Study of Existing Indian Voting System and Implementation of Hybrid Design using Biometric Security in Voting Authentication Process

Syeda Afrasheem Begum
Post Graduate Student
PDA Engineering College
Kalaburagi, Karnataka

Geeta Hanji, PhD
Professor
PDA Engineering College
Kalaburagi, Karnataka

ABSTRACT

Voting is an integral part of a democratic society. It is a decision making mechanism and security plays an important role in voting. In order to ensure high security, voting machine should be designed and developed with great care. According to Election authorities of India, paperless electronic voting systems are suffering from much vulnerability. By accessing the machines Election insiders and fraudsters are altering the election results. There is a need of voting system which is robust and secure. Here, an idea is proposed to upgrade the present voting system that is based on biometric traits (Iris, Fingerprint) of voter which are saved in a government database as Aadhar (U-id) number database. But one cannot have access to Aadhar (U-id) number Data base since it is a govt. Stored data base. So, a virtual data base is created here which is called as RFID number data base. This RFID number data base resembles the Aadhar (U-id) number data base. This data base includes the biometric traits of Voters. These biometrics traits provide secure and feasible authentication to the voters, thus preventing the fraud and illegal voting.

General Terms

Finger Print Recognition, Iris Recognition, Security, and Authentication.

Keywords

Aadhar, RFID, Biometrics, GUI

1. INTRODUCTION

Voting is an important process, through which people elect its government. Voting is shifting from manual paper-based processing to automate electronic-based processing .In “electronic voting” or “e-voting”, the voting machine is made up of some electronic means to ensure the security, reliability, guarantee and Transparency. Security is the heart of e-voting process. Therefore it is very important to design an e-voting system with great security methods. Mechanisms involving security can be inconvenient and time-consuming. A voting system must be designed which is less time consuming and convenient.

2. LITERATURE SURVEY ON VOTING TRENDS IN INDIA

Before 2004 there was a paper based voting system. This is called as ballot Paper system. Voters had to go to polling booth and cast their vote by marking on seal in front of the symbol of a candidate for which they wanted to cast their votes on ballot paper. Results were announced by counting the votes. The maximum vote gainer was declared as winner. India has population more than 120 crores the ballot paper voting is not much reliable, time consuming and very difficult to count the vote and there are also problems like replacement of ballot paper boxes with duplicate, damage of ballot paper, marking stamp seal for more than one candidate hence there is a strong need to overcome these problems. In order to overcome these problems Electronic Voting Machines Were introduced.

Electronic Voting Machine (EVM’s) mainly consists of two components:

1. Control Unit: It Stores and assembles votes, used by poll workers
2. Ballot Unit: It is placed in the election booth and is used the voters

Both the units are connected via 5m cable and one end of the cable is permanently fixed to ballot unit. The control unit has a battery pack inside, which motorizes the system. The ballot unit has 16 candidate button and the unused buttons are covered with a plastic masking tab inside the unit. An additional ballot unit can be connected when there are more than 16 candidates. The additional ballot unit can be connected to a port on the underside of the first ballot unit. EVM’s are internationally known as DRE’s (Direct recording Electronic). EVM’s are universally used in India since the general elections of 2004, when ballots were completely out of trend. They have been used in all the assembly polls and general elections of 2009. By using EVM’s, Votes are correctly recorded and there is no problem in counting, scalability, Accuracy, fast declaration of results and robustness of system. Main Problem lies in authentication, the person who is voting may not be the legitimate person. Other problems like capturing of booth by political parties, casting of votes by underage people and fraud voting may occur. A person is provided with the voter id card as a proof of identity, issued by Indian government .Lot of problems are seen in voter id cards like name misprinting, missing of name, no clear photo on photo id card, etc

3. ISSUES WITH PRESENT VOTING SYSTEM IN INDIA AND SECURITIES REQUIRED IN A VOTING SYSTEM

Several studies have been done on using computer technologies to improve elections. These studies tells about the risks of adopting electronic voting system, because of the software challenges, insider threats, network vulnerabilities, and the challenges of auditing.

