As per UGC guidelines an electronic bar code is provided to secure your paper

International Journal for Modern Trends in Science and Technology
Volume 12, Issue 04, pages 364-370.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol12issue04.html
DOI: https://doi.org/10.5281/zenodo.19454694

Design and Implementation of Secure Biometric Voting Machine Using Embedded System Featuring Anti-Spoof Fingerprint Verification

K.Varaprasad, K.N.Yamuna, T.Sireesha, M.Hima Bindu, B.Uma Maheswari

Department of Electronics and Communication Engineering, Vijaya Institute of Technology for Women, Enikepadu, Vijayawada, India.

To Cite this Article
K.Varaprasad, K.N.Yamuna, T.Sireesha, M.Hima Bindu & B.Uma Maheswari (2026). Design and Implementation of Secure Biometric Voting Machine Using Embedded System Featuring Anti-Spoof Fingerprint Verification. International Journal for Modern Trends in Science and Technology, 12(04), 364-370. https://doi.org/10.5281/zenodo.19454694

Article Info
Received: 06 March 2026; Revised: 28 March 2026; Accepted: 01 April 2026.

Copyright © The Authors ; This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

KEYWORDS

Biometric Voting Machine, Fingerprint Authentication, Anti-Spoofing, Embedded Systems, Secure Electronic Voting, Voter Verification, Microcontroller-Based System, Election Security

ABSTRACT

Free and fair elections require voting systems that are secure, reliable, and resistant to fraud. Traditional voting methods are vulnerable to impersonation, multiple voting, and manual errors. This project presents the design and implementation of a Secure Biometric Voting Machine using an Embedded System with Anti-Spoof Fingerprint Verification. The proposed system authenticates voters based on their unique Fingerprint Authentication, ensuring one- person–one-vote integrity. To enhance security, an Anti-Spoofing Mechanism is integrated to detect fake or artificial fingerprints, preventing unauthorized access through spoof attacks. The system is built around a Microcontroller-Based System that interfaces with a Fingerprint Sensor, display unit, control buttons, and secure memory. During Voter Verification, the captured fingerprint mismatched with pre-enrolled templates stored in the database. Only verified and non- duplicate voters are allowed to cast their vote, after which the system automatically locks further access for that voter. Election results are securely stored and can be retrieved only by authorized personnel. The proposed system enhances Election Security, increases transparency, and ensures reliable electronic voting.

1. INTRODUCTION

Democratic nations like India require secure and transparent electoral processes to build public trust in their electoral systems. Paper- based voting systems create security risks which include ballot stuffing, manual errors, impersonation, and delayed results. Electronic Voting Machines (EVMs) enhanced counting speed while decreasing Invalid votes but their manual

identity verification system still allows fraud and duplication to occur. The proposed project establishes a Secure Biometric Voting Machine through its adoption of Raspberry Pi 4 and Anti-Spoof Fingerprint verification technology.

The system uses fingerprint authentication with liveness detection techniques to prevent fake fingerprint attacks. The system combines its embedded hardware elements with software components to achieve real-time functionality and protect digital votes through secure storage methods.

The solution provides election security, maintains voting accuracy through one- person-one-vote principles, decreases operational human needs, and establishes a dependable voting method which operates at low costs while expanding its capacity to support future democratic elections.

1.1 Objectives

- To develop a real-time embedded biometric authentication system for secure voter verification.
- To implement anti-spoof fingerprint verification with liveness detection to prevent attacks by fake fingerprints.
- To develop a secure encrypted database for biometric template storage and digital vote management.
- To implement a system for preventing duplicate votes, enforcing the "One Person– One Vote" rule.
- To ensure an embedded architecture that is tamper-proof for secure and reliable election operations.

1.2 Principles

The design and development of the Secure Biometric Voting Machine are grounded on the following key principles:

- **Authentication Principle**

The system is designed to ensure that only registered voters are authorized to cast their votes using biometric fingerprint authentication.

