Anusandhanvallari
Vol 2024, No.1
June 2024
ISSN 2229-3388

Managing Secure Elections: Fingerprint Authenticated Voting System Design

[1]Dr. Sachin Misal, [2]Dr. Bade Ashwini Vivekanand*, [3]Prof. Vaishali Nikam, [4]Prof. Mahesh Mahankal

[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor, [4]Assistant Professor
[1]Affiliation Address: International Institute of Management Science, Chinchwad, Pune, India
[2]Affiliation Address: Siddhant College of Engineering, Pune, India
[3]Affiliation Address: SSMS's Institute of Management and Research, Pune, India
[4]Affiliation Address: International Institute of Management Science, Chinchwad, Pune, India

Abstract

This study presents the design and development of a fingerprint-authenticated voting system aimed at ensuring a robust and secure election process. The proposed system integrates hardware components such as a microcontroller, fingerprint sensor, push-button switches, and an LCD display to facilitate efficient voter authentication and vote casting. An R350 fingerprint sensor is employed to capture and store voters' fingerprint data in its internal memory. These biometric inputs are subsequently processed and verified using an integrated controller to ensure accurate identification. The human-machine interface (HMI) is implemented through a 16×2 LCD module, which provides real-time instructions and system status to the user, enhancing usability and interaction. Once authenticated, the voter is allowed to cast their vote through a simple interface, ensuring both security and ease of operation. The system effectively minimizes electoral fraud, such as duplicate voting and impersonation, by leveraging biometric verification. Overall, the proposed design offers a cost-effective, reliable, and user-friendly solution for secure electronic voting, making it suitable for deployment in modern electoral systems.

Keywords- HMI, fingerprint authenticated,CAN

I. Introduction

Free and fair elections are the cornerstone of any democratic system, requiring high levels of security, transparency, and reliability. However, conventional voting methods—such as paper ballots and standard electronic voting machines (EVMs)—continue to face significant challenges, including voter impersonation, multiple voting, ballot tampering, and administrative inefficiencies. According to various electoral studies, identity fraud and manual verification limitations remain key vulnerabilities, particularly in large-scale elections with diverse populations. These issues emphasize the need for advanced technological solutions that can ensure accurate voter authentication while maintaining the confidentiality and integrity of votes.

Biometric authentication, especially fingerprint recognition, has gained considerable attention as a secure and reliable method for personal identification. Fingerprints are unique, immutable, and difficult to replicate, making them highly suitable for authentication in critical applications. Compared to traditional identification mechanisms such as ID cards or passwords, biometric systems eliminate dependency on external tokens and reduce the risk of identity theft or misuse. As a result, integrating biometric verification into voting systems can significantly enhance electoral security and efficiency.

This research focuses on the design and implementation of a fingerprint-authenticated electronic voting system that leverages biometric technology to ensure secure voter verification. The proposed system incorporates a microcontroller-based architecture integrated with an R350 fingerprint sensor, push-button input switches, and a 16×2 LCD display for user interaction. The fingerprint sensor is responsible for capturing, processing, and storing voter templates within its internal memory. During the voting process, the system performs real-time fingerprint matching to authenticate voters before granting access to the voting interface.

The human-machine interface (HMI) plays a critical role in improving usability and accessibility. The 16×2 LCD module provides step-by-step instructions, system prompts, and status updates, enabling smooth interaction for users with varying levels of technical familiarity. Once authenticated, the voter can cast their vote using a simple input mechanism, ensuring ease of operation while maintaining system security.

From a system design perspective, the proposed model emphasizes data integrity, authentication accuracy, and operational efficiency. By eliminating redundant voting attempts and preventing unauthorized access, the system significantly reduces the likelihood of electoral fraud. Additionally, the use of embedded hardware components ensures a cost-effective and scalable solution that can be deployed in both urban and rural settings.

