Electronic Voting Machine Authentication using Biometric Information

Abeesh A I[1], Amal Prakash P[2], Arun R Pillai[3], Ashams H S[4], Dhanya M[5], Seena R[5]
UG Students, Dept: of Electronics and Communication Engineering,
College of Engineering Perumon, Kollam - 1,2,3,4
Assistant Professor, Dept: of Electronics and Communication Engineering,
College of Engineering Perumon, Kollam - 5,6

Abstract **This paper deals with the design and development of an Electronic Voting Machine(EVM)Authentication using Biometric Information. Here finger print is used as the Biometric information. The suggested fingerprint voting system allows the user to scan his/her fingerprint, in order to check his eligibility by comparing his current fingerprint with the one already stored in the systems database, this paper is designed using PIC16F877A microcontroller and other associated peripheral like GSM module, Finger print module, LCD etc. Once the users complete the identification process, they will be allowed to cast their vote using friendly geographical user interface. The counting of the votes will be immediately and that makes the voting process efficient, fast, and secure. The GSM communication which gives the feedback to the voter just after they cast their vote.**

I. INTRODUCTION

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. Technology is being used more and more as a tool to assist voters to cast their votes. To allow the exercise of this right, almost all voting systems around the world include the following steps:

- Voter identification and authentication
- Voting and recording of votes cast
- Vote counting
- Publication of election results

Voter identification is required during two phases of the electoral process: first for voter registration in order to stablish the right to vote and afterwards, at voting time, to allow a citizen to exercise their right to vote by verifying if the person satisfies all the requirements needed to vote (authentication).

Ancient archeological artifacts and historical items have been discovered to still retain a large number of fingerprints on them. Since this was a discovered significant stride in fingerprinting and identification have been made. In 1788 a detailed description of anatomical formations of fingerprints was made. Then in1823 fingerprints began to be classified into nine categories, (Handbook) and by the 19th century Sir Francis Galton had developed analytical methods for fingerprint matching. As the criminal justice system evolved, there arose the need for criminals to be uniquely identified by some physically identifiable trait. Richard Edward Henry of Scotland Yard began using fingerprinting in 1901 and its success eventually lead to its increased use in the law enforcement field

The field of biometrics was formed and has since expanded on to many types of physical identification. Still, the human fingerprint remains a very common identifier and the biometric method of choice among law enforcement. These concepts of human identification have led to the development of fingerprint scanners that serve to quickly identify individuals and assign access privileges. The basic point of these devices is also to examine the fingerprint data of an individual and compare it to a database of other fingerprints.

Nearly everyone in the world is born with a fingerprint that is unique; a separate and comprehensively identifying attribute that sets us apart from the other 6.5 billon people that inhabit this world. It is because of this fact that the fingerprint has proven such a useful part of biometric security. The very reason that fingerprint scanners are useful can be found in this fact as well. However, this is far from the only reason they are used.

Another important reason fingerprint scanners are used is, they provide a quick, easy, efficient, and secure measure through which, an individual with the proper access privileges can authenticate. The fingerprint of an employee for example, is stored in a database that the scanner queries every time it is used. There are two basic Boolean conditions the scanner then goes through when an individual‟s print is scanned. First, the print is usually searched for in a database of fingerprints, once it is found it then looks at the print to see what access privileges are associated with the print and compares them to the access they are trying to gain. If everything checks out the subject is allowed access and they are not otherwise. In any case, a log of the event is usually stored for security purposes the size of these devices is another reason they have become so mainstream recently. Fingerprint scanners can be deployed directly near a door for access or as a peripheral to a computer for logging in. Modern day scanners have even been embedded on computer keyboards, mice, and USB devices because engineers have been able to reduce their size. Fingerprint scanners are also very versatile in the function that they can serve. The most common use may be for access restriction; however, they have served as time

clocks, personal data retrievers, and even to cut down on truancy in some schools. Since they have experienced so much success in these areas, businesses are expanding upon their use and they are getting more public exposure

Finger printing recognition, the electronic methods of recording and recognizing an individual finger print, advanced substantially during the last decade of the 21th century. Today, identification can be achieved in a few seconds with reasonable accuracy. As a result, the use of automated fingerprint identification systems (AFIS) that record, store, search, match and identify finger prints is rapidly expanding. AFIS 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.