- **One Person – One Vote Principle**

Each voter is entitled to vote only once. Once a voter casts their vote, the system is designed to update the database to ensure that the voter does not vote twice.

- **Anti-Spoof Security Principle**

The system is designed to ensure that voters cannot use artificial fingerprints to cast their votes using liveness detection and anti-spoof fingerprint authentication.

- **Data Integrity Principle**

The votes and biometric templates are stored in a secure manner using encryption to ensure that they are not tampered with, altered, or accessed without authorization.

1.3. Processes Involved

The process of operating the Secure Biometric Voting Machine requires a systematic step-by-step procedure to ensure secure and error-free voting.

STEP-1:

*Voter Registration :*The voter's fingerprint is scanned using a fingerprint sensor and is stored in the form of a digital template in the secure database during the registration process.

STEP-2:

Voter Authentication : On the day of the election, the voter touches their finger to the fingerprint sensor. The systemscans the live fingerprint and matches it with the digital template.

STEP-3:

Anti-Spoof Verification : The system uses liveness detection methods such as texture analysis and capacitance measurement to check if the fingerprint is of a real human or a fake one.

STEP-4:

Duplicate Vote Check: After authenticating, the system checks the database to see if the voter has already cast their vote. If the status is "not voted," access is granted.

STEP-5:

Vote Casting

The authenticated voter chooses their desired candidate using control buttons. The vote is recorded securely in the system memory.

STEP-6:

Database Update: The voter's status is immediately updated to "voted" to implement the "One Person–One Vote" rule.

STEP-7:

Secure Vote Storage and Result Generation: All votes are stored in an encrypted database. After the completion of voting, the result is automatically generated and displayed for authorized personnel**.**

1.3 Operating Conditions

The proposed Secure Biometric Voting Machine using Embedded System with Anti-Spoof Fingerprint Verification is designed to operate under specific environmental, electrical, and security conditions to

ensure accurate, reliable, and tamper-resistant performance during elections.

- Environmental Conditions: The system functions effectively within a temperature range of 0°C to 50°C and relative humidity of 20% to 80% (non-condensing). For optimal performance, the device must be deployed in a clean and dust-free environment, away from excessive heat, moisture, and direct sunlight, which may affect the fingerprint sensor's accuracy.
- Power Supply Conditions: A stable DC power supply (5V–12V) is required for the embedded platform. To ensure uninterrupted operation during voting, the system should be equipped with a battery backup or Uninterruptible Power Supply (UPS). Proper voltage regulation is necessary to avoid system failure or data corruption.
- Hardware Operating Conditions: All hardware components, including the fingerprint sensor, display unit, and embedded controller (e.g., Raspberry Pi), must be properly installed, calibrated, and tested before deployment. Adequate cooling and ventilation must be maintained to prevent overheating during continuous usage.
- Biometric Capture Conditions :Accurate fingerprint acquisition requires the voter to place their finger properly aligned with moderate pressure on the sensor. The system performs best when the finger is clean, dry, and free from obstructions such as dirt or moisture. Improper placement may lead to authentication errors.
- Anti-Spoofing Conditions: The system operates with integrated anti-spoofing mechanisms to prevent fraudulent voting attempts using fake fingerprints. It detects artificial materials such as silicone, gelatin, or rubber by analyzing fingerprint texture, ridge patterns, and liveness characteristics like skin conductivity or natural deformation. Authentication is granted only when a live finger is detected. Any spoofing attempt is automatically rejected, logged, and flagged for security monitoring.
- Software Operating Conditions: The system runs on a pre-configured embedded operating system with required biometric drivers and anti-spoofing algorithms. Regular software updates and database synchronization are necessary to maintain performance, accuracy, and security.
- Security and Operational Conditions: Access to the system is restricted to authorized personnel using secure authentication methods. Each voter is allowed to cast only one vote, ensured through unique biometric identification. All biometric data and voting records are securely stored and encrypted to prevent unauthorized access or tampering.