3.1 Problems encountered during the usual elections are as follows

1. Validation of voters done incorrectly.
2. Polling Booths are captured.
3. Altering of election results by accessing the machines By insiders and frauds to alter.
4. The voters find the event boring and time consuming, Resulting in to a small number of voters.
5. Deceitful election mechanism.
6. No procedure to ensure the transparency to verify the votes Casted by the voters.

3.2 Different Stages of Election

1. Registration
2. Authentication
3. Vote Casting
4. Vote Tallying

3.3 Security requirements of e-voting system

1. Eligibility: only the legitimate person should be able to vote.
2. Authenticity: only the authorized person should be able to vote.
3. Uniqueness: No voter should be able to vote twice.
4. Accuracy: Recording of votes should be done correctly.
5. Integrity: Number of casted votes should not be altered.
6. Fairness: Incomplete tabulation of results should not be done.
7. Reliability: Systems must work robustly with greater assurance by minimizing the errors.
8. Confidentiality: Data should not be leaked.

4. PROPOSED SYSTEM

To overcome the above stated problems a new system is proposed which is time saving and provides more security. It provides 3 stages of authentication by electronic means, based on individual biometric traits of voters. The new system makes use of biometric traits of the voter for verifying the authenticity of the voters at the time of election. If scanned biometric data of the voter matches with the saved data, then he/she is allowed to vote, otherwise rejected and reported as fake voter. Every individual has unique Biometric properties like fingerprint, iris, gaits, voice, face etc. This cannot be matched with anybody. Finger prints, face images and iris samples are saved in national Aadhar.

4.1 Biometrics:

A biometric system automatically recognizes an individual based on unique feature or characteristic possessed by the individual. Biometric systems have been developed based on fingerprints, facial features, voice, hand geometry, handwriting, the retina and iris.

4.2 RFID Card

RFID number stands for radio frequency identification number. Here, it is only issued to those with the Aadhar card and hence this RFID Card is considered as a Secondary Aadhar card. This is because the government data base is stored in central server and one cannot have access to the data of central server. It requires special permissions from state or central government and also involves other issues. Therefore, a virtual data base is created by collecting the samples of Biometric traits of people, which is nothing but RFID data base. This stored RFID database can be compared with the presently scanned samples of databases for verifying the authenticity of the voters. The cards used here are Active RFID cards through which one can perform both read as well as write operations. RFID card works on the principle of Mutual Inductance.

4.3 Proposed System Design

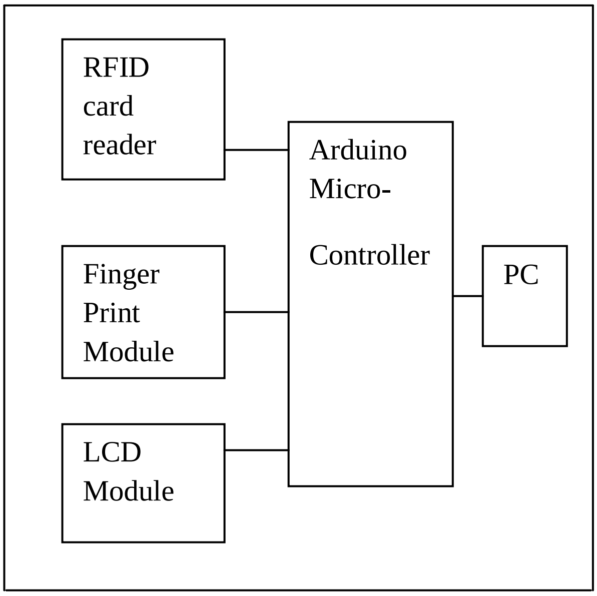

Fig 1: Block Diagram of the Proposed System

4.4 Description

Firstly, The PC and the machine are connected Via USB Cable. The machine gets started after this connection and a waiting message is displayed on the LCD.

