International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 12 | December - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Fingerprint Voting System

Shailja Sharma
Dept of Computer Science and Engineering
Chandigarh University
Gharuan, Punjab,India
shailjasharma707@gmail.com

Abhay Yadav
Dept of Computer science and engineering
Chandigarh University
Gharuan, Punjab ,India
abhayyadavabhay1404@gmail.com

Prince Kalia
Dept of Computer science and engineering
Chandigarh University
Gharuan, Punjab ,India
princekalia91@gmail.com

Saurav Singh
Dept of Computer Science and Engineering
Chandigarh University
Gharuan, Punjab, India
sauravS091@gmail.com

Ritesh Sinha
Dept of Computer Science and Engineering
Chandigarh University
Gharuan, Punjab, India
Sinha.ritesh3211@gmail.com

Abstract

It represents a cutting-edge approach to modernizing the electoral system for enhanced security and reliability. Building upon the "FINGERPRINT VOTING SYSTEM," that
incorporates advanced biometric technologies, including fingerprint and iris recognition. The primary objective is to eliminate issues such as inappropriate voting confirmation, vote duplication, and illegal casting of votes. The process begins with voter registration, where voter details and biometric data are collected, ensuring a comprehensive database. During the voting process, voters' fingerprint and iris data are compared with stored values. If both biometric data match, the individual is granted the opportunity to cast their vote. This dual biometric authentication adds an additional layer of security to the election process, minimizing the risk of fraudulent voting. Furthermore, our system utilizes IoT technology to securely store voting data in the cloud, eliminating the need for physical storage and reducing the risk of manipulation by unauthorized individuals. The data is collected and calculated automatically, allowing for real-time result updates. By the end of the day, the election results are displayed via IoT, ensuring transparency and efficiency.

Keywords: Iris and Fingerprint scanner, Fake votes, Digital image processing, Arduino, Safety.

1. Introduction

Voting is when people choose their leaders. In India, a big democratic country, voting happens not just for government but also for schools, banks, and other places. This study looks at something called "biometrics," which is about using things like fingerprints, eyes, or your face to check who you are. This helps make voting safe and quicker. Biometrics has two main ways of checking. One way is to compare what you give with just one thing in the computer. The other way looks at many things in the computer and sees if what you give matches any of them. This study mostly talks about fingerprints. Each person's fingerprint is different, like a special signature. We can use fingerprints to check if you're the right person. Online voting, where you can vote from anywhere, is becoming more common in India. It's faster and easier. In the old days, voting used paper and took a long time. Even after electronic
machines came, there were still problems. This study wants to fix those problems. It will use your fingerprint and check it with a special database to make sure you're the right person. If someone tries to vote more than once, a buzzer will sound to stop them.This makes voting better and safer.

Objective of the Research

The fingerprint voting system requires users to submit their fingerprints to the voting station. The project uses fingerprint devices and the Arduino system to create the application. The main goal of the project is to create a system that requires the user to show their fingerprint as proof of identity. The system reads the information in the fingerprint and identifies the information currently stored in the database. The content provided is consistent with the voting record. There is a campaign to get new free votes and information and a system to allow people to vote. If the fingerprint data provided does not match the stored

data, the system starts processing immediately and security agencies can continue to operate.

Background of the Research: This study was conducted based on the system using Arduino technology. The system reads the data from the fingerprint module, uses the stored data for verification and then carries out the transaction. The entire process is done using Arduino, fingerprints and buttons instead of the traditional paper process. The Arduino

controller, programmed in C/C++, interacts with the fingerprint module, analyzes the data in its memory and executes the commands specified in the control section.

Advantages of Fingerprint Based Voting System:

- It prevents wrong voting.
- Shorten voting time.
- Easy to move from mailbox to polling station
- Reduce the number of workers at polling stations.
- Calculate effortlessly, easily and accurately.
- Ensure careful voting.

