JSPWN

Journal of Signal Processing and Wireless Networks

Secured e-Voting System

Anitha.A, Ishwarya.D, Janani.S,Jagadeeswari.M
Department of Electronics and Communication Engineering, Sri Ramakrishna Engineering College, Coimbatore, India.
**Corresponding Author email : hod-ece@srec.ac.in*

ABSTRACT

Voting is the process by which democratic countries determine their government .Hence, Voting systems are more important than other critical systems .There are lots of methods to avoid duplicity in voting system, but we are not able to eradicate it completely. This paper determines the biometric scenario, where a person is authenticated at the voting booth by being verified by a camera. The application scenario is to avoid fake votes and to get larger security in voting process. Here, the image of the person is captured and tested with the database image to provide high security in voting.

ARTICLE HISTORY Received 10 November 2017 Revised 25 January 2018 Accepted 02 February 2018

KEY WORDS Raspberry Pi, Voting Machine,Face Recognizer

1. Introduction

An electronic voting (e-voting) system is a voting system in which the election data is recorded, stored and processed primarily as digital information. It uses an electronic means of casting and counting votes. Some of these advantages are lesser cost, faster tabulation of results, greater accuracy, and lower risk of human and mechanical errors. It offers improved accessibility for the people with disabilities, and it provides multiple-language support for the ballots. Electronic voting is gaining in popularity around the world. Electronic voting is a term that may encompass several different types of voting, embracing both electronic means of casting a vote and electronic means of counting votes.

A reliable cost effective secure electronic voting system is one that can be used in a cost effective way. The important obstacle in any e-voting system across the world is the security issue. Election's results may be modified when delivered to the Higher Elections Committee, unauthorized voter may vote instead of the eligible voter, a vote may not be calculated; also the voter has to ensure that nobody has the possibility to know his ballot data. The proposed Voting Model System overcomes these obstacles. Security evaluation experiments are performed successfully to the proposed system proving that it satisfies privacy, accuracy, reusability, eligibility and integrity. Voting systems have evolved from paper ballots to electronic voting (E-voting) applications, We have noticed significant efforts to develop real-world securer solutions. E-voting systems are security-critical systems that require early identification of security requirements and controls based on the analysis of potential vulnerabilities, threats, attacks, and associated risks. General purpose modelling languages and current tool support to model security concerns exist. However, they lack a comprehensive solution that includes tool support for verification of security goal completeness and risk analysis in specific domains. Also, communication between stakeholders in large-scale systems is difficult, specially because security is not the core skill of many requirements engineers.

2. Objective

Voting is to allow voters to exercise their right to express their choices regarding specific issues, pieces of legislation, citizen initiatives, constitutional amendments, recall and/or to choose their government and political representatives. The system uses facial pattern for voter identification and allows the authenticated person to cast vote.

3. Outline of this paper

The Raspberry Pi is a credit card sized single computer or SoC uses ARM1176JZF-S core. SoC, or System on a Chip, is a method of placing all necessary electronics for running a computer on a single chip. It needs an Operating system to start up. SD card will acts as a bootable hard disk. A camera will be used to take picture of citizen's national ID card and identify that this user is valid voter for that region. If the citizen is valid and also didn't vote then the person will be allowed to submit his/her vote. Each voting machine is locked by face recognition access module. As the user is identified his/her facial appearance will be sent to a specific machine for voting. Each voting machine is networked with the central raspberry pi voting identification system.

4. Existing system

Existing system is manual one in which the person who has to cast their vote will be having an identity card(Voter ID) for their reference to the government and only then the person is allowed to vote in the booth. By this way one could prepare the duplicate ID and could cast fake votes too. It is very difficult to maintain.

5. Proposed System

Biometric is the science that tries to get human biological features with automated machines to identify the authenticate. By the use of biometric products one can eliminate the need for password or PINs. It makes comfortable and fast to record features. The analysis of human data with facial patterns, fingerprints, and retina are called as Biometrics. Initially the application was focused only on high end consumers like government, defence and airport security. Nowadays, it became more commercial. Some of the commercial applications are personal computer login security, employee recognition, time and attendance system.

In this technique, the image of the voter is stored in database. By using this database technique one could vote only once and no misplacement of votes occurs. At the time of elections, for the recognition purpose web camera is used. Face recognition could also be an honest choice in e-voting systems, where you can provide an users adequate explanation and accuracy in voting.

One of the most challenging problem in face recognition deals with an appropriate separation of the data from the same data type. The goal is to implement a machine that is supported by the system that recognizes the person's identity in the database and allows him/her to vote. This can have the various applications such as automated person identification, recognition of gender, age, emotions etc.