1.5. Materials & Methods: The development of the Secure Biometric Voting Machine with Anti-Spoof Fingerprint Verification involves the integration of hardware components and software algorithms to ensure secure, accurate, and efficient voting. This section describes the materials used and the methodology adopted for system implementation.

I. Materials (Hardware Components) :The system is built using the following key hardware components:

- **Embedded Controller (Raspberry Pi):** Acts as the central processing unit, controlling all operations such as fingerprint processing, vote recording, and system coordination.
- **Fingerprint Sensor Module (with Anti-Spoofing):** Captures and verifies the voter's fingerprint while detecting fake or artificial fingerprints using liveness detection techniques.
- **Display Unit (LCD/LED):** Provides instructions to the user and displays voting status messages.
- **Input Interface (Push Buttons/Keypad):** Allows voters to select their preferred candidate after successful authentication.
- **Buzzer/Indicator LEDs:** Gives audio/visual feedback for successful authentication, errors, or spoofing attempts.
- **Power Supply Unit:** Provides regulated power (5V–12V DC) to all system components, with optional battery backup.

II. Methods:

The methodology of the Secure Biometric Voting Machine with Anti-Spoof Fingerprint Verification is based on a structured sequence of operations that ensures secure voter authentication, prevention of spoofing, and accurate vote recording.

1. **System Initialization**
   - The system powers on and initializes all modules including the Raspberry Pi, fingerprint sensor, LCD display, and input buttons.
   - The database of registered voters is loaded into memory.
   - The LCD displays a prompt such as "Place Finger to Vote".

2. Voter Enrollment (Pre-Election Phase)
   - Each voter's fingerprint is captured using the sensor.
   - The fingerprint is processed and stored as a template in the database.
   - A unique voter ID is assigned to prevent duplication.

3. Fingerprint Acquisition
   - During voting, the voter places their finger on the sensor.
   - The system captures the fingerprint image and extracts unique features (minutiae points).

4. Authentication Process
   - The captured fingerprint is compared with stored templates in the database.
   - If a match is found, the voter is authenticated.
   - If no match is found, access is denied.

5. Anti-Spoof Verification
   - The system performs liveness detection to ensure the fingerprint is from a real human finger.
   - It analyzes characteristics such as:
     - Skin texture
     - Natural ridge patterns
     - Finger pressure or deformation
   - Fake fingerprints made from materials like silicone or rubber are detected and rejected.

6. Vote Casting Procedure
   - After successful authentication, the LCD displays candidate options.
   - The voter selects a candidate using push buttons.
   - The selected vote is recorded securely in the system.

7. Duplicate Vote Prevention
   - Once a vote is cast, the system marks the voter as "voted" in the database.
   - Any further attempt by the same voter is automatically rejected.

8. Result Storage and Security
   - Votes are stored in an encrypted format to ensure confidentiality.
   - System logs are maintained for auditing and verification purposes.

9. Feedback and Confirmation
   - The system provides confirmation via:
     - LCD display ("Vote Recorded Successfully")
     - Buzzer sound or LED indication

10. Error Handling
   - The system handles errors such as:
     - Invalid fingerprint
     - Spoof detection
     - Hardware or communication failure
   - Appropriate messages are displayed to guide the user

III. Block Diagram

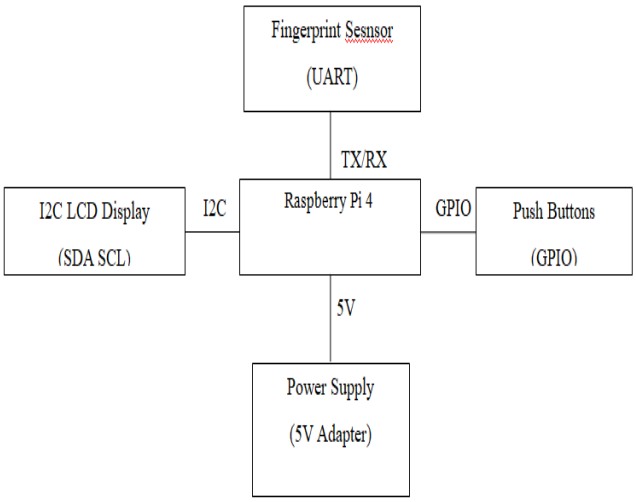

Fig. 1. Block Diagram

2. EXPERIMENTAL METHODOLOGY

Working principle of Secure Biometric Voting Machine with Anti-Spoof Fingerprint Verification

