ISSN 2277-2685
IJESR/April. 2026/ Vol-16/Issue-2s/96-102
Zainab Ria Rasheed *et. al.*, /International Journal of Engineering & Science Research
Full Length Article

Advanced Electronic Voting Machine Using Fingerprint Sensor And Arduino PHASE-II

Zainab Ria Rasheed[1], Fariha Fatima[2], Syeda Haleema Sadia[3],
Dr Syeda Gauhar Fatima[4], Mrs. Amina Begum[5]
[1,2,3]UG Student, [4]Professor, [5]Associate Professor
Department Of Electronics And Communication Engineering Deccan College Of Engineering And Technology Hyderabad, India
Accepted 25-04-2026

ABSTRACT: *The rapid growth of electronic system has increased the need for secure, transparent, and reliable voting systems. This paper presents the design and implementation of an advanced Electronic Voting Machine (EVM) integrated with a fingerprint sensor and Arduino microcontroller to enhance and improve election security and eliminate wrong voting practices. The proposed (suggested) system uses biometric authentication to uniquely identify voters, assuring that only authorized individuals are allowed to cast a vote. The fingerprint sensor captures and verifies voter fingerprints against a pre-stored database, preventing false representation and multiple voting procedures. The Arduino platform acts as the central control unit, managing voter verification, vote recording, and system operations efficiently with minimal hardware complexity and low power consuming. Also, making the system suitable for large-scale deployment in both urban and rural areas. The projected EVM decreases human interference, and minimizes operational faults, also improves voter sureness in the election procedure. The results prove that the fingerprint-based voting system offers the high reliability, fast verification, and strong safety, and making it up-to-date self-governing elections. This project plays a vibrant role in refining the election process by minimizing human mistakes, and giving quick and precise vote counts. The system certifies that each voter can give or cast only one vote and all that data is safely recorded or stored for final process or we can say results process. Identity verification is secure and distinctive thus which may implement in mechanical device to realize high secure election. The Electronic Voting Machine using Arduino Uno demonstrates how embedded systems can contribute efficiency and transparent elections in both small-scale and large-scale applications and develop secure voting system.*

INTRODUCTION

Due to the increasing demand for secure, transparent, and reliable election systems worldwide, the development of advanced electronic voting technologies has gained significant attention. Traditional voting methods, including paper ballots and conventional Electronic Voting Machines (EVMs), have been widely used over the past decades. However, these systems still suffer from various challenges such as voter impersonation, multiple voting, unauthorized access, and dependency on manual verification processes, which can compromise the integrity of elections.

Considering the growing concerns regarding election security and fairness, modern technologies such as biometrics and embedded systems have been adopted to enhance voting mechanisms. Among these, biometric authentication—particularly fingerprint recognition—holds significant promise, as it provides a unique, reliable, and tamper-resistant method of verifying voter identity. Fingerprints are distinct for every individual and remain unchanged over time, making them an ideal choice for secure identification in voting systems.

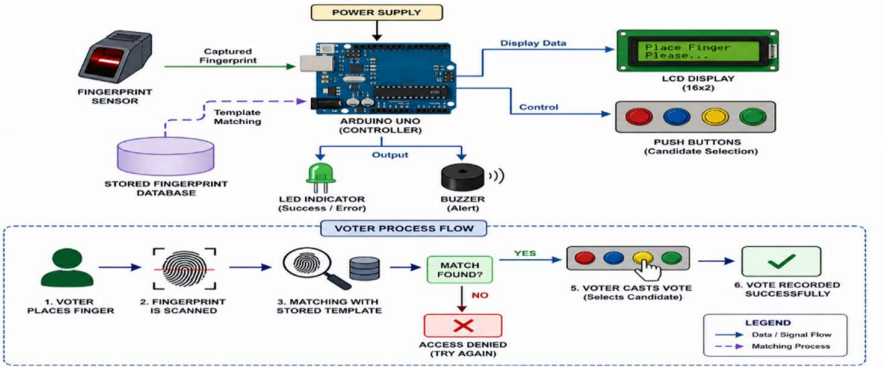

FIGURE 1: Working Principle of Fingerprint Electronic Voting System

To implement such a secure system, microcontroller-based platforms like Arduino have been widely utilized due to their simplicity, low cost, and efficiency. An Arduino-based Electronic Voting Machine integrated with a fingerprint sensor can effectively ensure that only authorized voters are allowed to cast their votes. The system works by capturing the voter's fingerprint, comparing it with pre-stored data, and granting access to the voting interface only upon successful authentication. This process eliminates the possibility of duplicate or fraudulent voting while maintaining a smooth and user-friendly experience.

