

Design and development of biometric enabled advanced voting system

¹Prof Jesudas J ²Soujanya D, ³Vedashree G M, ⁴Rachana K R
Department of Electronics & Communication Engineering,
Dr T Thimmaiah Institute of Technology

Abstract: The focus of this project is to design and development of a biometric enabled biometric electronic voting machine. The proposed biometric electoral voting system allows the user to scan fingerprint and iris so that his or her credentials can be compared to existing fingerprint and iris images already stored in the system's database. Counting is going on right away, making the voting process more efficient, faster and safer. This system requires the identification of the voter Aadhaar card, the voter's thumb impression as well as the iris image. Voter's complete data, including all voters fingerprint and iris image, is collected and stored in the database. While voting, the voter gives their Aadhaar card details and puts eye in front of the iris camera and finger inside a fingerprint scanner, the system looks for the seal already provided in the data base, and then compares the iris image to authenticate the voter's identity. If the data matches, the system commands the voter to vote through the electronic voting machine. If the fingerprints do not match, the voting presiding officer looks for the registration, or the iris image does not match after the fingerprint match, the voter is not allowed to vote, consider it vote rigging. Insecurity, rigging and violence continue to mar electoral processes in developing nations. It has been difficult to enforce security and transparency in the voting process. This paper proposes a secure and automated bimodal voting system.

Keywords: *Electronic voting system, iris, fingerprint*

I. INTRODUCTION

Biometric technologies are playing a vibrant role in various security applications. Biometric cannot be shared like Passwords. Finger Print, Iris and the Aadhar Card of the voter will be compared and validated to cast the vote. Finger Print Recognition system is based on the Minutiae feature. Minutiae is defined as Ridge Ending and Ridge Bifurcation. It consists of 2 steps Minutiae Extraction and Minutiae Matching. Finger Prints taken as an input from Finger Print Scanner will be compared with the obtained data and if the match is exceeding a predefined threshold, then finger prints are considered as matched and belonging to the same person. Voting is the most indispensable asset in any democratic country.

It is the process of selecting a suitable candidate to lead the people. A democratic nation is the people's country. Democratic government can only be right when there is provision for a trustworthy and secured electoral process. E-voting is an emerging technology that has improved the traditional method of voting. E-voting with the use of biometric has provided a more secure way of voting in a democratic country compared to the traditional voting where papers are used, and voting is insecure. Biometric is a physical and biological quality of an individual which is different for every person.

There are different types of biometric traits among which are facial recognition, Fingerprint, iris recognition, and palm print. Rigging of elections are still possible in today democratic process because one person could votes more than one. Most of

the system are not biometrically automated and as such would not be able to identify the imposters, who possesses more than one voter's card and as such could do multiply voting. With the application of bimodal biometric, the traits are unique to that right person only and can easily detects and stop imposters.

This project proposes a web-based and secured automatic bimodal biometric electronic voting system. The biometrics was used to identify individuals that are eligible to vote. The proposed method provided likely voters with a unique ID and a token code. The proposed electronic voting system also provided a dependable, transparent. It secured electronic voting system that eliminated the possibility of impersonation by using two biometric traits and automating the voting process to save time. The resulting system had the propensity to improve the integrity factor of the voting process by making it fast, transparent and robust. They developed a web-based voting system using fingerprint recognition. The design proposed was used for a university's presidential election. Four candidates and 40 voters registered for the election. Each voter's particulars, biometric and regular were collected and stored in a database. During the election, the registered voters were able to cast votes over the internet.

II. LITERATURE SURVEY

An election is a formal decision-making process by which a population or society chooses an individual to hold a political office. Elections have been the usual mechanism by which modern representative democracy operates that predates to as early as the 17th Century. Elections are conducted both by public entities such as the government as well as private and business organizations, for example, choosing representatives for the Board of

Directors of a company, professional club leadership and even, used in voluntary associations. Types In most democratic political systems, there are several types or categories of elections that are held which corresponds to the different layers of public governance or geographical jurisdiction. Common types of election categories thus include,

- Presidential Elections.
- Parliamentary Elections.
- Governorship Elections.
- Local Government Elections.

Considering our given domain, that is, within the university political sphere, there are also various types of elections that are conducted based on several criteria that help in delineating the staff of the university into categories such as Academic or Non – Academic, Senior Staff, Cooperative Union, to mention a little. The various ethnic groups in Nigeria also have different methods of electing their rulers (e.g. Obas, Emirs, Igwes, etc.) and/or key office holders in their traditional kingdoms.

III. METHODOLOGY

For the proposed voting method, we use a biometric system that uses multiple sources of biometric behavior [19]. This can be done by combining multiple features of an individual or multiple bio-extraction and matching algorithms running on the same biometrics. This system improves the accuracy of matching the data for the biometric system in the voting process. Since there is no way for any candidate to provoke government-issued biometric records before the election process, we use iris recognition and fingerprint scanning for accuracy and reasonable voting result. A.

Iris Recognition

Iris identification uses pattern recognition techniques based on high resolution and repulsive images of iris in the human eye. Iris is a stable organ throughout its life.

Therefore, it serves as a good biometric for establishing one's identity. Due to margin-of-error and speed, iris recognition is now the most reliable way to verify a person's identity. B.

Fingerprints Recognition

The human fingerprint is unique to each individual and is considered a kind of signature and verifies the identity of the individual [9]. It is one of the oldest and most widely used forms of biometric identification. A hill is defined as a single curved section, and a valley is the area between two adjacent ridges. The Ridge Flow model provides 18 minutes of detection features, such as local stops.