Problem Definition:

The problem addressed is the persistence of paper- based election systems in the 21st century despite the rapid growth of electronic technology. The inefficiencies and vulnerabilities of paper-based voting systems are highlighted, with a focus on issues such as fraud and corruption. An illustrative example is provided, citing a recent election invalidated due to fraudulent paper ballots. The associated costs, challenges in prosecuting crimes, and the lack of a reliable audit trail are emphasized. Another instance involves the production of additional ballots during an American election, leading to untraceable and potentially fraudulent submissions. The overarching concern is the need for a transition to electronic voting systems to ensure "One Person - One Vote" and address the shortcomings of traditional paper-based methods.

1.1 Existing System:

In the current system, electronic voting (often called e-voting) uses technology to help people vote and have their votes counted. These voting machines havetwo main features:

1. Control Unit: This unit consists of officials whosupervise the voting process.
2. Voting devices: Devices placed in private votingsites.

The two devices are connected by a five meter long cable. Instead of giving you a ballot, the voter presses a special button in the control room. This allows you, as a voter, to vote for your favorite candidate by pressing the blue button next to them and the symbol on the voting device. The controllers in these electronic voting machines permanently store their instructions in silicon. Made by the manufacturer. Once these rules are set, no one can change them. Fig:1

1.2 Proposed System:

This project is all about making the voting process much safer. In this project, we use both fingerprints and iris scans to let people vote. Some folks try to cheat by making fake ID cards to vote more than once, but in this project, we use a person's iris to make surethey're the real voter.
Using the iris makes voting really secure because each person's iris is unique, like a one-of-a-kind key. This way, we make sure nobody can cheat or vote more than once, improving the safety of the whole process.

1.3 Iris Recognition:

Iris recognition takes a clear eye picture, finds the iris, picks out the important stuff, and uses it to tell who the person is. It's like taking a special eye photo, finding the eye's special part, and using it to figure out who theperson is.
Iris recognition is completed by following modules:

1. Image Acquisition
2. Iris Segmentation
3. Feature Extraction
4. Recognition

1. Image Acquisition: It starts with getting a picture of the iris. Think of this step as taking a photo of the eye. It's the very first thing we do because without an eye picture, we can't do anything else. This picture is as raw and untouched as it comes, straight from the hardware used to capture it.

2. Iris Segmentation: Next, we use a special algorithm to pick out the iris part from the eye image and separate it from the eyelids, eyelashes, and any reflections. This is important to make sure we're only looking at the iris itself. We use a few tricks like circles and lines to do this, and we also use a threshold to find and remove the eyelashes and reflections.

3. Feature Extraction: In the third step, we find interesting points in the iris and discover the strongest features using some special tools. We calculate a mean feature from these different methods.

4. Recognition: This is the last part. We use machine learning models like SVM and KNN to recognize the iris based on the features we found.

2. Software Description:

1. Arduino IDE: The program for Arduino can be written in many different programming languages, but we need to use one that can turn the code into the kind of language the microcontroller understands. This special language is called "microcontroller language." Once we write the code, we put it into the controller.

2. **Embedded C:** Now, when we talk about programming for embedded systems, it's not like making regular computer programs. Embedded systems are a bit different because they have limited resources. They don't have much memory, power, or processing ability. They use smaller, more efficient parts than regular computers. Plus, embedded systems are closely connected to the hardware they work with. So, when we write code for them, we have to keep allthese special things in mind.

Fig:2

3. Literature Survey:

1. Vishal Vilas Natu, the “voting tool” is based solely on paper and electronic devices. More office work should maintain voter registration and voters should go to the polls for verification using the voter card. Once the identity verification is done by the election government, voters can use the machine to vote. The tool contains a list of applications and other content.Voters can vote for candidates by moving their fingers, thanks to various buttons in front of their special calls.

2. Khasawneh said that in elections held on paper, citizens collect their votes by placing their ballots in sealed containers distributed around the ballot boxes in an average country. When the election is over, all of these containers are opened and the votes are counted by authorized personnel. In this case, there may be errors in the customer and information in the previous process, in the creation and delivery of notifications, in the counting of votes or in some messages sent to voters. Voters are looking for ways to vote more often.

3. Prasad, Halderman presented at "Risk Assessment of Power Plants in India", an international research journal. The author says that security is the key to electronic voting and developed this system for security purposes to overcome the balance of various security measures.