OBJECTIVES OF PAPER

The most crucial factor for a system like e-VOTE to be successful is to exhibit a Voting Protocol that can prevent opportunities for fraud or for sacrificing the voter's privacy. The Voting Protocol that will be designed and implemented for the e-VOTE system will combine the advantages of existing protocols and techniques, while at the same time it will aim at eliminating most of the identified deficiencies and problems. The related attributes that the e-VOTE system will fully support, and against which it will be extensively tested and validated, are listed below. These attributes can be also considered, according to the literature, as a set of criteria for a "good" electronic voting system that can easily enjoy the trust and confidence of the voters and process organizers.

- Democracy: The system should be "democratic" in the sense that it will permit only eligible voters to vote (eligibility) and it will ensure that each eligible voter can vote only once (un-reusability).
- Privacy: The system should ensure that none of the actors involved in the voting process (organizers, administrators, voters etc.) can link any ballot (contextually) to the voter who cast it, and that no voter can prove that he or she voted in a particular way (untraceability).
- Integrity: The necessary mechanism should be employed in order to guarantee that no one can duplicate his or someone else's vote (unduplicability) and no one can change someone else's vote (unchangeability).
- Accuracy: The system functionality should ensure that no one can falsify or modify the result of the voting by eliminating a valid vote or counting an invalid vote in the final tally.
- Verifiability: The system should allow and support anyone to independently verify that all votes have been counted correctly.
- Convenience: The system should allow and assist voters to cast their votes quickly, in one session, and with minimal equipment or special skills.
- Flexibility: The system should allow a variety of ballot formats and it should be customized to the specific characteristics of the voting processes.
- Mobility: The system should not pose any restrictions on the location from which a voter can cast a vote.
- Efficiency: The election can be held in a timely manner (i.e. all computations during the election are done in a reasonable amount of time and voters are not required to wait on other voters to complete the process).
- Scalability: The size of the election should not drastically affect performance.

The paper requires the voter to submit his/her Fingerprint at the election place. The Fingerprint technology will be used in this paper to create the system. The primary goal of the paper is to make a system that requests the voter to give his/her Fingerprint as a personality proof. The fingerprint voting system reads the fingerprints data and compares it with the data previously stored inside the database. If the data exists in the database meets with the previously stored data, the voting system will enable the voter to enter into the system and give his/her vote. If the data of the Finger didn‟t meet with the stored data, then the system will instantly trigger the display and the authorities will come to take an action

II. PROPOSED SYSTEM

BLOCK DIAGRAM

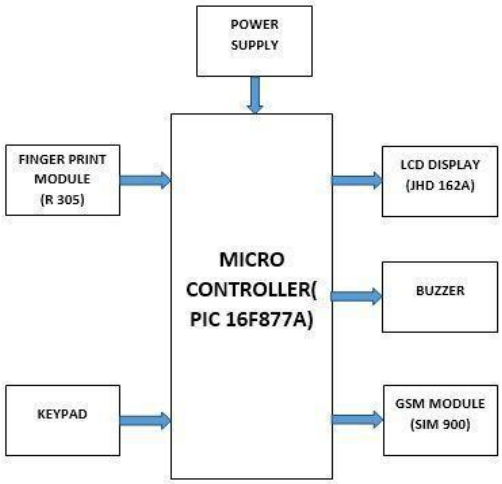


Fig. 2.1 Block Diagram

BLOCK DESCRIPTION

2.2.1 Power Supply:

These form an important equipment of any Electronics laboratory. Power supplies are essential for the testing and implementation of any useful electronic circuit. If power supplies are not available then the only way to

provide power to a circuit is the battery. For long-term use and frequent manipulation these are not feasible. More over these are not as flexible as modern day power supplies. They do not provide for overload protection and thermal protection.

The following units form the backbone of any modern day power supply

- Full wave bridge rectifier
- Filter circuit
- Voltage regulator

In the case if modern power supplies, the required power is derived from the AC mains. For this at first the 230V/50 Hz is step down using a step down transformer. Then The AC voltage is converted to DC using a rectifier circuit. The bridge rectifier is considered the apt choice since it avoids the center-tapped transformer. The ripples from the rectifiers output are removed by filtering.

