ISSN 2348 – 9928
IJAICT Volume 2, Issue 10, October 2015 Doi:01.0401/ijaict.2014.03.20 Published Online 05 (10) 2015

DESIGN AND IMPLEMENTATION OF BALLOT MALFUNCTIONING AVOIDANCE SYSTEM SECURITY OPTIMIZATION USING FINGERPRINT GSM VOTING SYSTEM

Prof. V.M. Umale
Associate Professor,
Electronics and Telecommunication Engineering,
Shri Sant Gajanan Maharaj College of Engineering,
Shegaon, India

Mrs. S.M. Shinde
PG Scholar,
Electronics and Telecommunication Engineering,
Shri Sant Gajanan Maharaj College of Engineering,
Shegaon, India

Abstract— Electronic voting (also known as e-voting) is a term encompassing several different types of voting, embracing both electronic means of casting a vote and electronic means of counting votes. Electronic voting technology can include punch cards, optical scan voting systems and specialized voting kiosks (including self-contained Direct-recording electronic (DRE) voting systems). It can also involve transmission of ballots and votes via telephones, private computer networks, or the Internet. Electronic voting systems may offer advantages compared to other voting techniques. An electronic voting system can be involved in any one of a number of steps in the setup, distributing, voting, collecting, and counting of ballots, and thus may or may not introduce advantages into any of these steps. The main aim of this paper is develop fingerprint Electronic Voting Machine with maximum security facilities.

Keywords—Punch Cards, Optical Scan, RE, Ballots, Fingerprint.

I. INTRODUCTION

Normally used punch cards Optical scan voting systems Malfunctions Excess amount of time Counting time is more. The Bio-metric based voting system Give acknowledgement to voter Avoid malfunctions Time maintenance system automatic counting of votes Bio Metric Authentication Technology and GSM Technology.

As embedded applications include more functionality, the challenge is making these functions accessible to the end user in a meaningful way.

- Design the hand held hardware with LCD, Keypad and RTC
- Design the power supply selector circuit for peripheral and controller.
- Write the programmer for the main controller using embedded ‘c’ for 8051.
- Design a driver for sending or receiving message.

II. WORKING PRINCIPLE

In this project we have two sections one is validating section another one is voting section. The validating section has finger print sensor and computer.

The finger print sensor gets the finger print of the voters and sends to the PC. In PC the finger print image is compared with existing image. If the image is matched, the computer sends the command the person is valid to the micro controller. After receiving the command the micro controller allow the voter to poll their vote. The voter poll the vote up to the voting time allocated by the election commissioner. If anyone try to poll their vote beyond the time limit, the GSM modem send the message alert to authorized person.