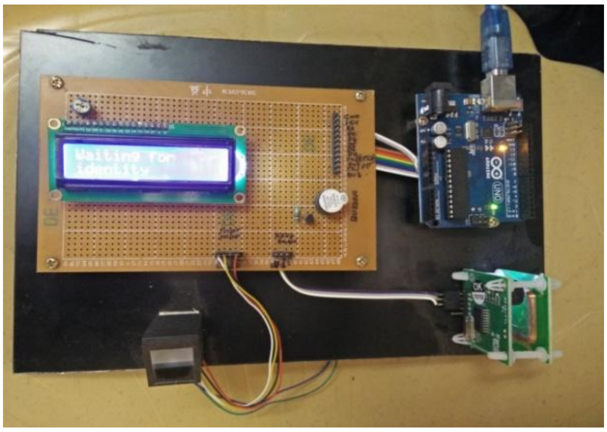

Fig 2: Displaying a waiting message before the first level of Authentication

At the first level, age of the voter is verified to ensure that the voter is an eligible person. A code is implemented in Arduino language of microcontroller which performs RFID card reading and displays the relevant Messages on LCD screen. Firstly, when the voter taps the card on RFID Card Reader Module, the RFID reader module sends the data obtained from the RFID card to the microcontroller. In this way serial communication is established between the microcontroller and the RFID reader. The microcontroller accesses the previously stored data in its memory. Then presently taken data and stored data are compared. A welcome message is displayed if a voter is a valid voter. This is the first level, which verifies the age of the voter by reading the data from the RFID card of the voter.

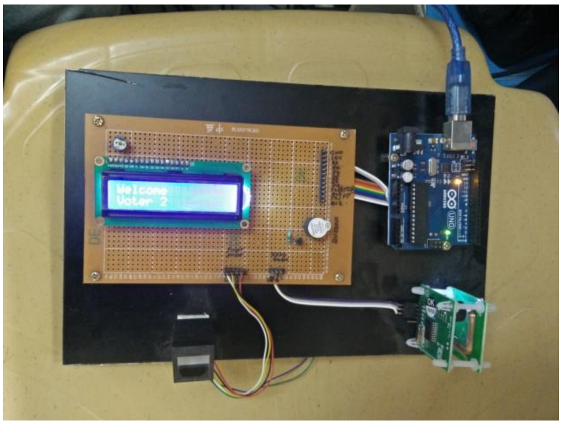

Fig 3: Initialization of first level of authentication

At the second level of authentication, the voter will be subjected to finger print recognition system. A code is implemented in Arduino Platform which performs Finger print recognition. A voter is subjected to Fingerprint recognition system, the Finger print Module Scans the finger of a voter. If this finger print matches with the previously stored one, a message is displayed on the LCD screen -"Level 2 passed".

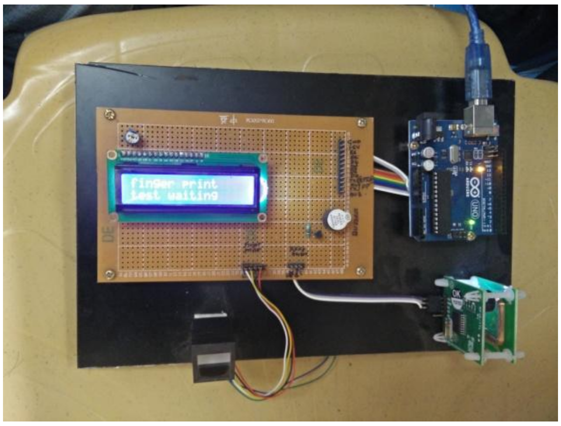

Fig 4: Initialization of second level of authentication

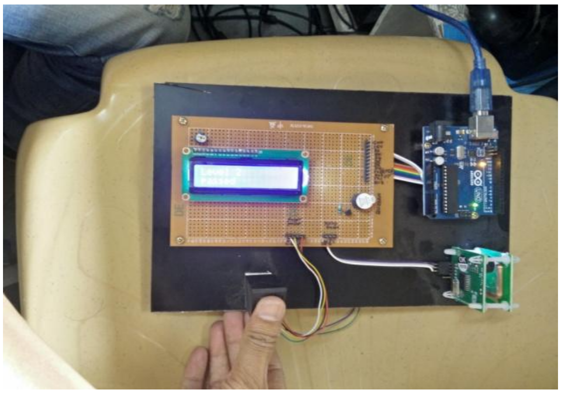

Fig 5: Completion of Second level of Authentication

At the third stage, the voter is subjected to Iris recognition System to validate all the details of the voter in case of any discrepancy found in the photo due to ageing etc. This way we can rule out the fraud voting.