The filter can be any of the following:

- L filter
- C filter
- LC filter
- CRC filter

The function of the voltage regulator is to provide a stable DC voltage for powering other electronic circuits. The voltage regulator must be capable of providing substantial output current. They must provide a constant voltage regardless of changes in load current, temperature, and AC line voltage. Although voltage regulators can be designed using opamps, it is quicker and easier to use IC Voltage regulators. Furthermore, IC voltage regulators are versatile and relatively inexpensive and are available with features such as programmable output, current / voltage boosting, internal short –circuit current limiting, thermal shut down, and floating operation for high voltage applications.

2.2.2 Micro Controller (PIC16F877A):

The PIC microcontroller PIC16F877A is one of the most renowned microcontrollers in the industry. This controller is very convenient to use, the coding or programming of this controller is also easier. One of the main advantages is that it can be write-erase as many times as possible because it use FLASH memory technology. It has a total number of 40 pins and there are 33 pins for input and output.

PIC16F877A is used in many PIC microcontroller papers. PIC16F877A also have many application in digital electronics circuits.

PIC16F877A finds its applications in a huge number of devices. It is used in remote sensors, security and safety devices, home automation and in many industrial instruments. An EEPROM is also featured in it which makes it possible to store some of the information permanently like transmitter codes and receiver frequencies and some other related data. The cost of this controller is low and its handling is also easy. Its flexible and can be used in areas where microcontrollers have never been used before as in coprocessor applications and timer functions etc.

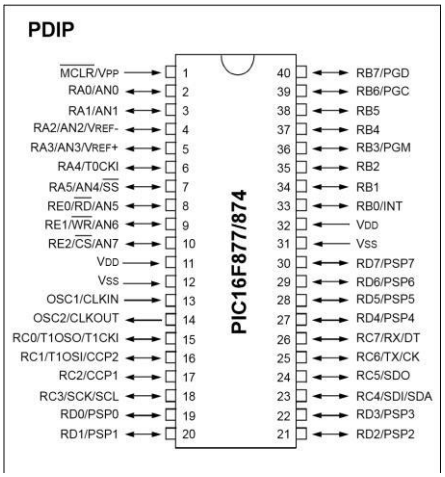


Fig. 2.2 Pin Diagram - PIC 16F877A

2.2.3Finger Print Module: Fingerprint capacity

R305 Fingerprint Module nominal storage capacity is 500, the actual test is 980.

Interface description

While the R305 Fingerprint Module RS232 and USB1.1, dual interface to communicate with the outside world; USB1.1 interface can be connected to the computer; RS232 interface is a TTL level, default baud rate is 57600, you can make changes, please refer to the communication protocol; may with the microcontroller, such as ARM, DSP and other devices with a serial connection, 3.3V 5V microcontroller can be connected directly. Connected to the computer needs to be level conversion, please note the level conversion, such as MAX232 circuit.

Fig. 2.3 Finger Print Module – R305

Detection on modules

After power-on fingerprint module, fingerprint capture window will flash, indicating that the self-test is normal, if not flash, please check the power is reversed, and so wrong. When the chips have to work some hot,, This is a normal phenomenon, has been rigorously tested, can be assured.

Features

- Small

Image capture chip and fingerprint algorithms are integrated chip fingerprint head, easy to install.

- Powerful

In the host computer (PC or microcontroller) command, independently fingerprint input, image processing, feature extraction, template generation, template storage, fingerprint matching (1: 1) or a fingerprint search (1: N) and other functions.

- Simple developed

Module has a rich command, the equivalent of a fingerprint library. Developers do not need to have expertise in fingerprint identification, according to the control commands provided can develop powerful fingerprint recognition applications themselves.

- Rich interface

Power supply: 4V-6V DC power supply. Serial communication port: standard UART protocol provides two levels (TTL / RS232), communication baud rate.

- Strong adaptability

Excellent series of algorithm performance, according to the principle of optical imaging professional design. Poor quality fingerprints for a good correction and fault tolerance.

Fingerprint image reading process, adaptive parameter adjustment mechanism so dry, wet fingers have a better image quality, wider application of the crowd.

- Adjustable security level

Suitable for different applications, users can set different security levels.

- Suitable for different applications

In accordance with the requirements of application systems, modules easily set to different modes of operation.