The experimental methodology of the Secure Biometric Voting Machine with Anti-Spoof Fingerprint Verification involves the systematic design, development, and evaluation of an embedded system that ensures secure, accurate, and tamper-resistant voting. The system is implemented using a Raspberry Pi as the central processing unit, interfaced with a fingerprint sensor for biometric acquisition, an LCD display for user interaction, push buttons for candidate selection, and a buzzer for feedback. The entire setup is

assembled to replicate a real-time voting environment, ensuring that the system can be tested under practical operating conditions.

The methodology begins with the hardware integration phase, where all components are connected through GPIO and serial interfaces. The fingerprint sensor is configured to capture and process fingerprint images, while the LCD is programmed to display instructions and system status messages. Push buttons are interfaced as digital inputs for vote selection, and the buzzer is connected to provide audio indications. A regulated power supply is used to ensure stable operation of all modules.

In the software implementation phase, the system is programmed using Python on the Raspberry Pi platform. Required libraries for fingerprint processing, GPIO control, and user interface handling are installed and configured. A voter database is created by enrolling fingerprints of authorized users, where each fingerprint is converted into a digital template and securely stored. The system also incorporates anti-spoofing algorithms to detect fake fingerprints based on liveness characteristics such as skin texture and natural finger response.

The working principle of the system is based on biometric authentication integrated with embedded control. During operation, when a voter places their finger on the sensor, the system captures the fingerprint and extracts unique features for identification. The captured data is compared with stored templates to verify the voter's identity. Simultaneously, the anti-spoofing mechanism ensures that the fingerprint is from a live human finger and not an artificial replica. If both authentication and liveness verification are successful, the system enables the voting interface.

Once authenticated, the voter selects a candidate using the push buttons, and the vote is recorded securely in the system memory. The system then updates the voter's status to indicate that the vote has been cast, thereby preventing multiple voting attempts. Feedback is provided through the LCD display and buzzer, confirming successful voting or indicating errors such as invalid fingerprint or spoof detection.

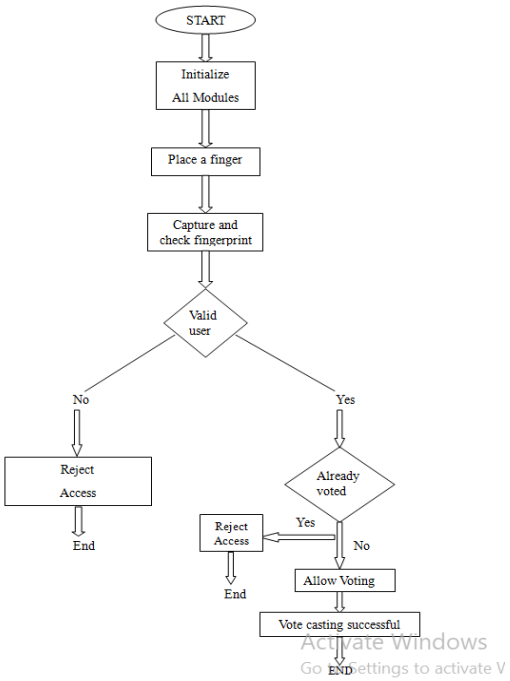

Fig. 2. Flow Chart

To evaluate the system performance, various experimental test cases are conducted, including genuine user authentication, rejection of unregistered users, detection of spoof fingerprints, and prevention of duplicate voting. The system is tested for accuracy, response time, and reliability under different conditions. The results demonstrate that the system effectively authenticates users, detects fraudulent attempts, and securely records votes with high efficiency. Overall, the experimental methodology confirms that the proposed system provides a secure, transparent, and efficient voting solution by combining fingerprint recognition, anti-spoofing techniques, and embedded system design, making it suitable for real-world electronic voting applications.