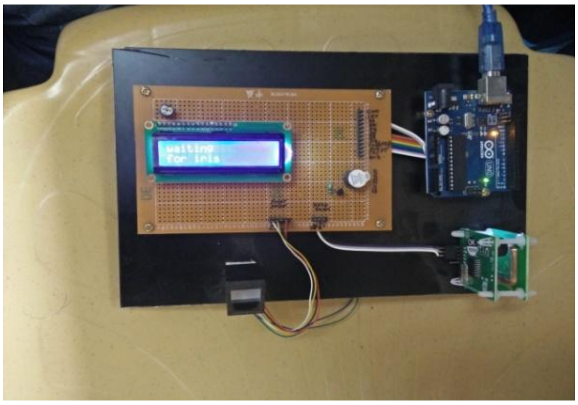

Fig 6: Initialization of Third level of Authentication

4.5 Flow chart for Iris Recognition

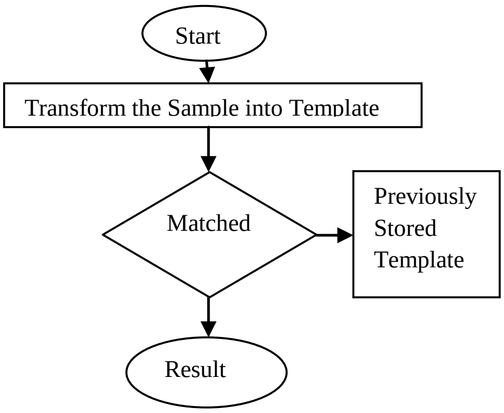
Start
Transform the Sample into Template
Matched
Previously Stored Template
Result

Fig 7: Flow Chart

4.6 Embedding Iris Recognition and Proposed Algorithm

The task can be accomplished as follows:

Designing of Iris recognition code in MATLAB, i.e. Recognition of Human Iris Pattern for Biometric Identification and obtaining the result of comparison in the form of GUI. Finger print recognition can also be done similarly

Iris Matching in MATLAB:

Step 1: Implement a code in MATLAB which performs iris recognition and finger print recognition.

Step 2: Draw a GUI (Graphical User Interface) in MATLAB. Write the appropriate call back codes. The following window will open:

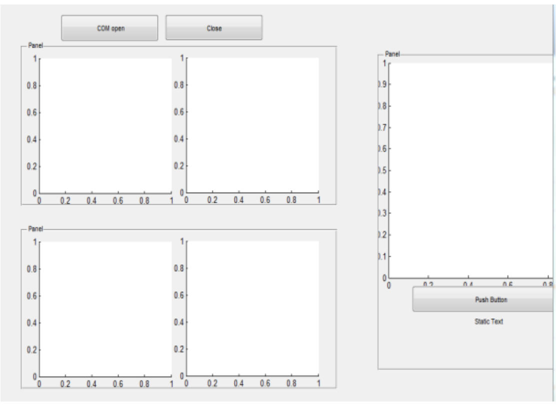

Fig 8: GUI in Mat lab

Step 3: Now browse camera image and the image from database (previously stored).