Technical parameters

Supply voltage: DC 4V ~
6.0V Supply Current:

Operating Current: 110mA
(typical) Peak current: 140mA

Fingerprint image time: <0.3
seconds Window area: 15**x**19 mm

Matching:

Than on the way
(1: 1) Search mode
(1: N)

Signature File: 256
bytes Template file:
512 bytes
Storage capacity: 500 (standard) / 1000 (custom) Safety level: five (from low to high: 1,2,3,4,5) False Accept Rate (FAR): <0.001%
False rejection rate (FRR): <1.0%
Search time: <1.0 seconds (1: 1000, average)
PC Interface: UART (TTL logic level) and USB1.1 Communication baud rate (UART) :(9600╳N) bps where N = 1 ~ 12 (default value N = 6, ie 57600bps) Working environment:

Temperature: -20 ℃ - + 60 ℃

Relative Humidity: 20% RH-85% RH (non-condensing)

Storage environment:

Temperature: -40 ℃ - + 85 ℃

Relative humidity: <85% H (non-condensing)

Applicable to lock, fingerprint safe, fingerprint access control and other occasions.

2.2.4 Keypad:

The system is designed to accommodate many number of candidates. The key pad used for the system contains 3 keys. One is reserved for resetting the whole system and the other two switches plays multiple roles such as candidate selection, voting, displaying the result and clearing the result.

2.2.5 GSM Module:

GSM/GPRS module is used to establish communication between a computer and a GSM-GPRS system**.** Global System for Mobile communication (GSM) is an architecture used for mobile communication in most of the countries. Global Packet Radio Service (GPRS) is an extension of GSM that enables higher data transmission rate. GSM/GPRS module consists of a GSM/GPRS modem assembled together with power supply circuit and

communication interfaces (like RS-232, USB, etc.) for computer. The MODEM is the soul of such modules.

Fig. 2.4 GSM Module – SIM 900

A GSM/GPRS module assembles a GSM/GPRS modem with standard communication interfaces like RS-232 (Serial Port), USB etc., so that it can be easily interfaced with a computer or a microprocessor / microcontroller based system. The power supply circuit is also built in the module that can be activated by using a suitable adaptor.

The modem (modulator-demodulator) is a critical part here. These modules consist of a GSM module or GPRS modem powered by a power supply circuit and communication interfaces (like RS-232, USB 2.0, and others) for computer. A GSM modem can be a dedicated modem device with a serial, USB or Bluetooth connection, or it can be a mobile phone that provides GSM modem capabilities.

2.2.6 LCD Module:

LCD (Liquid Crystal Display) screen is an electronic display module and find a wide range of applications. A 16x2 LCD display is very basic module and is very commonly used in various devices and circuits. These modules are preferred over seven segments and other multi segment LEDs. The reasons being: LCDs are economical; easily programmable; have no limitation of displaying special & even custom characters (unlike in seven segments), animations and so on.

A **16x2 LCD** means it can display 16 characters per line and there are 2 such lines. In this LCD, each character is displayed in 5x7 pixel matrix. This LCD has two registers, namely, Command and Data.

The command register stores the command instructions given to the LCD. A command is an instruction given to LCD to do a predefined task like initializing it, clearing its screen, setting the cursor position, controlling display etc. The data register stores the data to be displayed on the LCD. The data is the ASCII value of the character to be displayed on the LCD. Click to learn more about internal structure of a LCD.

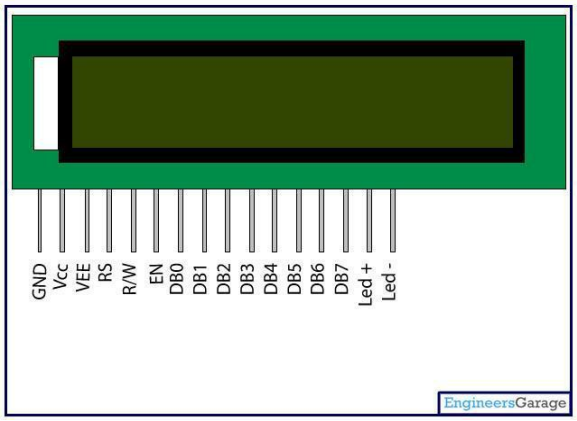


Fig. 2.5 Pin Diagram LCD Module – JHD 162A

2.2.7 Buzzer:

The **piezo buzzer** produces sound based on reverse of the piezoelectric effect. The generation of pressure variation or strain by the application of electric potential across a piezoelectric material is the underlying principle. These buzzers can be used alert a user of an event corresponding to a switching action, counter signal or sensor input. They are also used in alarm circuits.

