

Multi Level Security Based Electronic Voting System

S. Prassanna Perumal¹, S. Vijayalakshmi², KR. Vairamani³, K. Kalyani⁴

Students^{1, 4}, Assistant Professor^{2, 3}

Department of EEE

Saranathan College of Engineering, Trichy

Corresponding Authors: *prassannaex@gmail.com¹, bksviji@gmail.com², kvirams@gmail.com³,
kalyanisumathi21@gmail.com⁴*

Abstract

The impressive Multi level security based electronic voting system is introduced to ensure apposite voting procedures and voting counts. This idea prevents the illegal acts against the voting system and provides the voter authentication in an effective manner. This proposal plans to provide a fortification for each and every vote. It entirely changes the status of the election process and ensures the integrity of electoral system. The primary idea of this project is to make the voters as to have a trust in election through the methods of taking fingerprint, IRIS Scanner and providing a Voter card to each user to promise their uniqueness in the voting system and reduces the work of election committee. With the help of this method, the person can vote from any election booth easily.

Keywords: *Electronic Voting System (EVM), Microprocessor (MP), Fingerprint, IRIS Scanner, Barcode, GSM Modules, Keypad, LCD Display.*

I. INTRODUCTION

Electronic voting is an election method in which the votes are cast or collected electronically. A computer system whose main element is a software component that

maps the voting procedure electronically is called an e-voting system. A direct recording electronic (DRE) machine is a special case of such a system as it implements all steps in the voting process,

from start to declaration of results. There are two different forms of voting: distance and presence voting.

It reduces the time in both casting a vote and declaring the results compared to the old project ballot system. However, they have been under the suspicion over their alleged tampering capability and security problems during elections (especially after the 2009). After reign of Delhi High Court, and other courts and demands from various political issues, the Election Commission determined to introduce electronic voting with Voter-verified paper audit trail (VVPAT) system.

The Voter-verified paper audit trail system is introduced in 8 of 543 parliamentary constituencies as a pilot project. Also all voters became an active voter in one of the point that voters don't need to go to specific polling station; thus this is one factor of modifying inactive voters (manual voting) to active voter (Electronic voting).

In an active voter isn't long queue wait and the time-consume and efficiency for achieving voting process in E-voting is constant. Since technology has made great strides over the past decade, the most

important and revolutionary item is certainly the Internet, because of the convenience and popularity of the Internet, it becomes increasingly necessary to offer services via the web, the finger print sensor gets the finger print & IRIS Scanner get the iris image of the voters and it passes it to the computer. In computer the finger print image & IRIS Scanner image is compared with the image in database. If it matches, the computer informs the command the person is valid to the micro controller and displayed. If anyone try to poll their vote beyond the time limit, system will be blocked.

The proposed E-Election system that focused on blended of biometrics-fingerprint, IRIS Scanner and ID barcode reader for enhancement of the voting system and modifies the Project ballot to web bases ballot. Biometrics is the term given to the use of biological traits or behavioural characteristics to identify an individual. The traits may be fingerprints, hand geometry, facial geometry, retina patterns, voice recognition, and handwriting recognition in our proposed system the combine uses of impression for the purpose of voter identification or authentication, barcode reader for (voter ID card) and thumb as the

thumb impression, iris image of every individual is unique, it helps in maximizing the accuracy.

A database is created containing the thumb impressions & iris image of all the voters in the constituency. Illegal votes and repetition of votes is checked for in this system. Hence if this system is employed the elections would be fair and free from rigging one of the most important government services like elections became a severe pressure on people involved in that process, according to many constraints that must be applied to the beneficiaries of this service and which are divided into two parts, candidates and voters.

II. ELECTRONIC VOTING MACHINE

Electronic voting machine is a device that has the programmed to conduct a campaign of election in a fair and quick a manner. The idea of electronic voting machines (EVM) started by the chief election commissioner in 1977. This was a technical development of the Electronics Corporation of India Limited (ECIR), Hyderabad and with Bharat Electronics Limited (BEL), Bangalore. The full control of the machine is with the presiding officer or the chief polling officer of the area as the control unit while the

other unit called balloting unit is placed inside the compartment. Electronic Voting Machine (EVM) retains all the characteristics of voting by Project, while making polling a lot more convenient and absolutely consistent. And, also it, helps maintain total voting privacy without the use of ballot Project.