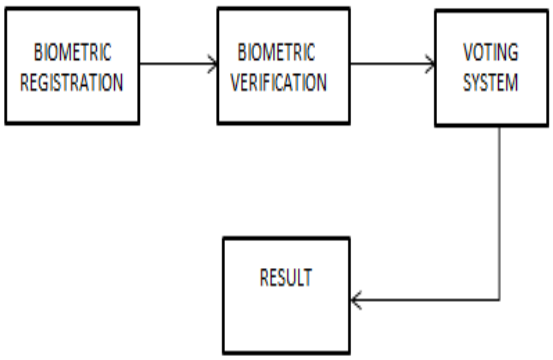

Fig.1 Biometric electronic voting Architecture

Biometric Registration: The process of capturing an eligible voter's image which is used to verify the image which was captured to the image stored in the database for the authentication or for a verification process.

Biometric Verification: A face recognition system operates either in verification mode or in identification mode. The current image will be verified with the image in the database and the result will be provided by accuracy.

Voting System: Here, if the images are matched then the system allows the person to poll his/her vote.

Result: The accurate result will be provided to an organization so that the voting process can be done in a fine and secured manner.

6. Methodology

Images of the each person who is eligible to vote are captured and stored in the database. In the polling booth there will be a web camera, which captures the image (face) of the voter and will compare this particular image to the images which are already stored in the database. A comparison algorithm is loaded into the raspberry pi, which in turn will match the image of the person to the image provided in the database, the LED will glow and the person may proceed the voting. If there is any mismatch in the captured image, the buzzer starts to alarm.

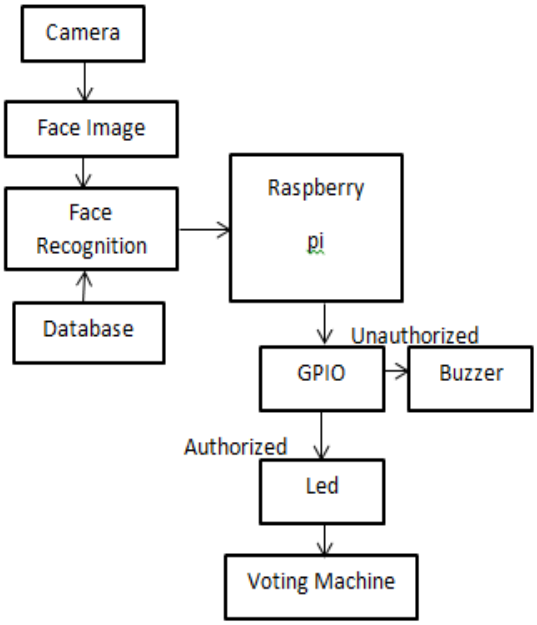

Fig. 2 Block Diagram of e-voting

The proposed system uses an Local Binary Pattern) algorithm (LBP).

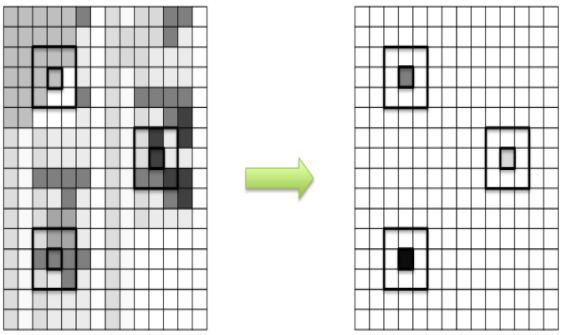

Fig. 3 Grayscale Image to LBP Mask

The LBP value for a pixel in the grayscale image can be calculated by comparing the central pixel value with the neighbouring pixel values. The comparison algorithm will get started from any neighbouring pixel and then it can transverse either in clockwise or anti-clockwise direction but the same order must be used for all the pixels. The comparison will be performed by consideration of the central pixel and neighbouring 8 pixels.

If the current pixel value observed by the webcam is greater or equal to the neighbouring pixel value, then the corresponding bit in the binary array is set to 1 wherein the current pixel value is less than the neighbouring pixel value, the corresponding bit in the binary array is set to 0.

The central pixel value is 32.The neighbouring pixels values are compared with the central pixel value, if the value is greater than the central value then it is marked as 1

else it is marked as 0.It is calculated in counter clockwise direction.

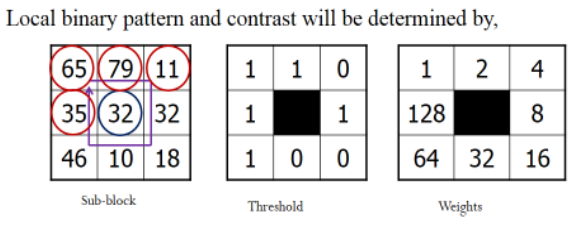

Fig.4 Calculation of LBP values

The LBP value ranges from 0 to 255, so the size of the LBP Descriptor will be 1x256. We then normalize the LBP histogram.

1. Load the colour image.
2. Convert to grayscale image.
3. Calculate the LBP mask.
4. Calculate the LBP Histogram and normalize it.