II. Literature Review

The application of biometric technologies in electronic voting systems has been widely studied to improve election security, reliability, and efficiency. Traditional voting methods, including paper ballots and conventional electronic voting machines, suffer from limitations such as voter impersonation, multiple voting, and lack of transparency. These issues necessitate the adoption of advanced authentication mechanisms to ensure fair electoral processes [1].

Biometric authentication, particularly fingerprint recognition, has proven to be an effective solution due to its uniqueness, permanence, and ease of implementation. Fingerprint-based systems eliminate the dependency on physical identification cards, thereby reducing the chances of identity fraud. Research has shown that biometric voting systems can significantly enhance voter verification accuracy and reduce electoral malpractices [2].

Several researchers have proposed fingerprint-based electronic voting systems using embedded platforms. For instance, Waili et al. developed a fingerprint-based voting system using microcontroller technology, demonstrating improved voter authentication and system efficiency [3]. Similarly, studies have shown that integrating fingerprint sensors with microcontrollers enables real-time verification and secure vote casting, making such systems suitable for practical deployment [4].

In addition to standalone biometric systems, hybrid approaches combining multiple authentication techniques have also been explored. A hybrid biometric voting system integrating fingerprint and facial recognition was proposed to enhance accuracy and reliability. The study reported improved performance compared to single biometric systems, although it increased system complexity and cost [5].

The integration of network-based technologies has further expanded the capabilities of electronic voting systems. Some researchers have explored the use of secure communication protocols and centralized databases to enable real-time vote monitoring and result processing. These systems enhance transparency and reduce the time required for vote counting [6].

Despite these advancements, biometric voting systems face certain challenges. The accuracy of fingerprint recognition can be affected by factors such as poor image quality, environmental conditions, and sensor limitations. Studies on biometric system performance highlight the importance of image quality and feature extraction techniques in ensuring reliable authentication [7]. Additionally, concerns related to data privacy, database security, and system scalability remain critical issues that must be addressed before large-scale implementation.[15]

Overall, the literature indicates that fingerprint-authenticated voting systems offer a promising approach to improving election security and efficiency. However, further research is required to optimize system performance, reduce costs, and address privacy and security concerns for real-world deployment.

Further research has explored the implementation of fingerprint-based voting systems with real-time processing capabilities. A study by Namballa et al. (2020) proposed a real-time fingerprint voting system that uses biometric authentication to validate voters before allowing vote casting. The system demonstrated that integrating fingerprint modules with embedded systems can significantly reduce duplicate voting and improve system reliability by enabling instant verification and processing [8,12,13].

Another important contribution is the work by Gangadurai et al. (2021), which introduced a fingerprint-based voting system integrated with national identity databases such as Aadhaar. This approach links biometric data with a centralized database, enabling efficient voter identification without the need for physical ID cards. The study highlights that such integration can streamline the voting process while reducing identity fraud and administrative overhead [9,16].

In addition, research on secure mobile voting systems has explored the combination of biometric authentication with encryption techniques. A study published in 2021 proposed a mobile-based e-voting system that uses biometric verification along with advanced encryption algorithms such as AES to ensure secure transmission and storage of voter data. The system emphasizes the importance of data confidentiality and secure communication in remote voting environments, particularly when biometric data is involved [10].

III. Design Methodology

In our project we have used fingerprint sensor for the purpose of voter identification & authentication. As the thumb impression pattern of every individual is unique, it helps in minimizing the error & proxy voting. A database is created storing the fingerprint images of all the voters as required.[11]

The proposed fingerprint-authenticated voting system is developed to ensure secure voter identification and prevent electoral malpractices such as proxy voting and duplication. The system integrates biometric authentication with embedded hardware components to provide a reliable and efficient voting process.

The overall methodology is divided into several stages, including system design, voter enrollment, authentication, vote casting, and result generation.