4. AM Jagtap about "Electronic Voting System using Biometrics, Raspberry Pi and TFT Module", the voter will enter his Aadhar ID on the touch screen and then the voter's fingerprint will be scanned and the touch screen module will be compared with the data stored in the Database. comparison cloud If there is a match, the rest of the process just begins.

5. "Secure Smart Voting System using Aadhar" by Madhuri B, Adarsha MG, Pradhyumna KR and Prajwal BM, which identifies a person's fingerprint to determine their eligibility to vote. Get and verify voter data from Aadhar database.

6. "Biometric Voting Machine Based on Fingerprint Scanner and Arduino", Dr. In Atharva Jamkar, Omkar Kulkarni, Aarti Salunke and Anton Pljonkin, where the fingerprint-based biometric voting system is divided into two parts, users must register in the first part and users must register in the second part. The second part of users will vote for the desired candidate.

7. Soma Bhattacharrya, Dibyangana Roy, Esha Pramanik, Trishita Nath, Snapan Kundu introduced "Wireless Voting Machine", a biometric scanner that works in two different stages. Initially, voters' fingerprints were taken and stored in a file to protect voter identities. When a voter puts his or her fingerprint on the scanner while voting, the scanner simply compares it with the fingerprint stored in the system database.

8. B Madan Mohan Reddy, D Srihari in "Aadhaar linked RFID based biometric voting system for secure voting" using RFID tags containing credentials stored in LPC 2148. A fingerprint scanner is used to verify whether the RFID belongsto the person.

9. Jefferson D. et al. Voting security has been scrutinized and criticized; Accenture's use of its website and fingerprint technology to ensure security was highlighted.

10. Zhao Qijun et al. A modified pore model for fingerprint pore extraction is proposed, focusing on the automatic identification of sweat pores. They discuss methods such as skeletonization and isotropic pore modeling for efficient extraction.

11. R. Moheb et al. A method is presented to extract images from web pages and accurately identify skins. Their techniques involve extracting images from web pages and identifying areas of skin color.

12. Manvijit Kaur et al. A fingerprint certificate using detail extraction technology is proposed, showing the world of details related to fingerprint identification.

13. Hoi Le and Lub Duy Bui proposed an online fingerprint authentication method that uses a fast and interference-resistant hashing method. They introduced the best strategy to increase the speed and accuracy of fingerprint recognition.

14. Mayank Vatsa et al. [12] proposed to combine pores and protrusions with details to improve fingerprint identification. Their algorithm uses a two-step process that uses Level 2 features and Level 3 pore and protrusion features to optimize the fingerprint image.