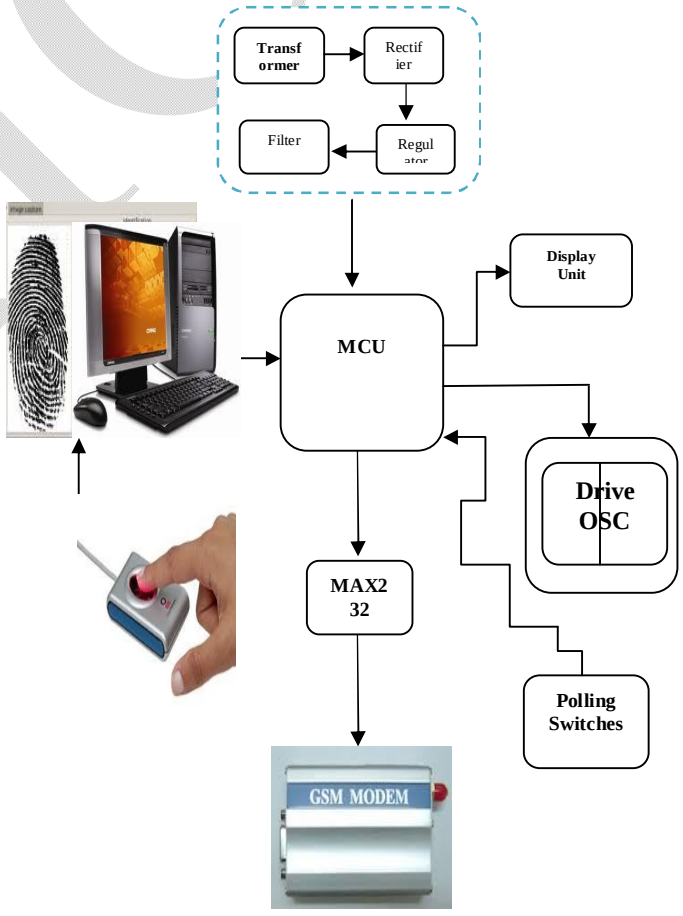

Fig 1 : Block Diagram

III. SYSTEM OVERVIEW

SM630 background highlight optical fingerprint verification module is the latest release of Mi axis Biometrics Co., Ltd. It consists of optical fingerprint sensor, high performance DSP processor and Flash. It boasts of functions such as fingerprint Login, fingerprint deletion, fingerprint verification, fingerprint upload, fingerprint download, etc. Compared to products of similar nature, SM630 enjoys the following unique features:

● ***Self-proprietary Intellectual Property***

optical fingerprint collection device, module hardware and fingerprint algorithm are all self developed by Miaxis.

● ***High Adaptation to Fingerprints***

When reading fingerprint images, it has self-adaptive parameter adjustment mechanism, which improves imaging quality for both dry and wet fingers. It can be applied to wider public.

● ***Low Cost***

Module adopts Miaxis' optical fingerprint collection device, which dramatically lowers the overall cost.

● ***Algorithm with Excellent Performance***

SM630 module algorithm is specially designed according to the image generation theory of the optical fingerprint collection device. It has excellent correction & tolerance to deformed and poor-quality fingerprint.

● ***Easy to Use and Expand***

User does not have to have professional know-how in fingerprint verification. User can easily develop powerful fingerprint verification application systems based on the rich collection of controlling command provided by SM630 module. All the commands are simple, practical and easy for development.

Technical Specifications
Operating Voltage: 4.3V~6V
Rating Voltage: 6.5V(exceeding this value will cause permanent damage to the module)
Operating Current: <80mA(Input voltage 5V)
Fingerprint Template: 768 templates
Search Time: <1.5s(200 fingerprint, average value in test)
Power-on Time: <200ms (Time lapse between module power-on to module ready to receive instructions)
Tolerated Angle Offset±45°
User Flash Memory: 64Kbyte

IV. CODING METHOD

The communication between HOST and Module must be coded as Communication Packet. One communication packet includes the following: packet Head (2 bytes), Packet flag (1 byte), Packet length (1 byte), Packet Content(N bytes), Check sum (1 byte), Packet head: 0x4D 0x58

Packet flag: 0x10: command packet, 0x20: data packet, 0x21: last packet, 0x30: response packet.

* ***Command Description***

Table 1 : Communication Protocol

No.	Name of Command	Command Code
1	Add fingerprint	0x40
2	Delete fingerprint	0x42
3	Search fingerprint	0x44
4	Empty fingerprint database	0x46
5	Search information in fingerprint database	0x4B
6	Download fingerprint template	0x50

Table 2 : Response Code

No.	Name of Command	Response Code
1	Receive correct	0x01
2	Receive error	0x02
3	Operation successful	0x31
4	Finger detected	0x32
5	Time out	0x33
6	Fingerprint process failure	0x34
7	Parameter error	0x35
8	Fingerprint matching with this ID found	0x37
9	No matching fingerprint with this ID	0x38

Add fingerprint

Description: Add fingerprint at the designated position
Length: 3 bytes
Format: Command code 0x40 + high byte of the to-be-added fingerprint ID + low byte of the to-be-added fingerprint ID
Flowchart: After module receives the command to add fingerprint, it goes to the status of adding fingerprint. The

flowchart is as follows:

For example

1 HOST send command to add fingerprint at position 0: 0x4D + 0x58 + 0x10 + 0x03 + 0x40 + 0x00 + 0x00 + 0xF8

2 Module responds by receive correct: 0x4D + 0x58 + 0x30 + 0x01 + 0x01 + 0xD7

3 First time to press finger. Module will respond as operation successful after processing the first fingerprint: 0x4D + 0x58 + 0x30 + 0x02 + 0x40 + 0x31 + 0x48

4 Press finger again, and module will respond as operation successful after processing: 0x4D + 0x58 + 0x30 + 0x02 + 0x40 + 0x31 + 0x48