An Electronic Voting Machine (EVM) consists of two Units – a Control Unit and a Balloting Unit joined by a five-meter cable. The balloting unit enables the voters to provide their votes. Each balloting unit can accommodate more than 10 candidates. Such units can be connected to a single control unit. EVMs are powered by an ordinary 6 volt alkaline battery. This design helps the use of EVMs throughout the country without interruptions because several parts of India do not have power supply and/or erratic power supply.

Electronic Voting Machine:

This highly intelligent Electronic Voting Machine consists of the Three Security level.

1. Fingerprint Level
2. Barcode Level
3. IRIS Scanner Level

1. Finger print Level



Fig. 1 Fingerprint Level

Fingerprint Level is shown in Fig. 1. Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identities. The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies.

Fingerprint processing includes two parts: fingerprint enrolment and fingerprint matching (the matching can be 1:1 or 1:N). When enrolling, user needs to enter the finger two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1: N matching, or searching, system will search the whole finger library for the matching finger. In

both circumstances, system will return the matching result, success or failure.

2. Barcode Level



Fig. 2 Barcode Level

Barcode Level is shown in Fig. 2. A barcode reader (or barcode scanner) is an electronic device that can read and output printed barcodes to a computer. Like a flatbed scanner, it consists of a light source, a lens and a light sensor translating optical impulses into electrical ones.

Additionally, nearly all barcode readers contain decoder circuitry analyzing the barcode's image data provided by the sensor and sending the barcode's content to the scanner's output port.

3. Iris Scanner Level



Fig. 3 Iris Scanner Level

IRIS Scanner Level is shown in Fig. 3. CIS 202 is the latest Cogent Iris Scanner. This rugged dual iris capture scanner offers a robust yet low cost solution for rapid and simultaneous iris capture in less than two seconds. This USB-powered scanner enables users to safely capture high resolution iris images, while eliminating intrusive capture position or user discomfort.

Compliant with NIST SAP level 40, CIS 202 has near infrared illuminators, LED lighting, and built-in spectral imaging sensitivity control to capture light in the range of 700-900 nanometer's. CIS 202 image output meets industry interchange format specifications by supporting ANSI NIST Type-17 records, with raw images conformant to ISO 19794-6 rectilinear image standards.

Enclosed in a durable and adjustable casing that meets IP 54 rating, CIS 202's sturdy, hand-friendly goggle design is ideal for biometric application such as civil registry enrolment, biometric document issuance, applicant identification, border control, and inmate release management.

OPERATION:

Multi Level Security Based Electronic Voting System. Finger print sensor is the special type of sensor which is used to identify the human finger print. Finger print sensor is interfaced with microcontroller through the arm processor circuit. The arm processor circuit is used to activate the finger print sensor at time of finger is placed on the sensor. Then the related data is stored in the microcontroller.

Retinal scanning is a different, ocular-based biometric technology that uses the unique patterns on a person's retina blood vessels and is often confused with iris recognition. Iris recognition uses video camera technology with subtle near infrared illumination to acquire images of the detail-rich, intricate structures of the iris which are visible externally.

Digital templates encoded from these patterns by mathematical and statistical algorithms allow the identification of an individual or someone pretending to be that individual.

The hand held laser scanner does not have to be closed to the bar code in order to do its job. It uses a system of mirrors and lenses to

allow the scanner to read the bar code regardless of orientation, and can easily read a bar code up to 24 inches away. To reduce the possibility of errors, a laser scanning may perform up to 500 scans per second. Specialized long-range laser scanners are capable of reading a bar code up to 30 feet away. The bar code will be different for each voter. So that, after detecting the barcode the controller will send the student details with time to the PC.