4. Block Diagram:

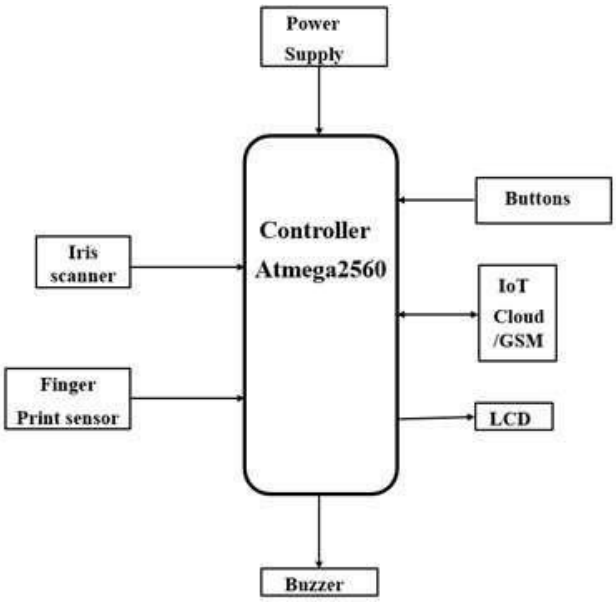


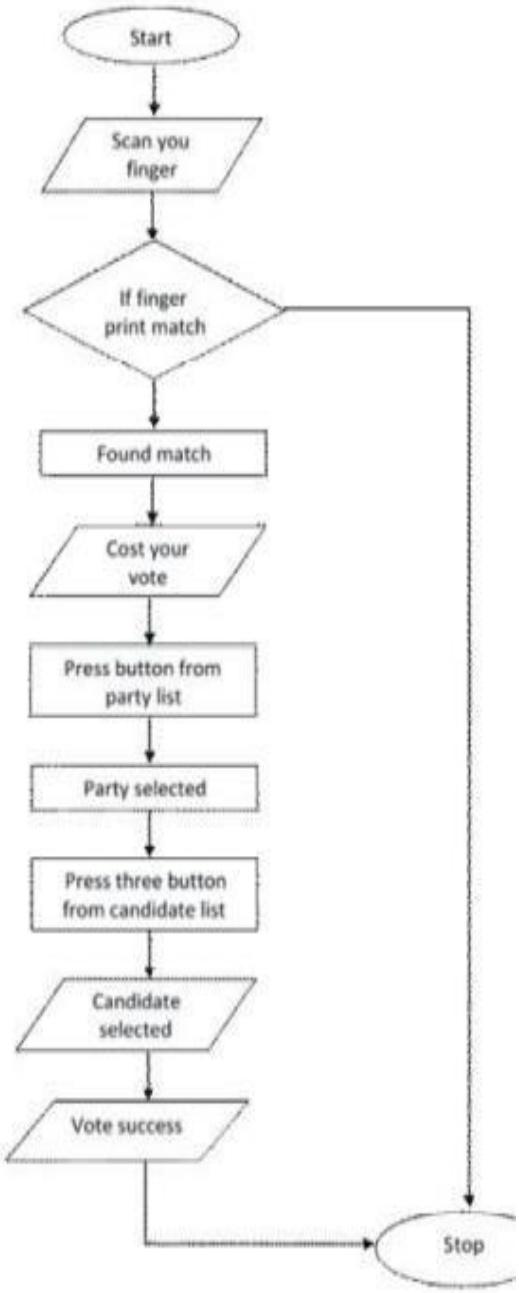
Fig 3: Fingerprint voting machine using Arduino

5. Working principle:

A fingerprint voting system operates on the premise of biometric authentication to ensure the integrity and security of the electoral process. During voter registration, individuals provide their fingerprints, which are securely stored in a central database along with other identification details. On election day, voters visit their designated polling stations where they undergo identity verification using fingerprint scanners. These scanners capture the unique features of a voter's fingerprint, comparing them against the stored data to confirm the individual's identity. Upon successful verification, the voter is authorized to cast their ballot, either electronically or on paper. To enhance security, measures such as encryption, secure data transmission, and stringent data privacy safeguards are implemented. The system includes mechanisms for auditing and verification, allowing independent observers to monitor and confirm the accuracy of the voting process. The deployment of a fingerprint voting system necessitates careful consideration of legal, ethical, and technical aspects to uphold the reliability and fairness of the election.