3. RESULTS

Fingerprint Authentication Performance Fingerprint Recognition Accuracy:

The R307 fingerprint sensor successfully captured and verified fingerprints of Registered voters. During testing, the system correctly identified authorized users and allowed them to proceed with the voting process. The fingerprint matching algorithm compared the scanned fingerprint with the stored database templates and confirmed the identity of the voter.

A. Authentication Reliability:

The system demonstrated reliable performance in recognizing fingerprints even after multiple attempts.

Registered fingerprints were matched accurately, while unregistered fingerprints were rejected by the system.

B. Unauthorized Access Prevention:

When unregistered fingerprint was placed on the sensor, the system immediately detected the mismatch and displayed an "Invalid User" message on the LCD screen. This ensured that only valid voters could access the voting system.

C. Authentication Speed:

The fingerprint verification process took only a few seconds, providing a fast and efficient authentication mechanism without causing delays

D. Voting Process Performance Vote Casting Operation:

After successful authentication, the voter was allowed to cast their vote using the keypad. The keypad enabled the user to select the desired candidate easily. Once the vote was selected, the system recorded the vote securely in the system database.

E. User Interface Efficiency:

The LCD display provided clear instructions to guide the voter through the process. Messages such as "Place Finger", "Authentication Successful" "Select Candidate" and "Vote Recorded" helped the user understand each step of the voting process.

F. Vote Confirmation:

After the vote was successfully recorded, the system displayed a confirmation message on the LCD screen. This ensured that the voter was aware that their vote had been successfully registered.

G. Duplicate Voting Prevention Single Vote Enforcement:

One of the main objectives of the system is to prevent duplicate voting. Once a voter successfully casts a vote, the system stores the fingerprint ID in the database to indicate that the voter has already voted.

H. DuplicateVoteDetection:

If the same voter attempts to vote again, the fingerprint is recognized, and the systemdisplays an "Already Voted" message on the LCD display. The system blocks the voting option, preventing multiple votes from the same individual.

- **System Integrity:**

This mechanism ensures fairness and transparency in the voting process by eliminating the possibility of repeated voting by the same voter.

I. Hardware Component Performance:

The Raspberry Pi successfully managed all system operations, including fingerprint verification, keypad input processing, LCD output display, and vote recording.

J. LCD Display Performance:

The LCD screen displayed messages clearly and helped users follow the voting process step by step.

K. LED Indicator Functionality:

LED indicators were used to show system status, such as successful.

L. Overall System Performance System Efficiency:

The system demonstrated efficient operation in terms of fingerprint authentication, vote recording, and duplicate vote prevention

M. Security Enhancement:

The integration of biometric authentication significantly improved the security level of the voting system by preventing impersonation and unauthorized voting.

N. User-Friendly Operation:

The voting system interface was simple and easy to use, making it suitable for voters with minimal technical knowledge.

O. Reliability:

The system performed consistently during multiple testing sessions, confirming its reliability and stability for secure voting applications.

Fig. 3. Results of the System

4. CONCLUSION

The Secure Biometric Voting Machine was developed to improve the security, transparency, and reliability of the voting process. Traditional voting systems often face challenges such as voter impersonation, duplicate voting, and manual errors. To address these issues, this project integrate biometric authentication with an

embedded system to ensure that only authorized voters can participate in the voting process.

The systemizes RaspberryPi as the main controller, which co-ordinates the operation of all connected hardware components. The R307 fingerprint sensor is used to capture and verify the fingerprints of voters, ensuring accurate identification. The LCD display provides clear instructions and feedback to users, while the keypad allows voters to select their preferredcandidate.LED indicators are used to display the system status during authentication and voting.