Fig. 2.6 Buzzer

The buzzer produces a same noisy sound irrespective of the voltage variation applied to it. It consists of piezo crystals between two conductors. When a potential is applied across these crystals, they push on one conductor and pull on the other. This, push and pull action, results in a sound wave. Most buzzers produce sound in the range of 2 to 4 kHz.

III. IMPLEMENTATION

CIRCUIT DIAGRAM

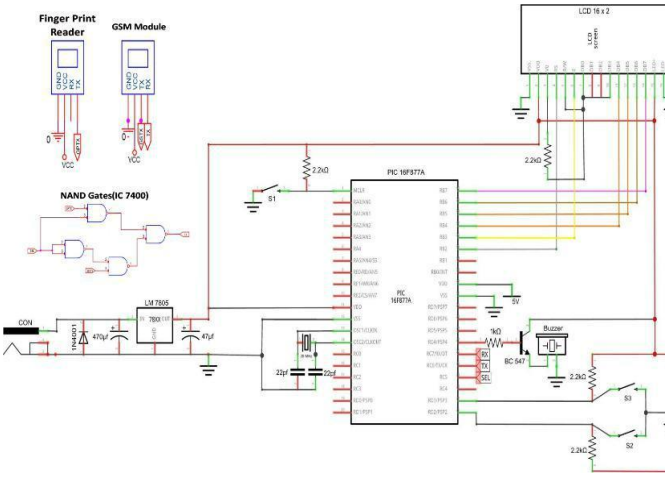


Fig. 3.1 Circuit Diagram

COMPONENT LIST

Component	Specification
LCD Module	**JHD 162A**
Finger Print Module	**R 305**
GSM Module	**SIM 900**
PIC Microcontroller	**PIC 16F877A**
Buzzer	
Crystal Oscillator	**20 MHz**
Nand Gate	**IC 7400**
Voltage Regulator	**LM 7805**
Capacitors	**470 µf** **47 µf** **22 pf**
Resistors	**2.2 kΩ** **1 kΩ**
Diode	**1N4001**
Transistor	**BC 547**

WORKING

Supply Section of this circuit consists of a 12 volts adaptor, and a IC 7805 IC. The output of the second regulator (IC 7805) is +5 volts, which is used for all other digital applications. The Voting machine consists of control unit and ballet unit. Ballet unit consist of two keys, which are connected to 2 separate pins of PIC micro controller, ports pins RD3 and RD2 which are usually made low. The display section uses PORT B of the micro controller. The contrast of this LCD is adjusted by changing the values of resistor which is grounded at another end. The finger print module and GSM module is multiplexed and connected to the TX and RX pins of the PIC micro controller. During the process, when the voter place his/her registered finger in the scanner, the system will check whether it matches with the pre-stored impression in the database. If it is presented, the system will allow the voter to cast their votes by enabling the voting unit and display unit shows the details of the Voter. If not, it results in an error message. The voter can cast their vote by selection and Confirm button. A Buzzer is used to indicate whether a voter has exercised his vote correctly and also for recognizing any malpractice during the whole process. This buzzer is connected to a supply of +5 volts by means of a pull up resistor. After the successful completion of voting process, the control unit sends a message to the registered number of the corresponding voter through GSM module. The election result can be obtained by pressing both the Reset switch and Selection switch simultaneously for a time duration, the display unit will show the name and votes obtained by each candidate. The results can be cleared by long pressing the Confirm switch for a time duration.