The whole data will be stored in the PC. We can retrieve the data when needed.

Microcontroller received the data from the finger print sensor & Iris Scanner. Then compared with stored data if the person finger & iris is valid for that voter name mentioned in the voter ID card, the microcontroller displays the information as “Enter your vote” on the LCD display. Then we can cast our vote to desired person through key pad.

The key pad consists of set of key in which each key represents candidate name or symbol. If the person finger print is not valid for that particular voter name, the microcontroller will display the “Authentication Fail” on the LCD display

and also activate the driver circuit for alarm. So the alarm makes the sound for indicating the Authentication Fail.

The GSM/GPRS Modem comes with a serial interface through which the modem can be controlled using AT command interface. SMS is an area where the modem can be used to provide features. These SMS can be transmitted on certain trigger events in automation system. SMS can also be used in areas where small text information has to be sent.

The DPDT relay is controlled by the BC 547 switching transistor. When you want to transfer the information from the microcontroller to PC, we have to press the button. So the high signal is given to base of the BC547 transistor. Hence the transistor is turn ON and energizes the DPDT relay. Now the information from the microcontroller is transferred to PC.

1. Block Diagram

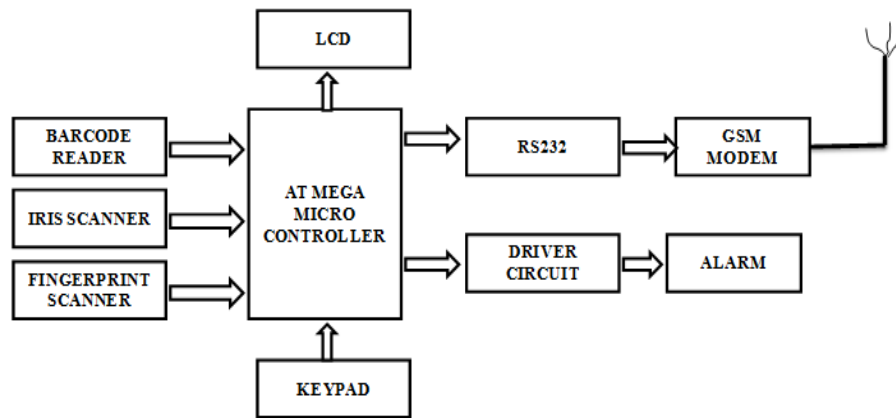


Fig. 4 Block diagram

2. Matchmaking algorithm between pre-register thumb image and real thumb image of voter in voting day

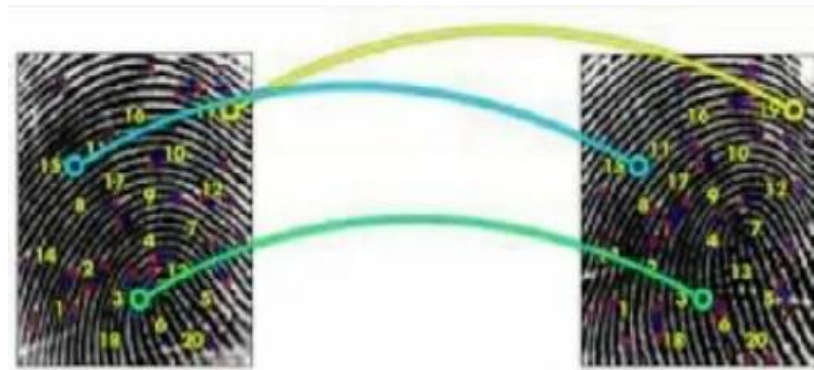


Fig. 5 Finger print match making circuit

Fig. 5 shows the fingerprint matchmaking algorithm between pre-register thumb image and real thumb image. If comparison operation is not properly done, the microcontroller is displays the “Result is not

in Time” on the LCD display. If the sensing finger print is not valid with stored entries then the microcontroller displays the “Authentication Fail” on the LCD display.