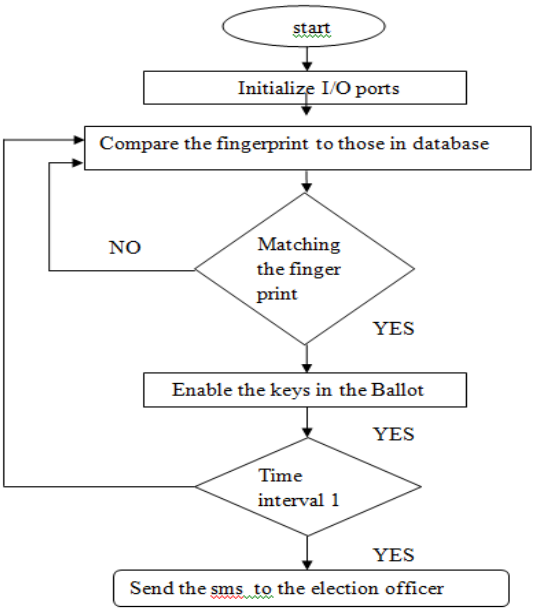

Fig 2 : Flow Chart

V. FINGER PRINT VERIFICATION

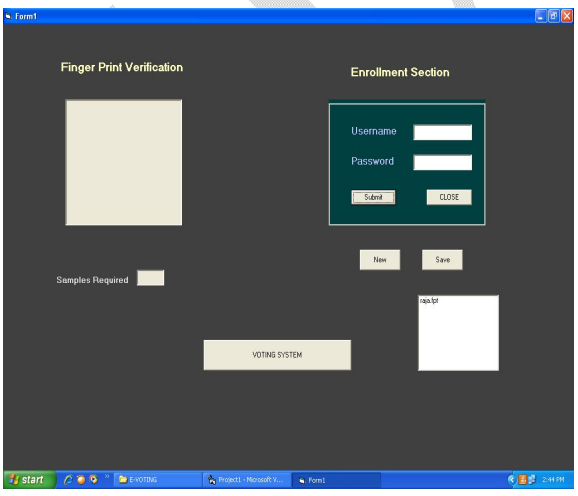

Fig 3: Finger print verification window

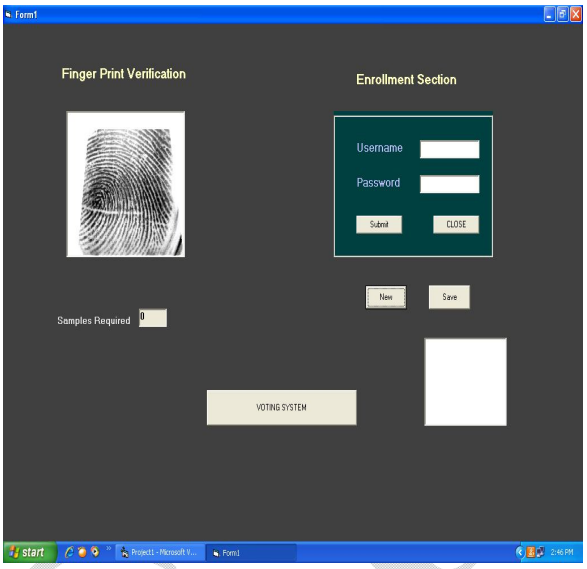

Fig 4 : Casting the fingerprint template

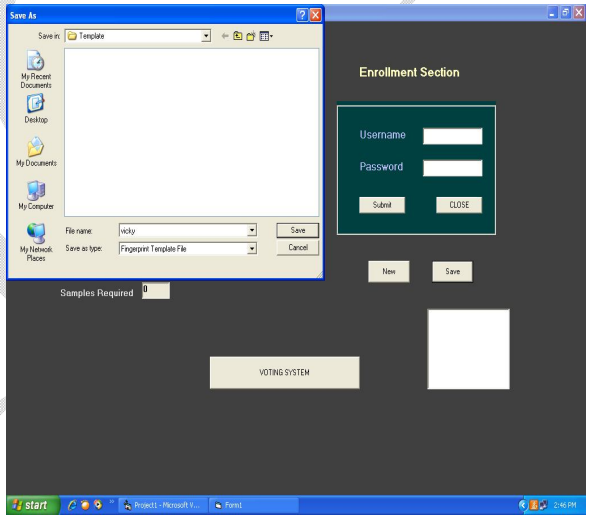

Fig 5: Saving the finger print template

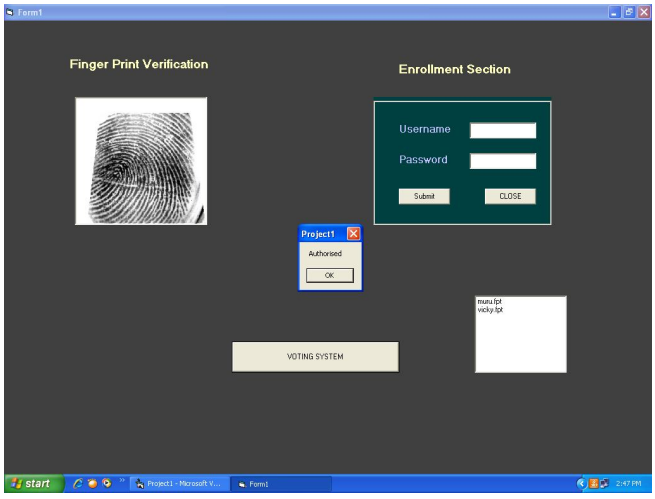

Fig 6 : Voting system window

ISSN 2348 – 9928
Doi:01.0401/ijaict.2014.03.20 Published Online 05 (10) 2015

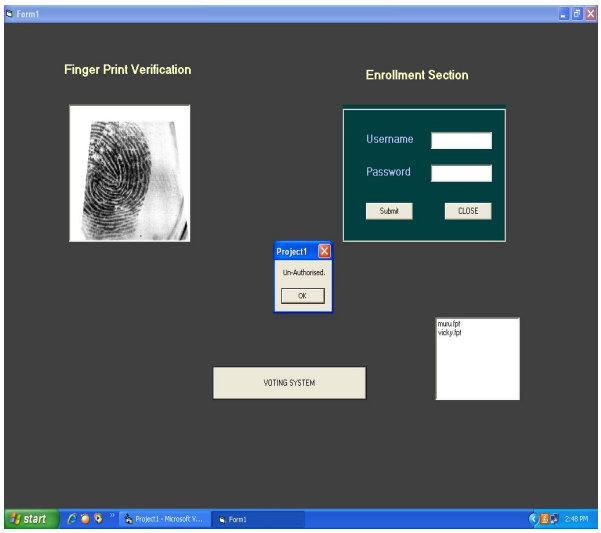

Fig 7 : Voting system window

Table 3 : Result

Sr.No.	No. of Party	No. of Votes
1	BJP	0
2	CONGRESS	0
3	SHIVSENA	1
4	MNS	0

SEND MESSAGE TO THE CENTRAL OFFICER

VI. PROPOSED MODEL

We proposed an internet and GSM mobile voting scheme, where the GSM and the internet authentication infrastructure is used to provide voter authentication and improve voter mobility.

Authentication is always a difficult requirement to fulfill for remote voting schemes, most of which apply a public-key based signature scheme for voter authentication. In this scheme, by using the existing GSM and internet authentication infrastructure, the public-key overhead is largely reduced. This scheme also enhances the security and provides more mobility and convenience to voters.

Where the voters' privacy is protected by applying a blind signature scheme. In this paper, we presented the basic structure and protocol of our GSM and internet based mobile voting system. However, further work is needed to address the importance place in the trust on the AC, and this are therefore investigating options for enhancing and extending the GSM and internet mobile voting scheme. In future work, it will discuss end-user device (ME) and application security. It will also address how the voters obtain the voting application and solutions to provide the integrity of the voting application running on the ME. The Trusted Platform Module and smart card solutions will be considered.

First of all, in 2003, 60% of France citizens prefer internet voting to paper voting. This indicates that more and more people intend to vote though their own electronic devices. Secondly, the usability study run by professors from the University of Maryland indicates that Audio-only mode of Diebold machine has some problems such as the keypad mapping is inconsistent and delays make the audio quality pretty bad.

The idea of Designing Audio-only system is fantastic for the people with disabilities but technically developers should improve the audio quality for the Diebold machine. Thirdly, there is no significant solution for the people with disabilities using online voting system. Since the internet voting system will get more and more popular, the accessibility of system still needs to be improved. Fourthly, the electronic voting systems should try to be free and open source to users. Last but not least, some internet voting systems such as ADDER does not offer to a voter a method for physically verifying if this voter actually submitted the vote by him/herself or this was her/his actual choice. Hence, solving this complex problem will be challenging

The application for this electronic voting system by using GSM mobile technology and internet is only for casting vote.

