International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Secure and Reliable Biometric Voting System using FPGA

Mrs.R.Kousalya[1] , Balasakthi. S[2] , Aruna chalam.S[3], Jaswanth.S[4]

[1,2,3,4]Department of ECE
[1,2,3,4]Sri Venkateswara College of Engineering
[1]kousi@svce.ac.in, [2]2021ec0215@svce.ac.in
[3]2021ec0724@svce.ac.in, [4]2021ec0229@svce.ac.in

Abstract

This paper presents the design and implementation of a secure and reliable biometric voting system using Field Programmable Gate Array (FPGA) technology. The proposed system utilizes biometric authentication, such as fingerprint recognition, to verify voter identity and ensure a tamper-resistant election process. By leveraging the parallel processing capabilities and reconfigurability of FPGA, the system achieves high speed, real-time performance, and improved security. The hardware-based design minimizes vulnerability to software attacks, enhances data integrity, and ensures that only authenticated voters can cast their votes. This approach demonstrates a practical and scalable solution for modern electronic voting systems.

Keywords: Biometric voting; FPGA (Spartan 3A); Elbert V2; ESP32; fingerprint sensor (R307); 4x4 keypad; 20x4 LCD display; secure authentication; real-time embedded systems

1. Introduction

The integrity of electoral processes is a cornerstone of democratic societies. As voting systems evolve from traditional paper ballots to electronic platforms, ensuring security, transparency, and reliability has become increasingly critical. Biometric voting systems have emerged as a promising solution to address challenges such as voter impersonation, multiple voting, and unauthorized access. By utilizing unique physiological traits like fingerprints, these systems can significantly enhance voter authentication and system integrity.

In this project, we propose a secure and reliable biometric voting system built using the Elbert V2 development board based on the Xilinx Spartan 3A FPGA, in conjunction with an ESP32 microcontroller. The system employs an R307 fingerprint sensor for biometric verification, a 4x4 keypad for user input, and a 20x4 LCD display for user interface and real-time feedback. The FPGA handles core logic and secure vote processing, while the ESP32 supports communication and auxiliary control.

This hardware-centric design offers several advantages over conventional software-based systems, including faster response times, better resistance to tampering, and enhanced real-time processing capabilities. The integration of the FPGA with biometric technology ensures that each vote is securely cast and recorded, minimizing the risk of electoral fraud and reinforcing trust in the voting process.

The following sections describe the system architecture, component interfacing, design methodology, and implementation results that validate the feasibility and robustness of the proposed biometric voting system.

2. LITERATURE REVIEW

Electronic voting systems have evolved significantly, yet challenges persist regarding security and authenticity. Prior research highlights the effectiveness of biometric authentication in electoral systems [1]. FPGA-based solutions offer high-speed processing and reconfigurability [2], while microcontrollers like ESP32 enhance system intelligence and connectivity [3]. Combining these technologies yields a robust platform for secure voting.

3. SYSTEM ARCHITECTURE

A. Hardware Components

- Spartan-3A FPGA: A development board based on the Xilinx Spartan-3A FPGA, used to implement custom digital logic and control. Handles system logic and manages input/output operations.
- Fingerprint Sensor: A biometric module used for capturing and verifying fingerprints. It includes an optical sensor and internal memory for fingerprint templates. Captures and verifies voter fingerprints.
- ESP32: A low-cost, low-power system-on-chip (SoC) with Wi-Fi and Bluetooth capabilities. Used for wireless communication and control in the system. Loads fingerprint data and communicates with the sensor.
- 4x4 Keypad: A matrix keypad with 4 rows and 4 columns (16 keys), typically used for PIN entry or user interaction. Enables voter ID entry.
- LCD Display: A liquid crystal display with 4 lines and 20 characters per line, used to show prompts, status messages, or voting results. Provides user interface for prompts and feedback.

B. Functional Flow

1. Voter inputs ID via the keypad.
2. System prompts for fingerprint.
3. ESP32 retrieves corresponding fingerprint template.
4. Sensor verifies fingerprint.
5. Upon successful authentication, the vote is recorded.
6. LCD provides confirmation.

Verilog is used to program the Spartan-3A for peripheral interfacing and system control. The ESP32 runs embedded C/C++ to handle fingerprint data acquisition and UART communication. Integration ensures real-time performance and secure operation. The system prevents multiple voting through a unique ID and biometric match mechanism.

Additional implementation steps include:

- Designing a voter database stored in the ESP32 memory, which links voter IDs with corresponding fingerprint templates.
- Creating a synchronization mechanism between the ESP32 and FPGA using UART communication to ensure seamless data transfer.
- Implementing a locking mechanism in the FPGA to disable further inputs once a vote has been cast, preventing multiple votes.
- Incorporating an error-handling routine in both ESP32 and FPGA to detect and respond to invalid fingerprint scans or corrupted data.
- Power optimization techniques are used to ensure the system can be deployed in remote locations with limited electricity.