3. Entry mode

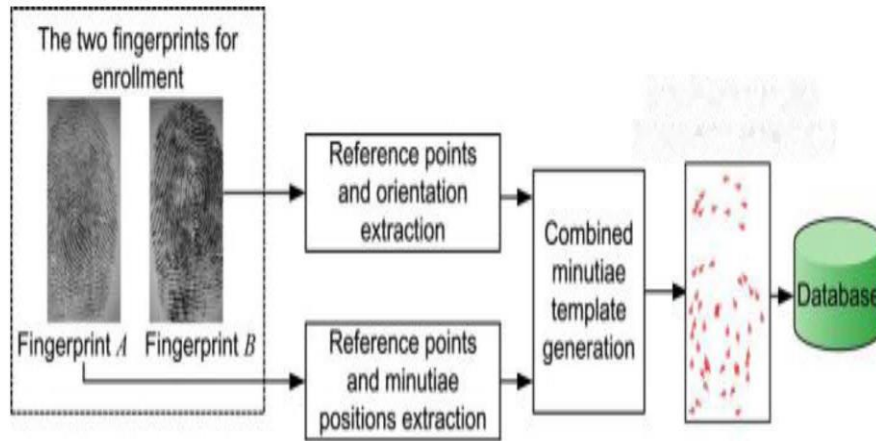


Fig. 6 Entry mode sensor

In entry mode the sensor is interfaced with PC is as shown in Fig. 6. In PC we have written software which helps the users entries stored in the sensor memory cells along with respective ID numbers.

4. Verification mode

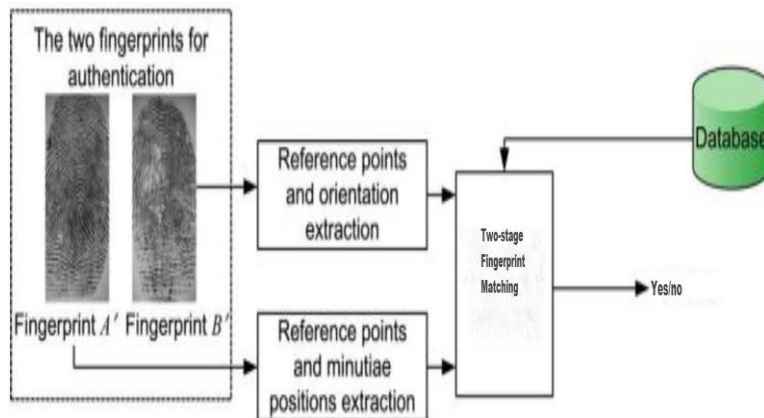


Fig. 7 Verification mode sensor

In the verification mode the sensor is interfaced with microcontroller is illustrated in Fig.7. In order to verify the finger we have to place the finger on the sensor and press the button. The microcontroller sends the protocol to the Arm processor circuit. Now the sensor is activated and senses the finger print which is compared with stored entries in the memory. If the sensing finger print is matched, the arm processor circuit sends the corresponding person ID number to the microcontroller. The microcontroller displays the received ID number on the LCD display.

5. Barcode readers can be differentiated by technologies as follows

Pen-type readers consist of a light source and photodiode that are placed next to each

other in the tip of a pen or wand. To read a bar code, the person holding the Pen must move the tip of it across the bars at a relatively uniform speed is shown in Fig. 8. The photodiode measures the intensity of the light reflected back from the light source as the tip crosses each bar and space in the printed code. The photodiode generates a waveform that is used to measure the widths of the bars and spaces in the bar code. Dark bars in the bar code absorb light and white spaces reflect light so that the voltage waveform generated by the photodiode is a representation of the bar and space pattern in the bar code. This waveform is decoded by the scanner in a manner similar to the way Morse code dots and dashes are decoded.