OVERALL VIEW

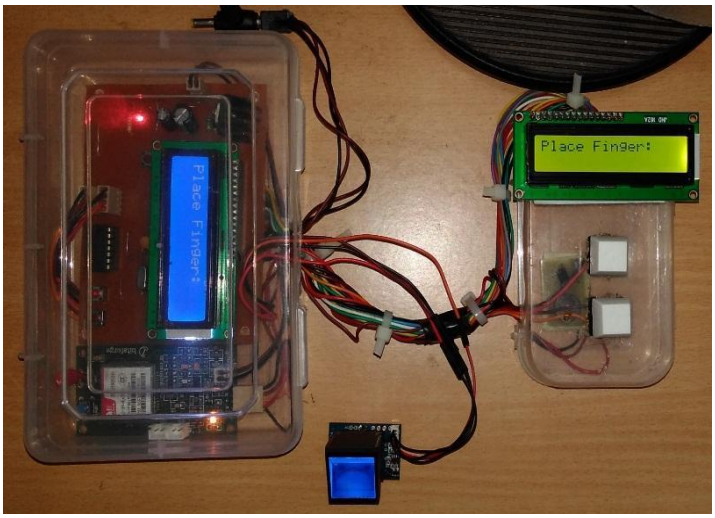
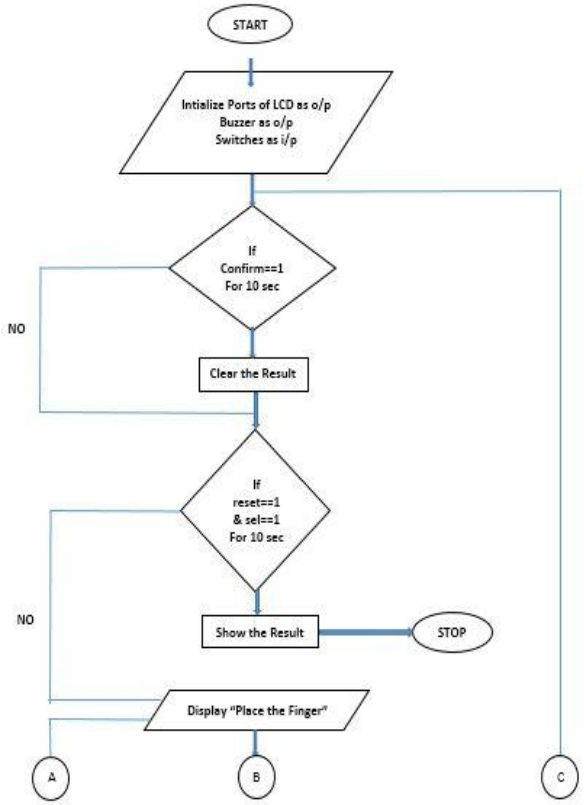
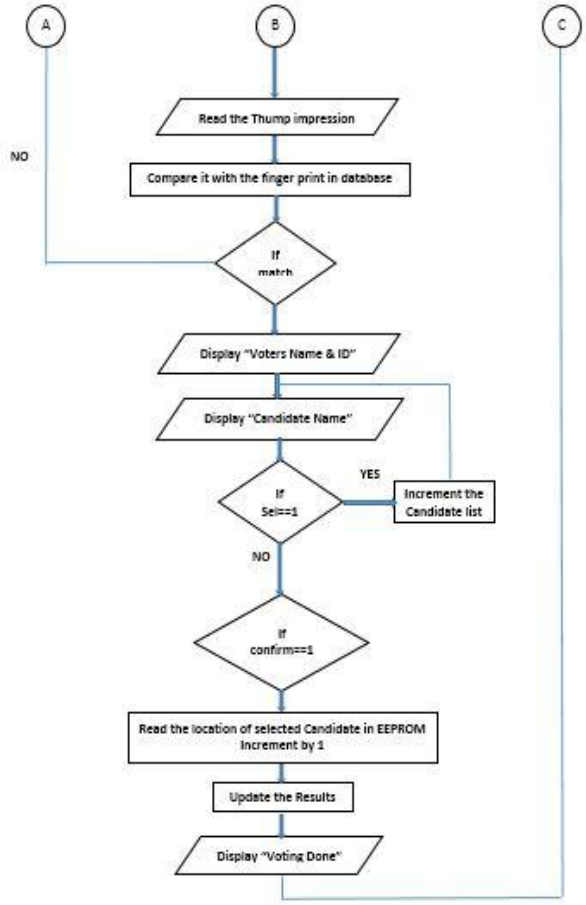


Fig. 3.4 Overall View

SOFTWARE DESCRIPTION

Flowchart:





IV. ADVANTAGES& DISADVANTAGES

ADVANTAGES

- Providing the preventive measures system for voting.
- It completely rules out the chances of invalid votes results in fewer problems in electoral preparations, law and order, candidate's expenditure.
- It results in polling time, provide easy and accurate counting without any mischief at the counting center.
- It capable of Saving considerable printing stationary and transport of large volume of electoral material.
- Lower risk of human and mechanical errors.