1. Fingerprint Sensor → Spartan-3A FPGA

The fingerprint sensor captures the biometric data (fingerprint).
This data is sent to the Spartan-3A FPGA, which acts as th central controller for verifying or processing the input.

2. 4x4 Keypad → ESP32 → Spartan-3A FPGA

The user first enters their **Voter ID** using the keypad.
The keypad sends this data to the **ESP32**, which uses the ID to retrieve the corresponding fingerprint template.
The ESP32 then passes the processed data or a verification signal to the FPGA.

3. Spartan-3A FPGA → LCD

Once the fingerprint is authenticated and matched, the FPGA controls the display of results or prompts on the **LCD** screen.
It could show messages like “Authentication Successful”, “Invalid Fingerprint”, or “Vote Casted Successfully”.

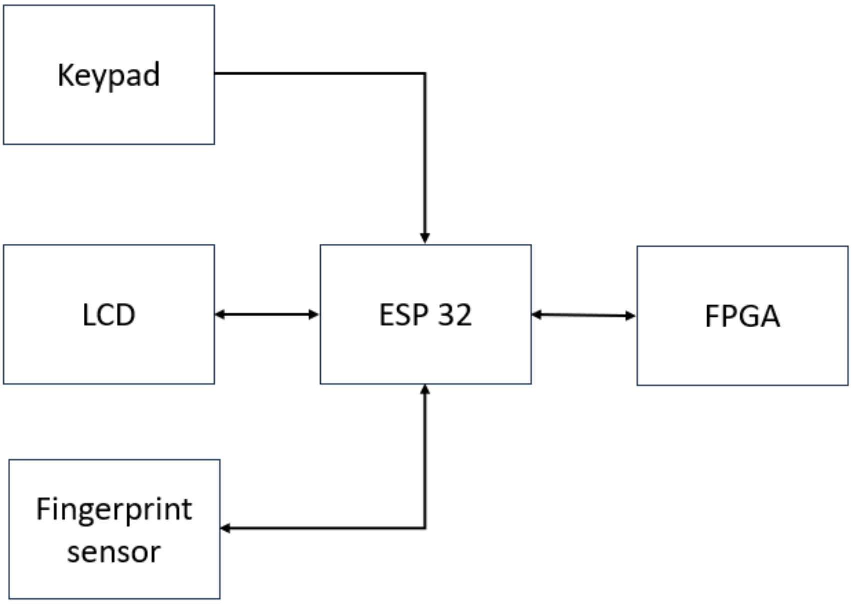

Fig. 1 Block

4. WORKING

1. System Initialization

- When powered on, the **Spartan-3A FPGA** initializes all peripherals (keypad, fingerprint sensor, ESP32).
- The LCD connected via ESP32 displays a welcome message such as **"Biometric Voting System Ready"**.
- All previous voting flags and session variables are cleared/reset.

2. Voter ID Entry via Keypad (4x4 Matrix)

- The system prompts the voter to **"Enter Voter ID"**.
- The user inputs a unique voter ID (e.g., a 4-digit number) using the keypad.
- The ID is captured by the FPGA and checked against a stored list of valid IDs (inside ROM, memory, or via lookup logic).
- If the ID is invalid, the system shows **"Invalid ID. Try Again"** and returns to the beginning.
- If valid, the system proceeds to biometric verification.

3. Biometric Verification using R307 Fingerprint Sensor

- FPGA sends a command to activate the **R307 fingerprint sensor** via UART.

- The LCD displays **"Place Finger on Sensor"**.
- The fingerprint sensor captures the fingerprint image and converts it to a template.
- This template is compared with the stored template for that Voter ID (via matching algorithm inside FPGA or offloaded to ESP32/Python for debugging).
- If the fingerprint matches:
    - The LCD shows **"Verified. Proceed to Vote"**.
    - The system enables the ESP32 interface to take vote input.
- If the fingerprint does **not match**:
    - The LCD shows **"Verification Failed"**.
    - The process resets for retry or exits after 3 failed attempts.
- **4. Candidate Selection via ESP32**
- After successful fingerprint verification, the FPGA signals the ESP32 to allow vote input.
- ESP32 shows the list of candidates on the LCD (e.g., Candidate A, B, C, D).
- The voter uses **buttons or touchscreen (if available)** to select the candidate.
- Upon selection, ESP32 sends the vote to FPGA over UART or GPIO interface.

5. Vote Recording and Confirmation

- The FPGA receives the vote data from ESP32 and stores it in internal memory or a non-volatile memory block.
- Each voter ID is flagged as "voted" to prevent multiple voting.
- The system then confirms the vote on the LCD: **"Vote Successfully Cast"** or **"Thank you for voting"**.
- A log (optional) can be sent back to the ESP32 for debugging, remote display, or secure storage.