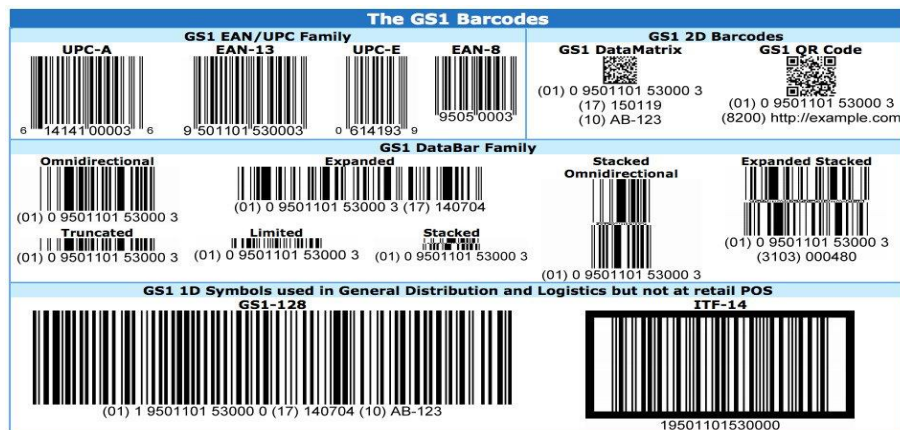


Fig. 8 Barcode pen-type readers

6. Matchmaking algorithm between pre-register thumb image and real thumb image for IRIS Scanner by technologies as follows



Fig. 9 Iris Scanner match making

All publicly deployed iris recognition systems acquire images of an iris while being illuminated by light in the near infrared wavelength band (NIR: 700–900 nm) of the electromagnetic spectrum. The majority of persons worldwide have "dark brown eyes", the dominant phenotype of the human population, revealing less visible texture in the VW band but appearing richly structured, like the cratered surface of the moon, in the NIR band. (Some examples are shown here.) Using the NIR spectrum also enables the blocking of corneal specular reflections from a bright ambient environment, by allowing only those NIR

wavelengths from the narrow-band illuminator back into the iris camera.

Advantages of this system

- Improve security performance in the voting System.
- Improve security performance in the verification method.
- Avoid the forgery vote.
- Low power consumption.
- Cast the vote easily.

CONCLUSION

This project focuses on the voting technologies that provides assurance to the people who really have right to vote in their constitution and ensures secured riggleless voting using the methods of Multi Level Security of the uniqueness in the voting procedures. This system uses account identification number to maintain the voters account, finger print image as biometric security, voter card for authentication & secret key for cross verification of the database. Thus the system provides a multilevel security and adequate proof of authenticity which is the advantage over the earlier election system. The entire work also offers a reduced man power as well as time to conduct voting.

REFERENCES

- 1) Baig,K., Ishtiaq, U., Kanwal, A., Ishtiaq, U., & Javed, M. (2011). "Electronic Voting System Using Fingerprint Matching with Gabor Filter". COMSATS Institute of Information Technology, Lahore, 2011.
- 2) Shanu Agrawal, Pradeep Majhi, Vipin Yadav, "Fingerprint Recognition Based Electronic Voting Machine" International Journal of Engineering and Technical Research ISSN: 2321-0869, Special Issue, 2009.
- 3) G. Keerthana, P. Priyanka, K. Alise Jenifer, R. Raja dharashini, Aruna Devi. P. "Impressive Smart Card Based Electronic Voting System", International Journal of Research in Engineering and Technology, Vol. 4, No. 3, March 2015.
- 4) Diponkar Paul and Sobuj Kumar Ray (2013). "A Preview on Microcontroller Based Electronic Voting Machine", International Journal of Information and Electronics Engineering, Vol. 3, No. 2, March 2013.
- 5) Hazzaa, F., & Kadry, S., (2012). New System of E-Voting Using Fingerprint. International Journal of Emerging Technology and Advanced Engineering
- 6) ShwetaA.Tambe, Prof. P. S.Topannavar. The Steganography and Biometric Based Online Voting System, International Journal of Advanced Research in Computer

Science and Software Engineering,
Vol. 5, No. 4, March 2015.

- 7) Hazzaa, F. I, Kadry, S., & Zein, O.
K. (2012). Web-Based Voting
System using Fingerprint: Design
and Implementation. International
Journal of Computer
Applications in Engineering
Sciences.