During the testing phase, the system successfully authenticated registered voters and prevented unauthorized access. It also ensured that each voter could cast their vote only once by maintaining records of previous votes. The integration of biometric verification significantly improved the reliability and security of the voting process.

The implementation of the Secure Biometric Voting Machine demonstrates the effectiveness of biometricauthenticationin improving voting system security. The system successfully verified voter identities using fingerprint recognition and prevented duplicate voting. The use of Raspberry Pi allowed efficient control of the hardware components and smooth execution of the voting process.

The results of the project show that biometric technology can greatly enhance the integrity and transparency of elections. By eliminating manual verification methods and reducing the chances of fraud, the system provides a more secure and reliable voting mechanism.

Overall, the developed system is user- friendly, cost-effective, and capable of providing accurate results. With further improvements and large-scale deployment, biometric voting systems can play a significant role in modernizing election processes and ensuring fair democratic practices.

5. FUTURE WORK

Future work will focus on enhancing the security and efficiency of the biometric voting system. Improvements can be made by integrating advanced biometric technologies such as face recognition or iris scanning along with fingerprint authentication to provide multi-level security. The system can also be upgraded by connecting it to a secure cloud database for real-time data storage and monitoring. Additionally, the implementation of stronger anti-spoofing techniques and improved encryption methods can further protect voter data and prevent unauthorized access. Testing the system in large-scale election environments will help evaluate its performance, reliability, and scalability. These improvements can make the biometric voting system more robust and suitable for real- world electoral applications.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Amitesh Yadu (2024), A Smart Voting System Combining Fingerprint and Facial Recognition for Enhanced Security, Shodh Kosh Journal.

[2] Ramya K. R. (2024), Electronic Voting Machine (EVM) using Fingerprint, International Advanced Research Journal in Science, Engineering and Technology (IARJSET).

[3] M. Satyanarayana, Rajiv Pranam. T, P. Sai Charan Reddy, S. Sai Srinivas (2023), Biometric-Based Electronic Voting System, International Journal for Research in Applied Science and Engineering Technology (IJRASET). DOI: https://doi.org/10.22214/ijraset.2023.50796

[4] Nandakumar.(2022),IoT Based Voting Machine with Fingerprint Verification, International Journal for Researching Applied Science and Engineering Technology (IJRASET).

[5] Jones Kevin Arthur, Thomas Robinson, R. Latha (2014), Implementation Aspects of Biometric System in Electronic Voting Machine to Avoid Electoral Frauds, International Journal of Innovative Science, Engineering and Technology. Available at: https://www.ijiset.com/v1s3/IJISET_V1_I3_43.pdf

[6] Olayemi M.Olaniyi, TalihaA. Folorunso, AliyuAhmed, Olugbenga Joseph(2016), Design of Secure Electronic Voting System Using Fingerprint Biometrics, International Journal of Information Engineering and Electronic Business.

[7] Shubhranil Chakrabortyet al. (2021), Designing of a Biometric Fingerprint Scanner – Based Secure and Low-Cost Electronic Voting Machine, International Advanced Research Journal in Science, Engineering and Technology (IARJSET).

[8] J. Nandha kumar, "IoT-Based Voting Machine with Fingerprint Verification," International Journal for Research in Applied Science and Engineering Technology (IJRASET), vol.10, no.3, pp.2456–2460,2022.

[9] S. Das, et al., "Deep Learning-Based Facial Recognition Voting System with Anti-Spoof Detection," International Journal of Advanced Computer Science and Applications, vol.12, no.6, pp.310–316, 2021.

[10] Ganamati et al., "A Study on Multi-Biometric Authentication Systems Using Deep Learning Techniques," International Journal of Computer Science and Information Security, vol. 18, no. 4, pp.85–92, 2020.