1. System Design and Components

The system is designed using embedded hardware components that work together seamlessly to perform the voting operations efficiently and securely. At the core of the system is the ATmega328P microcontroller, which acts as the central processing unit, managing and coordinating all tasks. The R350 fingerprint sensor is utilized for capturing and storing the unique fingerprint data of voters, enabling reliable biometric authentication. Push-button switches are incorporated to facilitate various functions such as enrollment, fingerprint matching, and casting votes. Additionally, a 16×2 LCD display is included to provide clear instructions and real-time status

updates to users throughout the voting process. Together, these components enable the microcontroller to control fingerprint verification, accurately count votes, and output relevant information on the display, ensuring a smooth and secure voting experience.

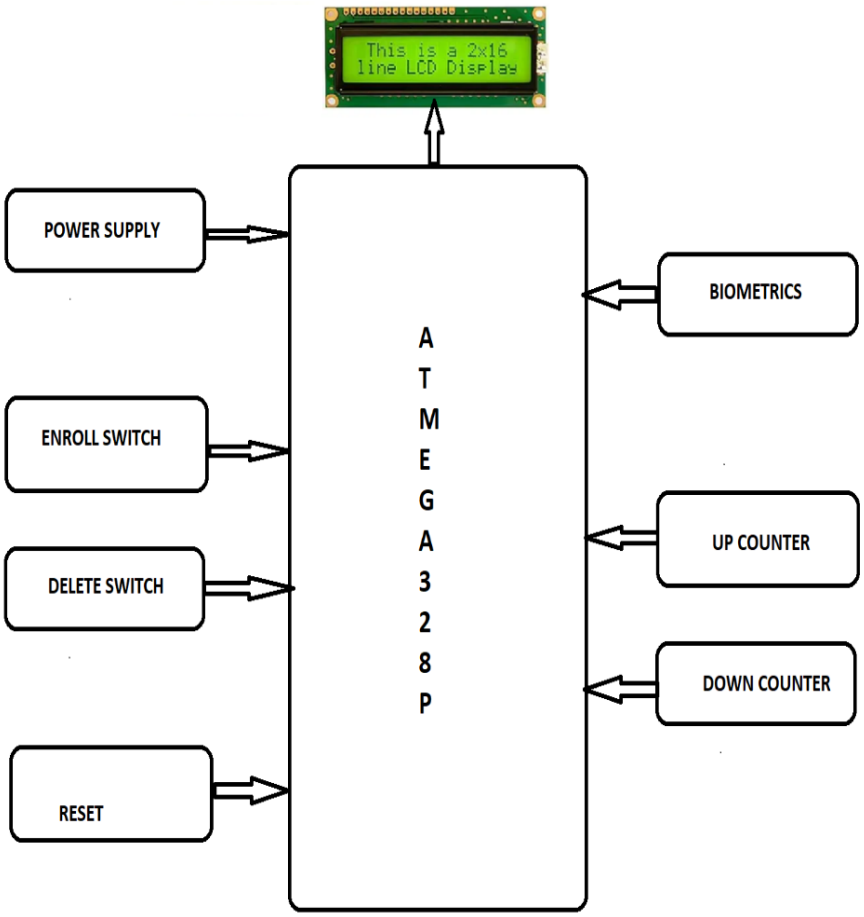

Fig 1. Block Diagram of System

2. Voter Enrollment

Before the voting process begins, each voter must register their fingerprint in the system to ensure secure and accurate identification. During enrollment, the voter places their finger on the fingerprint sensor, which captures the fingerprint image and extracts unique features from it. These distinct fingerprint characteristics are then stored in the system's database, with each fingerprint assigned a unique identification number. The system can register a maximum of 25 voters due to hardware limitations. To maintain the integrity of the voter database, the system actively checks for duplicate fingerprint entries; if a fingerprint that has already been registered is attempted again, the system detects this duplication and displays an error message on the LCD screen. Duplicate registrations are therefore prevented, ensuring that each voter is uniquely identified and can participate in the election process only once.