IV. IMPLEMENTATION

Registration

This is a register page where voters, candidates and election commission officials can register themselves. These should provide the best basic information on what is known. All information entered on the website is stored in the relevant database. The Election Commission official has the right to accept a qualified consumer and a suitable candidate, otherwise he / she has the right to refuse their registration.

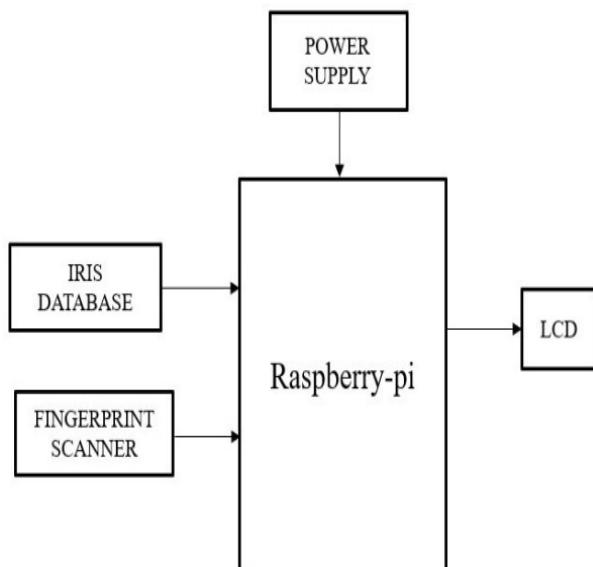


Fig 1: Block Diagram for proposed system

V. RESULT AND ANALYSIS

Procedure for authentication of fingerprint

1. Enroll
2. Detect
3. Delete

```

Fingerprint templates: [1, 2, 4, 7]
1) enroll print
2) find print
3) delete print
-----
>
    
```

Fig 2: To authenticate fingerprint

```

> 1
Enter ID # from 1-127: 9
Place finger on sensor.....Image taken
Templating...Templated
Remove finger
Place same finger again.....Image taken
Templating...Templated
Creating model...Created
Storing model #9...Stored
    
```

Fig 3: Enrolling a fingerprint

```

> 2
Waiting for image...
Templating...
Searching...
Detected # 9 with confidence 63
-----
    
```

Fig 4: Detecting the fingerprint

```

> 3
Enter ID # from 1-127: 9
Deleted!
-----
Fingerprint templates: [1, 2, 4, 7, 8]
1) enroll print
2) find print
3) delete print
    
```

Fig 5: Deleting the fingerprint

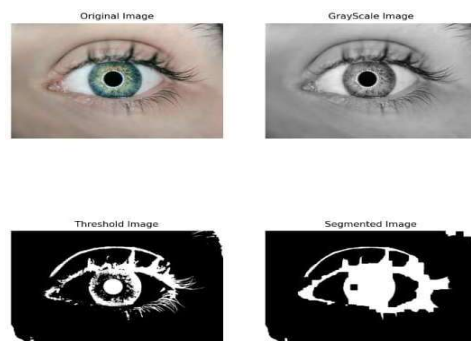


Fig 6: Iris segmentation

VI. CONCLUSION

Electronic voting machines in India are currently unsafe. There are many security issues in the system. The present design of EVM shows the optimal and unbiased result for the public for purely security purposes. The review suggested in this paper is a very secure biometric test voting machine. We have been able to get popular votes with the help of different sensor technologies, databases, and using some IoT in the voting machine, it can develop a better system to detect the biometric mis-match at all booth, which creates alert in polling booth as well as the polling boards can communicated for the same.

REFERENCES

- [1] Samarth Agarwal, Afreen Haider, "Biometrics Based Secured Remote Electronic Voting System". *IEEE Conference*, Sep 2020.
- [2] P.M.Benson Mansingh, T. Joby Titus, "Biometric voting system using RFID Linked with the Aadhar database" *IEEE Journal*, august 2020.
- [3] S Jehovah Jireh Arputhamoni, Gnana Saravanan "Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection Image Processing" *IEEE Conference*, May 2021.
- [4] Suresh Kumar, Tamil Selvan G M, "Block chain Based Secure Voting System Using Lot", *IEEE Journal*, Jan 2020.
- [5] Hanzhuo Tan, Ajay Kumar, "Towards More Accurate Contactless Fingerprint Minutiae Extraction and Pose-Invariant Matching" *IEEE Conference* 2020.
- [6] Chandra KeerthiPothina, AtlaInduReddy "Smart Voting System using Facial Detection" *IEEE Journal*, April 2020.
- [7] Chengsheng, Yuan, Zhihua, Xia, "Fingerprint Liveness Detection using an improved CNN with image Scale Equalization" *IEEE Journal* 2019.
- [8] Anurag Chowdhury, Simon Kirchgasser, Andreas Uhl, Arun Ross "CNN Automatically Learn the Significance Of Minutiae Points for Fingerprint Matching?" *IEEE Conference*, Mar 2020.
- [9] 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.
- [10] 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.
- [11] California Internet Voting Task Force. "A Report on the Feasibility of Internet Voting", Jan.2000.
- [12] Chaum D., "Secret-ballot receipts: True voter-verifiable elections", *IEEE Security and Privacy* 38-47, 2004.
- [13] Darcy, R., & McAllister, I., "Ballot Position Effects", *Electoral Studies*, 9(1), pp.5-17, 1990.