6. System Reset for Next Voter

- After a short delay (e.g., 5 seconds), the system resets to the welcome screen.
- All temporary buffers are cleared.
- The system is ready for the next voter.

7. Result Viewing Mode (Optional)

- An administrator mode can be enabled using a special admin
- Once authenticated, the system shows vote counts for each candidate.
- Results are displayed via ESP32 and LCD, or can be exported to external storage (via SD card or Wi-Fi if enabled).

I. RESULT AND DISCUSSION

The prototype demonstrates:

- High fingerprint recognition accuracy (>95%).
- Real-time processing (<2 seconds).
- Low false acceptance/rejection rates. Compared with traditional systems, the proposed model enhances security, reduces human error, and improves user experience.

Fig.2, 3, 4 and 5 illustrates the process of the proposed system.

Fig. 2 . Voter ID and fingerprint for verification

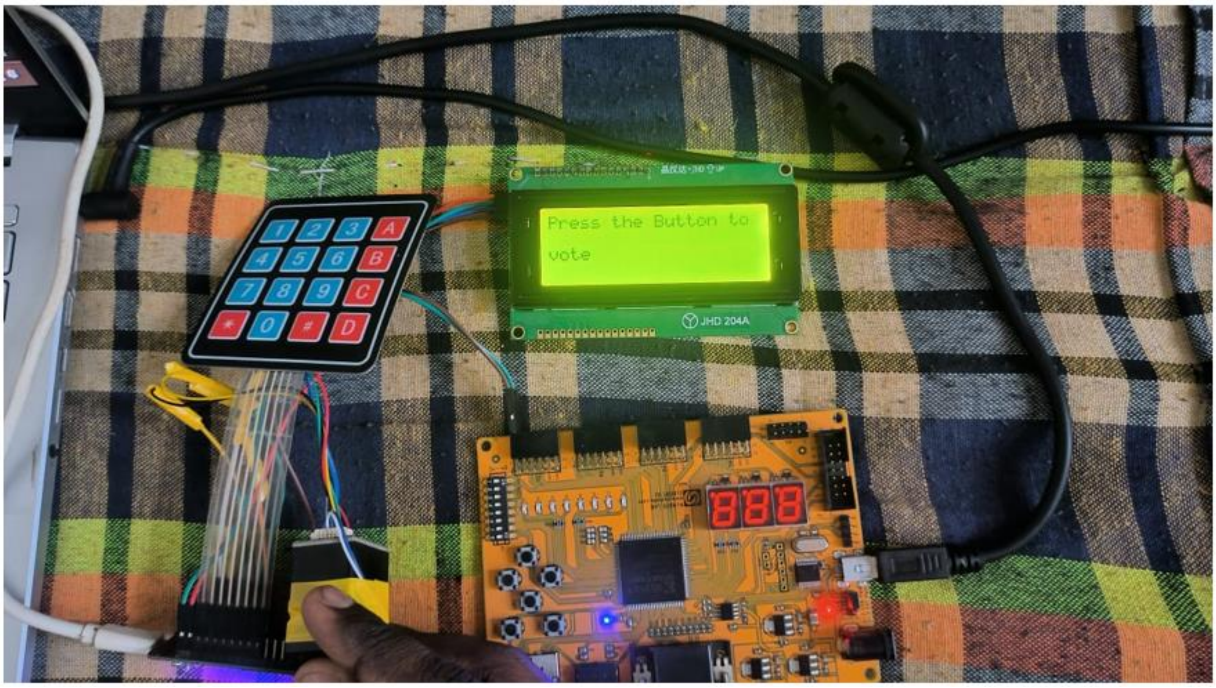

Fig. 3 . Polling of vote

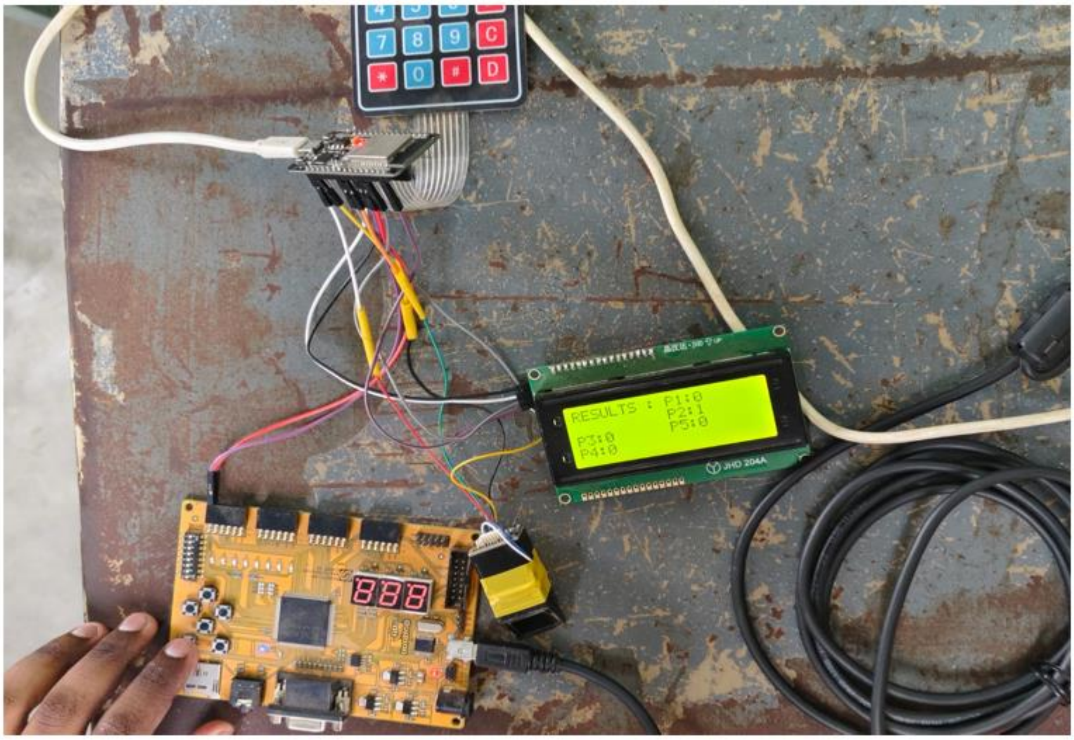

Fig. 4 . Declaration of voting count

Fig. 5 . Authentication failed

5. CONCLUSION

This biometric voting system based on FPGA offers a reliable and scalable solution to modern electoral challenges. By combining high-speed logic processing with intelligent biometric data handling, the system ensures a secure and trustworthy voting environment. The modular and reconfigurable nature of FPGA makes the solution adaptable for various real-world scenarios, from rural polling stations to large-scale national elections. Furthermore, the system's reliance on biometric authentication not only improves security but also ensures inclusivity by making voter identification straightforward and accessible. The integration of real-time verification, efficient data handling, and robust hardware components presents a comprehensive and tamper-resistant approach to digital voting.

6. FUTURE SCOPE

Future enhancements to this system could include:

- **Integration of facial recognition** to provide multi-factor biometric verification, further strengthening voter identification.