3. Voter Authentication

During the voting phase, authentication is carried out to verify the identity of each voter and ensure that only

registered individuals are allowed to cast their vote. To begin the authentication process, the voter presses the Match button, prompting the LCD display to show the message: *"Place your finger."* The fingerprint sensor then scans the voter's fingerprint and compares it with the stored templates in the database. If the scanned fingerprint matches a registered entry, the voter is successfully authenticated and granted access to cast their vote. Conversely, if the fingerprint does not match any stored data, access is denied, preventing unauthorized individuals from participating in the election. This authentication step is crucial for maintaining the integrity and security of the voting process.

4. Vote Casting Process

After a voter is successfully authenticated, they are allowed to cast their vote in the election. The system provides three candidates, labeled **CAN1, CAN2, and CAN3**, from which the voter can choose. Using the push-button switches, the voter selects their preferred candidate, and the vote is immediately recorded in the microcontroller's memory. Once the vote has been cast, the system locks the voter's ID to prevent any further voting attempts, ensuring that each voter can participate only once. By enforcing this mechanism, the system upholds the principle of **"one person, one vote"**, preventing multiple or fraudulent voting and maintaining the integrity of the election process.

5. Security and Error Handling

The system incorporates multiple checks to enhance both reliability and security throughout the voting process. Duplicate fingerprint registration is actively restricted, ensuring that no voter can enroll more than once. Similarly, the system prevents multiple voting attempts by locking a voter's ID after a vote has been cast, maintaining the integrity of the election. Any invalid or unrecognized fingerprints are automatically rejected, preventing unauthorized access. Additionally, the 16×2 LCD display provides real-time instructions and error messages to guide voters, minimizing confusion and operational mistakes. Together, these measures reduce system errors, enhance security, and ensure a smooth and user-friendly voting experience.

6. Result Generation

After all voters have cast their votes, the system generates the election results automatically. By pressing the **Result** button, the microcontroller calculates the total number of votes received by each candidate. The results are then displayed clearly on the 16×2 LCD screen, showing the vote counts for **CAN1, CAN2, and CAN3**. The candidate with the highest number of votes is declared the winner of the election. This automated counting process eliminates the possibility of manual errors, ensures accuracy, and provides instant results, making the election process faster, more transparent, and reliable.

IV. Overall Workflow

The complete system works in the following sequence:

Algorithm: Fingerprint-Authenticated Voting System

Step 1: System Initialization

1. Initialize microcontroller, LCD display, fingerprint sensor, and input buttons.
2. Load stored fingerprint templates from internal memory.
3. Display *"System Ready"* on the LCD.

Step 2: Voter Enrollment (Pre-Voting Phase)

1. Prompt the voter: *"Place your finger for enrollment"*
2. Capture fingerprint image using R350 sensor.
3. Extract unique features (minutiae points) from the fingerprint.
4. Check for duplicates in the stored database:
   - If fingerprint exists → Display error *"Duplicate Entry"* → Reject registration
   - If fingerprint does not exist → Assign unique ID and store template.
5. Repeat until maximum of 25 voters are registered.

Step 3: Voter Authentication (Voting Phase)

1. Prompt the voter to press the **Match** button.
2. Display *"Place your finger"* on LCD.
3. Scan fingerprint using the sensor.
4. Compare scanned fingerprint with stored templates:
   - If match found → Authenticate voter → Proceed to vote casting.
   - If no match → Deny access → Display *"Authentication Failed"* on LCD.

Step 4: Vote Casting

1. Display voting options: CAN1, CAN2, CAN3.
2. Voter selects preferred candidate using push-button switches.
3. Record vote in microcontroller memory linked to voter ID.
4. Lock voter ID to prevent multiple voting.

Step 5: Result Generation

1. After all voters have cast their votes, press the **Result** button.
2. Count total votes for each candidate (CAN1, CAN2, CAN3).
3. Display the results on LCD:
   - Votes per candidate
   - Candidate with the highest votes → Declared winner

Step 6: End Process

1. Display *"Voting Completed"* on LCD.

2. Reset system for the next election cycle if needed.

V. Conclusion

The proposed fingerprint-authenticated voting system demonstrates a secure, efficient, and user-friendly approach to modernizing the election process. By integrating biometric verification with embedded hardware components, the system ensures that only registered voters can participate, thereby preventing proxy voting, duplicate voting, and unauthorized access. The use of the R350 fingerprint sensor in combination with the ATmega328P microcontroller allows accurate fingerprint capture, real-time authentication, and reliable vote recording. Push-button interfaces and the 16×2 LCD display provide clear instructions and feedback, enhancing usability and reducing operational errors.

