```

```
 LCD_out(2,3,txt14);

LCD_chr(2,11,Ekram);

}
```