6. Flowchart:

Fig 4: Flowchart on fingerprint recognition



7. Result:

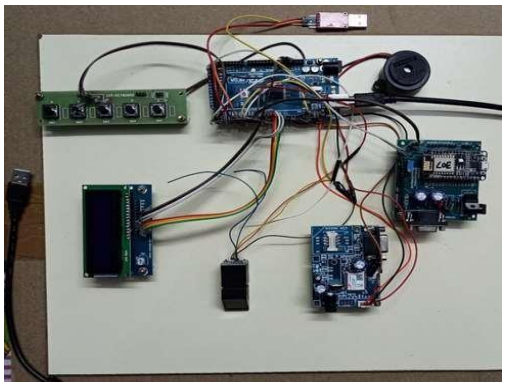


Fig 5: Hardware Output

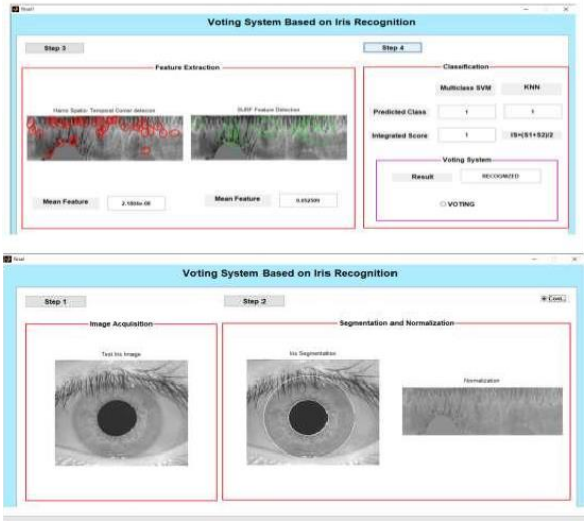


Fig 6: Software output of Iris recognition

8. Conclusion:

This paper presents an iris recognition system using cannyedge detection and HOUGH transform for segmentation. The database needs to be updated annually or before elections so that eligible citizens can be registered and the dead are kept off the ballot. This article discusses voter security in general, focusing on making the election process stronger and more reliable by eliminating virtual voters. We also discussed that segmentation technology based on Hough transform and Daugman algorithm can be segmented in the iris domain, while feature extraction and fractional integration algorithm based on HSTCP and SURF can identify it accurately and successfully. about 93%. This law helps everyone vote hassle-free. Voting app will increase the voting percentage. No textbook required. In this way, we get very good, clear and fast results. Using this innovation, we managed to overcome many problems in the current system. These machines work better than current technology. This technology detects iris from image and identifies iris from AADHAR database and checks if 2 images match. In case of a match, it allows voting by checking whether the voting rules and rules are violated, which is considered the safest way of iris detection.

9. References:

[1] Prateek Verma, Maheedhar Dubey, Praveen Verma, “Comparison of Various Segmentation Techniques in Iris Recognition” LAMBERT ACADEMIC PUBLISHING (LAP), GmbH & co.
KG, Dudweiler Landstrabe, Saarbrucken, ISBN 13:978-3-6 59-13597-2, Germany, MAY-2012.

[2] “Segmentation Techniques for Iris Recognition System”, International Journal of Scientific & Engineering Res V volume 2, Issue 4, April-2011, ISSN 2229-5518 IJSER © @ 2011 BY Surjeet Singh,Kulbir Singh.

[3] J. Daugman. How iris recognition works. Proceedings of 2002 International Conference onImage Processing, Vol. 1, 2002.

[4] Chinese Academy of Sciences –Institute of Automation. Database of 756 Greyscale Eye Images. http://www.sinobiometrics.com Version 1.0, 2003.

[5] “Recognition of Human Iris Patterns for Biometrics Identification “This project is submitted for the Bachelor of Engineering degree of the Schoolof Computer Science and Software Engineering, TheUniversity of Western Australia, 2003 BY LIBOR MASEK.

[6] Shafií, M, Adebayo, O. S, Damian, O., Mohammed, D. (2013). "The Design and Development of Real-Time E-voting System inNigeria with Emphasis on Security and Result Veracity, International Journal of Network andComputer Security. MECS (http://www.mecs-press.org/) Vol. 5, pp 9-18

[7] Enokela, J. A. (2010), —Security of Programs and Data for an Electronic Voting System, Pacific Journal of Science and Technology, Vol. 11(2), pp.283-287.

[8] Gunjal B., and Mali S, (2013). —Secure e-voting system with Biometric and Wavelet Based Watermarking

Technique in Ycgcb color space. IEEEInternational Conference on Information Technology, pp 1-6.

[9] Anandaraj, S., R. Anish, and P. V. Devakumar. "Secured electronic voting machine using biometric." In 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), pp. 1-5. IEEE, 2015.

[10] Naik, Devendra Vijay. "Smart wireless authenticating voting machine." In 2015 International Conference on Communications and Signal Processing (ICCSP), pp. 0785-0788. IEEE, 2015.

[11] Reddy, B. Madan Mohan, and D. Srihari. "RFID based biometric voting machine linked to aadhaar for safe and secure voting." International Journal of Science, Engineering and Technology Research (IJSETR) 4, no. 4 (2015): 995-1001.

[12} Arooj, Ansif, and Mohsin Riaz. "Electronic voting with biometric verification offline and hybrid evms solution." In 2016 Sixth International Conference on Innovative Computing Technology (INTECH), pp. 332-337. IEEE, 2016.

[13] Gomathi, B., and S. Veena Priyadharshini. "Modernized voting machine using fingerprint recognition." International Journal of Scientific & Engineering Research 4, no. 5 (2013): 156-161.