Moreover, automated vote counting and result display eliminate manual errors and provide quick, transparent outcomes, ensuring the integrity of the election process. Although the system is currently limited to a maximum of 25 voters due to hardware constraints, it serves as a practical, scalable model for small-scale secure elections. Overall, this system highlights the potential of combining biometric technology with embedded systems to create fair, tamper-resistant, and trustworthy voting platforms.

VI. References

[1] D. Chaum, "Secret-ballot receipts: True voter-verifiable elections," *IEEE Security & Privacy*, vol. 2, no. 1, pp. 38–47, 2004.

[2] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, 2004.

[3] T. Waili, A. N. M. Zaid, and M. H. Alkawaz, "Advanced voting system using fingerprint," International Journal on Perceptive and Cognitive Computing, vol. 6, no. 1, pp. 1–6, 2020.

[4] S. R. Madane and P. R. Indurkar, "Biometric based voting system using microcontroller," International Journal of Engineering Research & Technology, vol. 9, no. 5, pp. 120–124, 2020.

[5] S. N. Syed et al., "A novel hybrid biometric electronic voting system: Integrating fingerprint and face recognition," arXiv preprint arXiv:1801.02430, 2018.

[6] R. Rivest and W. Smith, "Three voting protocols: ThreeBallot, VAV, and Twin," USENIX/ACCURATE Electronic Voting Technology Workshop, 2007.

[7] F. Alonso-Fernandez et al., "Quality assessment in biometric systems: A review," IEEE Access, vol. 10, pp. 4218–4245, 2022.

[8] M. Namballa, T. Kaka, M. Vaishnavi, D. S. Suma, and K. Sriram, "Realtime Fingerprint Based Voting System," International Journal of Engineering Research & Technology (IJERT), vol. 9, no. 9, pp. 1–5, 2020.

[9] E. Gangadurai, R. Divakaran, and U. Aruneshwaran, "Fingerprint-Based Voting System," Journal of Telecommunication Study, 2021.

[10] M. A. Alzubaidi et al., "Secure Mobile Internet Voting System Using Biometric Authentication and Wavelet-Based AES," Journal of Information Security and Applications, vol. 61, 2021.

[11] Amrapali Pataskar, Prasad Shete, Santosh Londhe, Ashwini Bade, "Voting System Design with Finger Print Authentication", Published in International Journal of Science, Engineering and Technology, 2022

[12] Ankita R. kasliwal, Jaya S. Gadekar, Manjiri A. Lavadkar, Pallavi K. Thorat, Dr. Prapti Desmukh,"Aadhar Based Election Voting Syestem",IOSR- Journal of Computer and Engineering),[p-ISSN2394-9333],PP 18-21.

[13] Thiruthanigesan Kanagasabai et al,"Fingerprint voting system using Arduino,Middle-East Journal of Scientific Research,25 (8): 1793- 1802,2017.

[14] N. N. Nagamma and et al. "Aadhar based fingerprint EVM system", International Journal of Electronics Engineering Research,ISSN 0975- 6450 vol.9,No.6(2017) pp. 923-930.

[15] Deepika Iswarya, Rathna Prabha, Trini Xavier, "A Survey on E-Voting System Using Arduino Software", International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering (An ISO 3297: 2007Certified Organization), vol. 5, no. 2, pp. 687-690, February 2016.

[16] Navnath Baban Belote, Sneha Revankar, "Next Generation Electronic Voting Machine", International Journal of Advanced Research in Computer and Communication Engineering, vol. 5, no. 6, pp. 622-624,2016.