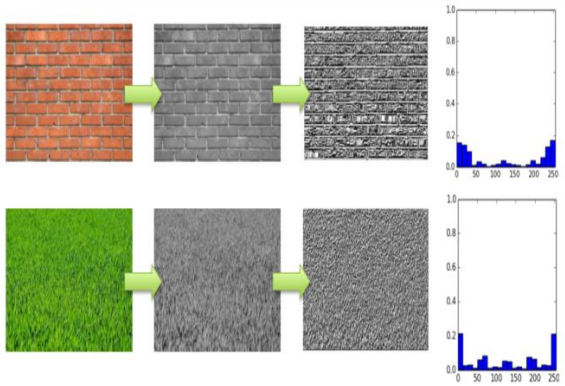

Fig.5 Color Image ->Gray scale Image -> LBP Mask -> Normalized LBP Histogram

Here the implementation of 8 point neighbourhood is used but most of the implementation uses the circular neighbourhood.

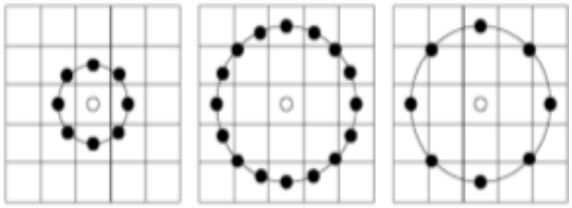

Fig.6 Circular Neighbourhood

7. Analysis of an electronic voting system

A security analysis of the source code to one such machine used in a significant share of the market. Our analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts. We identify several problems including unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes. Any paperless electronic voting system might suffer similar flaws, despite any certification it could have otherwise received. We suggest that the best solutions are voting systems having a voter-verifiable audit trail, where a computerized voting system might print a paper ballot that can be read and verified by the voter.

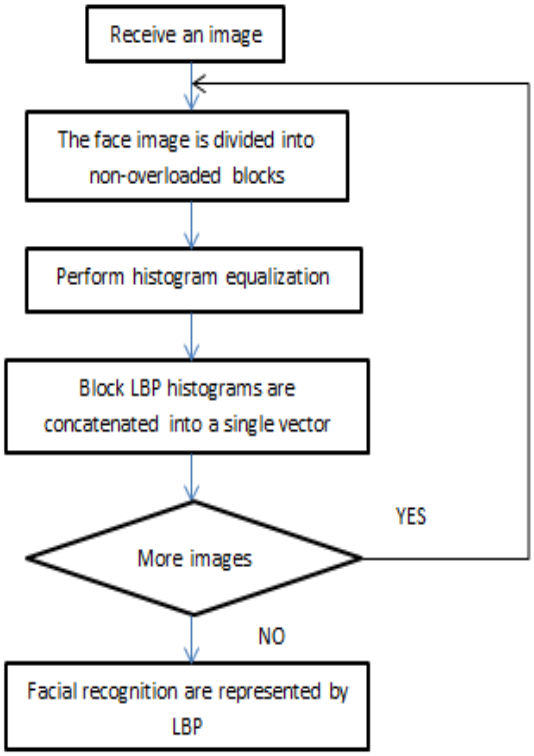

Fig.7 Flow Chart

8. Conclusion

This project is designed using Raspberry Pi microcontroller. The proposed e-voting system is designed especially to solve the cost effective, accuracy and transparency problems in a highly secured approach.

References

1. D. Balzarotti, G. Banks, M. Cova, V. Felmetsger, R. A. Kemmerer, W.Robertson, F. Valeur, and G. Vigna (2010), "An Experience in Testing the Security of Real-World Electronic Voting Systems," IEEE Transactions on Software Engineering, Vol. 36, No. 4, pp. 453-473.
2. A. Villafiorita and K. Weldemariam, and R. Tiella (2009), "Development, Formal Verification, and Evaluation of an E-Voting System with VVPAT," IEEE Transactions on Information Forensics and Security, Vol. 4, No. 4, pp. 651-661.
3. T. Kohno, A. Stubblefield, A. Rubin, and D. Wallach (2004), "Analysis of an Electronic Voting System," Proc. of IEEE International Symposium on Security and Privacy, pp. 27-40.

4. D. Molnar, T. Kohno, N. Sastry, and D. Wagner (2006), "Tamper-Evident, History Independent, Subliminal-Free Data Structures on PROM Storage-or-How to Store Ballots on a Voting Machine," Proc. of IEEE International Symposium on Security and Privacy, pp. 365-370.
5. Khasawneh, M., Malkawi, M., & Al-Jarrah (2008), "A Biometric-Secure e-Voting System for Election Process," Proc. of the 5th International Symposium on Mechatronics and its Applications (ISMA08), DOI: 10.1109/ISMA.2008.4648818.
6. C Circus (2012), "Role of Biometric Technology in Aadhaar Authentication", UIDAI, pp. 01-23.
7. Yinyeh, M. O., and Gbolagade, K. A. (2013), "Overview of Biometric Electronic Voting System in Ghana," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 7, pp. 624-627.
8. Y Bhavan (2009), Biometrics Design Standards For UID Applications, UIDAI, pp. 01-57.