DISADVANTAGES

- Each fingerprint voting system depends on an important external factor which isthe fingerprint's image. The resolution and the quality of the image have huge impact tothe system. This system is working perfect with low quality image but it doesn't workwell with very low quality image. Very low quality image leads to rejecting the image orto false rejection.

- Database Images have a large size it has resolution of eight bits per pixel.Uploading a large number of fingerprints image to the database demands a large

memoryspace as well as large number of voters mean more fingerprint picture must be uploadedin to the database and that makes the database response slower the leads to slower votingprocess.

V. FUTURE SCOPE

Memory of finger print module can be expanded .We can use a 1mb flash memory finger print module for increasing the capacity.External memory can be provided for storing the finger print image, which can be later accessed for comparison.Smart Card reader module is supposed to be introduced with the existing module for further security, and to reduce the database storage.Audio output can be introduced to make it user friendly for illiterate voters.Retina scanning can also be developed.

VI. CONCLUSION

For over a century, fingerprints have been one of the most highly used methods for human recognition; automated biometric systems have only been available in recent years.This work is successfully implemented and evaluated. The arrived results were significant and more comparable. It proves the fact that the fingerprint image enhancement step will certainly improve the verification performance of the fingerprint based recognition system.Because fingerprints have a generally broad acceptance with the general public, law enforcement and the forensic science community, they will continue to be used with many governments,, legacy systems and will be utilized in new systems for evolving applications that require a reliable biometric.This biometric voting system would enable hosting of fair elections in India.This will preclude the illegal practices like rigging. The citizens can be sure that they alone can choose their leaders, thus exercising their right in the democracy.

VII. REFERENCE

[1] Ashok Kumar D., Ummal Sariba Begum T., “A Novel design of Electronic Voting System Using Fingerprint”,International Journal of Innovative Technology & Creative Engineering (ISSN:2045-8711),Vol.1,No.1. pp: 12 19, January 2011.
[2] Benjamin B., Bederson, Bongshin Lee., Robert M. Sherman., Paul S., Herrnson, Richard G. Niemi., “Electronic Voting System Usability Issues”, In Proceedings of the SIGCHI conference on Human factors in computing systems, 2003.
[3] California Internet Voting Task Force. “A Report on the Feasibility of Internet Voting”, Jan.2000.
[4] Chaum D., “Secret-ballot receipts: True voter-verifiable elections”, IEEE Security and Privacy38-47, 2004.
[5] Darcy, R., & McAllister, I., “Ballot Position Effects”, Electoral Studies, 9(1), pp.5-17, 1990.
[6] Gritzalis D., [Editor]., “Secure Electronic Voting”, Springer-Verlag, Berlin Germany, 2003.
[7] D. Balzarotti, G. Banks, M. Cova, V. Felmetsger, R. A Kemmerer, W. Robertson, F. Valeur, and G. Vigna, “An Experience in Testing the Security of Real-World Electronic Voting Systems,” IEEE Transactions on Software Engineering, vol. 36, no. 4, 2010.
[8] Mazidi Md.Ali, Mazidi J.G., McKinlay R. D., the 8051 microcontroller & embedded systems, (Pearson Prentice Hall, Delhi, 2006).
[9] Alam, M.R. ; Univ. Kebangsaan Malaysia ; Masum, M. ; Rahman, M. ; Rahman, A.,Design and implementation of microprocessor based electronic voting system, Computer and Information Technology, 2008. ICCIT 2008. 11th International Conference, 24-27 Dec. 2008.
[10] D. Molnar, T. Kohno, N. Sastry, and D. Wagner, “Tamper-Evident, History Independent, Subliminal-Free Data Structures on PROM Storage-or-How to Store Ballots on a Voting Machine (Extended Abstract),” in Proc. of IEEE Symp. Security and Privacy, pp. 365-370, 2006.
[11] R. Hite, “All Levels of Government are needed to Address Electronic Voting System Challenges,” Technical report, GAO, 2007.