1. If the two are same, the result will be "MATCHED", as can be seen in the following window:

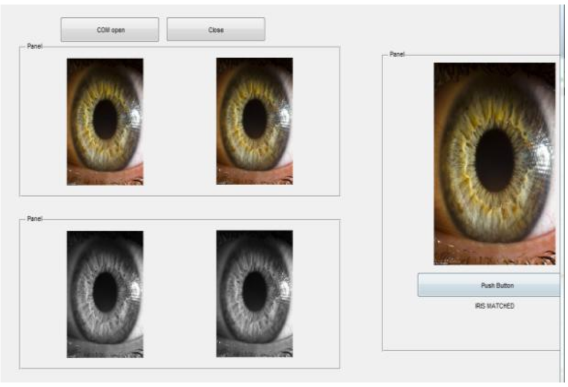

Fig 9: Iris Comparison

2. If the images are not matched, then the result will be "NOT MATCHED" as in the following window. [1]1

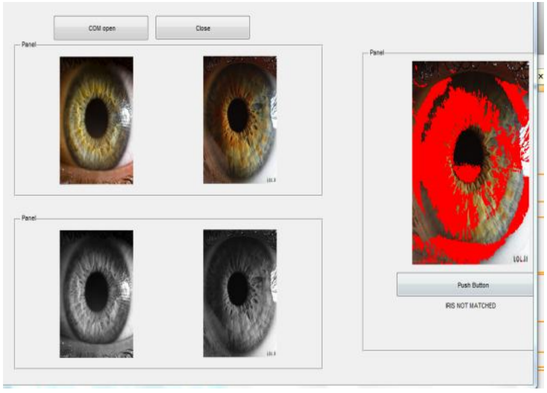

Fig 10: Iris Comparison

If the voter passes all the 3 stages of authentication then the voter is considered as a valid voter and it is displayed on the LCD Screen and can proceed for voting.

5. CONCLUSIONS

The proposed system provides best solutions to the problems related to the Indian voting system but, it is vulnerable to security attacks. Confidential biometric data may be leaked due to network connectivity or system hacking. Full implementation is not an easy task; it involves political issues, financial issues and regional issues. Illiteracy is the main hurdle in this project to come true because for illiterate persons this is not easy to work with machine interface.

6. FUTURE SCOPE

Other biometric traits may be added for making the method more robust in terms of security as one get time-and-cost effective solutions with the advancements in technology. The voting system can also be made flexible in terms of being able to be operated from anywhere in the country through online procedures.

7. REFERENCES

[1] Diponkar Paul and Suboj Kumar Ray, Member IACSIT, Vol. 3, No. 2, March 2013, "A preview n microcontroller Based electronic Voting machine", International journal Of Information and Electronics Engineering.

[2] D. Balzarotti, G. Banks, M. Cova, V. Felmetsger, R. A. Kemmerer, W. Robertson, F. Valeur, and G. Vigna, vol.36, No. 4, 2010. "An Experience in Testing the Security of Real-World Electronic Voting Systems", IEEE Transactions on Software Engineering.

[3] A. Villafiorita and K. Weldemariam, and R. Tiella, vol. 4, No. 4, 2009. "Development Formal Verification and Evaluation of an E-Voting System with VVPAT", IEEE Transactions on Information Forensics and Security.

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

[5] Anil K. Jain, Arun Ross and Salil Prabhakar, Vol. 14, No.1, January 2004. "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems For Video Technology, Special Issue on Image- and Video Based Biometrics.

[6] Anil K. Jain and Umut Uludag, Vol. 25, No. 11, pp.1094-1098, Nov 2003. "Hiding Biometric Data", IEEE Transactions on Pattern Analysis and Machine Intelligence.

[7] http://uidai.gov.in/aadhaar.html

[8] S. Prabhakar, S. Pankanti, and A. K. Jain Vol. 1, No. 2, pp.33 -42, 2003 "Biometric Recognition: Security and Privacy Concerns", IEEE Security and Privacy Magazine.

[9] J. L. Wayman, Vol.1, No. 1, pp. 93-113, 2001, "Fundamentals of Biometric Authentication Technologies" International journal of Image and Graphics.

[10] L. Hong, A. K. Jain, and S. Pankanti, ProcAutoID'99s, Pp.59-64, Oct 1999 "Can Multi Biometrics Improve Performance"? Summit (NJ), USA.