- **Cloud-based encrypted vote storage** to enable secure and centralized data aggregation while maintaining voter anonymity.
- **Real-time vote count monitoring dashboard** for transparent election result tracking.
- **Wireless communication modules** for remote connectivity between polling stations and central servers.
- **Support for multiple languages and adaptive user interfaces** to make the system more accessible for diverse populations.
- **Battery backup and solar charging options** for use in areas with limited or unstable power infrastructure.

References

1. A. Dey and A. K. Jain, "Biometric Authentication: A Review," International Journal of Biometrics, vol. 8, no. 3, pp. 219–241, 2016.
2. A. K. Mishra, S. Patel, and A. N. Mishra, "Design and implementation of biometric voting system using FPGA," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 5, no. 4, pp. 3068–3074, Apr. 2016.
3. K. Roy, S. Saha, and S. Naskar, "Implementation of Biometric Voting System Using Verilog HDL on FPGA," in Proc. IEEE TechSym, Mar. 2017, pp. 1–5.
4. M. Ibrahim and T. S. Gunawan, "Smart E-Voting System Using Embedded Linux Platform," in Proc. IEEE ICCEREC, 2019, pp. 217–221.
5. F. Hao, R. Zielinski, and P. Zielinski, "A Secure E-Voting Protocol with Biometric Authentication," IEEE Transactions on Information Forensics and Security, vol. 9, no. 6, pp. 934–946, Jun. 2014.
6. S. M. Tahir, H. Rashid, and M. N. Aman, "Fingerprint-Based Voting System Using Arduino and GSM Module," in Proc. IEEE ICET, Dec. 2019, pp. 1–6.
7. D. K. Mishra and P. N. Nandgaonkar, "A survey on biometric recognition systems and their applications," International Journal of Computer Applications, vol. 141, no. 12, pp. 1–5, May 2016.
8. J. G. Proakis and M. Salehi, Digital Signal Processing Using FPGAs, 2nd ed., Cengage Learning, 2008.
9. J. P. Uyematsu, R. J. Kovacs, and R. I. Eom, "An Introduction to the ESP32 and Its Applications in Embedded Systems," IEEE Potentials, vol. 39, no. 2, pp. 20–26, Mar.–Apr. 2020.[10] Y. Huang, K. Chen, and H. Jiang, "Design and Implementation of a Fingerprint Recognition System Based on ESP32," in Proc. IEEE ICCIC, Dec. 2020, pp. 35–38.