Advantages:

- This makes vote counting and result tabulation faster and more accurate. Although any election can be conducted using hand counted paper ballots, these two categories of elections can require time-consuming, costly, and error-prone hand counts.
- The introduction of electronic voting would motivate the younger generation to take an interest in voting, as they are more likely to vote in this way.
- This technology combats common Indian electoral fraud problems, such as capturing polling places or stealing ballot boxes.
- Equally, mention that some people cannot be bothered to go to a polling station particularly if it is far away, and that this is when alternatives such an electronic voting are most important.
- Many complain that the presence of candidates and canvassers at polling stations is irritating and too much of an attempt to influence voters' choice. This will not happen in electronic voting system.
- This voting system will bring the voter to vote from any places other than his or her home town for example a military person can cast his vote, a student who is studying far from his place can cast vote.

- Accuracy of counting is one of the main advantage of this system.
- It reduces figures by making spoiled ballots impossible and unintentionally blank ballots difficult.
- Proxy vote or double voting is not possible.

Limitations:

- Illustrate that the idea of a polling station is familiar and proven to work, as well as being simple and easy to understand.
- Electronic voting is still much more in the trial stage than postal voting, and has not been tested so extensively. It is also said to be more problematic.
- It is argued that many voters find electronic voting confusing or too much of a change.
- These technologies also allow for more sophisticated voter interfaces, potentially resolving many voter access problems for those with disabilities or those using minority languages. Visual interfaces may also be useful for illiterate voters, but this presumption has not been rigorously tested in environments with little computer literacy.
- Any computer program can have an undetected, unintentional error (a "bug"). Any computer program can be changed by malicious programming ("hacked") in a way that is undetectable after the fact. This is true of all manufacturers and, in fact, of all computer software.
- The cost and complexity may well make E-voting prohibitively expensive, especially for relatively simple elections. The cost for the equipment of voting is high this give a main problem to those remote people who have not even a mobile equipment

VII. CONCLUSION AND FUTURE WORK

We proposed a GSM mobile voting scheme, where the GSM authentication infrastructure is used to provide voter authentication and improve voter mobility. Authentication is always a difficult requirement to fulfill for remote voting schemes, most of which apply a public-key based signature scheme for voter authentication. In our scheme, by using the existing GSM authentication infrastructure, the public-key overhead is largely reduced. Our scheme also enhances the security and provides more mobility and convenience to voters. Where the voters' privacy is protected by applying a blind signature scheme. In this paper, we presented the basic structure and protocol of our GSM based mobile voting system. However, further work is needed to address the importance we place in the trust on the AC, and we are therefore investigating options for enhancing and extending the GSM mobile voting scheme. In future work, we will discuss end-user device (ME) and application security. We will also address how the voters obtain the voting application and solutions to provide the integrity of the voting application running on the ME. The Trusted Platform Module and smart card solutions will be considered. Even the best election observation cannot solve the transparency problems with Electronic voting by using internet and GSM described above. However, good election observation can review system design and, perhaps, undertake extensive technical validation of a prototype terminal. Such efforts may be important if election results are contested, but they are unlikely to be determinative. The procurement of ballot boxes or ballots from a given supplier in a given election does not bind the electoral authority to the same supplier for future elections. this technology, however, is not "mix-and-match." Procurement from a given supplier binds the electoral authority's future decisions, perhaps becoming a point of unhappiness if the donor reduces its commitment over time.

References

[1] Koichiro Niinuma, Unsang Park and Anil K. Jain, "Soft Biometric Traits for Continuous User Authentication," IEEE Transactions on Information Forensics and Security, Vol. 5, No. 4, pp. 771-780, Dec. 2010.

[2] Anil K. Jain, Patrick Flynn and Arun A. Ross, "Handbook of Biometrics," Springer Science, ISBN-13: 978-0-387-71040-2, 2008.

[3] http://eci.nic.in/eci_main1/index.aspx.

[4] http://www.bravenewballot.org/e-voting-in-india.html.

[5] Assimo Tistarelli, Stan Z. Li and Rama Chellappa, "Handbook of Remote Biometrics for Surveillance and Security," Springer Science, ISBN 978-1-84882-384-6, 2009.

[6] Sonja Hof, "E-Voting and Biometric Systems," University of Linz, Austria. ISBN 978-1-848-384-6, 2013

[7] Dimitris A. Gritzalis, "Principles and requirements for a secure e-voting system," Computers & Security, Vol. 21, No 6, pp. 539-556, 2002.