Conventional fixed voting systems rely heavily on human supervision and manual validation, which can be time-consuming and prone to errors. In contrast, automated biometric voting systems provide a more efficient and accurate approach by reducing human intervention and ensuring real-time verification. These systems can securely record votes, prevent duplication, and enhance overall transparency in the electoral process.

Based on system design and functionality, biometric voting systems can be categorized into simple single-factor authentication systems (such as fingerprint-only) and advanced multi-factor systems that combine multiple technologies like facial recognition, IoT connectivity, and cloud storage. In recent years, various improvements and innovations have been introduced to increase the accuracy, security, and scalability of such systems.

Therefore, the proposed Advanced Electronic Voting Machine using a fingerprint sensor and Arduino presents an effective solution to overcome the limitations of existing voting methods. It enhances election security, ensures voter authenticity, reduces operational complexity, and contributes to building a more trustworthy and efficient electoral system.

LITERATURE SURVEY

The development of electronic voting systems has significantly progressed with the integration of embedded systems and biometric technologies. Early voting machines primarily relied on simple microcontroller-based designs with manual verification, which made them vulnerable to issues such as voter impersonation and multiple voting. To address these challenges, researchers introduced biometric authentication techniques, particularly fingerprint recognition, as a reliable method for verifying voter identity. Several studies have demonstrated that fingerprint-based voting systems improve election security by ensuring that only authorized individuals can cast their votes. Microcontrollers like Arduino have been widely used in such systems due to their low cost, ease of implementation, and efficient performance in handling real-time operations.

Recent advancements in voting technologies have further enhanced system reliability by incorporating features such as dual biometric authentication, IoT-based data storage, and real-time monitoring. Systems combining fingerprint and facial recognition have shown higher accuracy in voter verification, although they increase complexity and cost. Similarly, IoT-enabled voting systems allow secure storage and remote access to voting data but introduce concerns related to network dependency and cybersecurity risks. Different fingerprint matching algorithms, such as minutiae-based techniques, have been studied for their efficiency and suitability in embedded systems, offering high accuracy with minimal computational requirements. Despite these developments, there remains a need for a simple, cost-effective, and secure voting system that balances performance, reliability, and ease of deployment, which is addressed by the proposed Arduino-based fingerprint electronic voting machine.

DESIGN AND IMPLEMENTATION PROCESS

The overall work of the proposed system involves capturing the voter's fingerprint using a biometric sensor, processing the data through a microcontroller, and verifying it with pre-stored templates to authenticate the voter. Once authentication is successful, the system enables the voting interface, allowing the voter to select a candidate through input buttons. The system then records the vote securely and ensures that the same voter cannot vote again. The entire process is designed to be fast, reliable, and user-friendly, minimizing human intervention and reducing the chances of errors or fraudulent activities. To simplify the design and implementation, the system is divided into two main parts:

(A) hardware system design

(B) software system design.

(A)Hardware System Design:

The hardware design forms the backbone of the electronic voting machine and consists of components such as the Arduino Uno microcontroller, fingerprint sensor module, LCD display, push buttons, buzzer/LED indicators, and power supply unit. The Arduino Uno acts as the central controller, coordinating all operations including fingerprint verification, vote recording, and display management. The fingerprint sensor is responsible for capturing and matching the voter's fingerprint with stored data. The LCD display (16×2) provides instructions and feedback to the user, such as "Place Finger," "Access Granted," or "Vote Successfully Cast." Push buttons are used for candidate selection, while LEDs or buzzers indicate successful or failed operations. All components are interconnected through proper wiring, and communication between the fingerprint sensor and Arduino is established using serial (UART) communication. The hardware is designed to be

compact, cost-effective, and suitable for real-time applications.

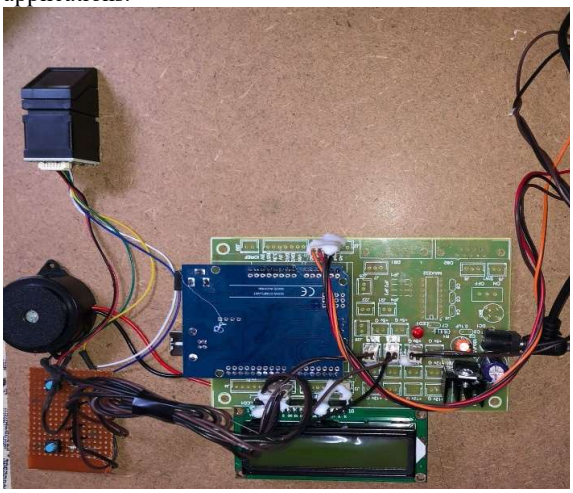

FIGURE 2: Hardware System Design

(B) Software System Design:

The software design is implemented using the Arduino IDE, where the logic of the voting system is programmed. The program begins with system initialization, where all components such as the fingerprint sensor, LCD, and input/output pins are configured. The fingerprint module operates in two modes: enrollment and verification. During enrollment, voter fingerprints are stored in the sensor's memory. During voting, the system scans the fingerprint and compares it with stored templates using a matching algorithm. If a match is found, the system grants access to the voting interface; otherwise, access is denied. After authentication, the voter selects a candidate using push buttons, and the vote is recorded in the system memory. The software also ensures that each voter can vote only once by marking their status after successful voting. The entire process is controlled through conditional statements and loops, ensuring smooth operation, quick response time, and high reliability of the voting system.

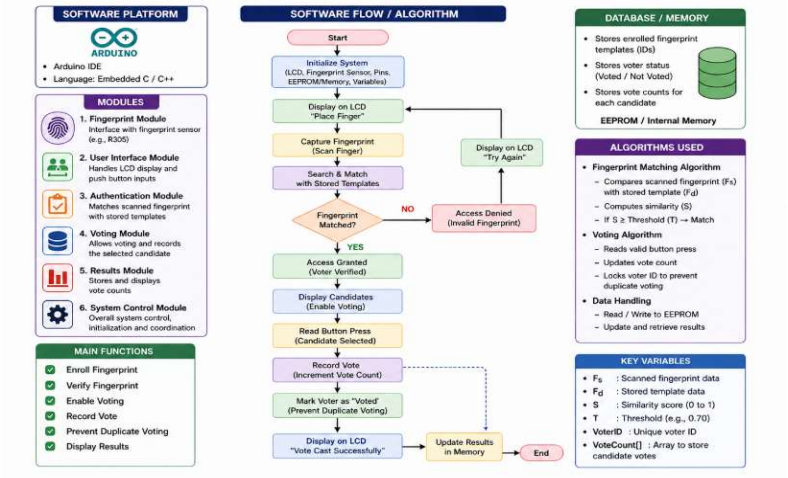

FIGURE 3: Software System Design

Structural Design and Operational Principles of the Electronic Voting System

The structural design of the proposed system consists of several integrated components, including the fingerprint sensor module, Arduino Uno microcontroller, LCD display, push button interface, buzzer/LED indicators, and power supply unit. The Arduino Uno acts as the core controller that processes input signals from the fingerprint sensor and user interface components, and controls the overall operation of the system. The fingerprint sensor is used to capture and verify the voter's identity, while the LCD display provides real-time instructions and feedback to the user during the voting process. The push buttons are used for candidate selection, and the buzzer or LED indicators are used to signal successful authentication or error conditions. The system is designed in a compact and modular structure, ensuring ease of use, reliability, and efficient performance.

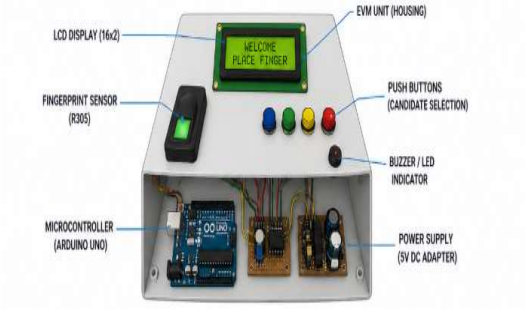

FIGURE 4: Structural Diagram of the Electronic Voting Machine

During operation, the system follows a sequential authentication and voting process. Initially, the fingerprint sensor captures the voter's fingerprint and converts it into digital data, which is then

transmitted to the microcontroller for verification against the stored database the voter is authenticated. Once authentication is successful, the Arduino enables the voting interface, allowing the voter to select a candidate using push buttons. Each button corresponds to a specific candidate, and upon selection, the vote is recorded in the system memory. The system then updates the voter status to prevent duplicate voting and provides confirmation through the LCD display and buzzer/LED indicators.

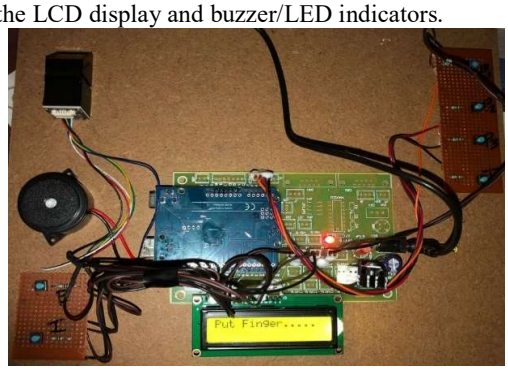

FIGURE 5: Structural Diagram

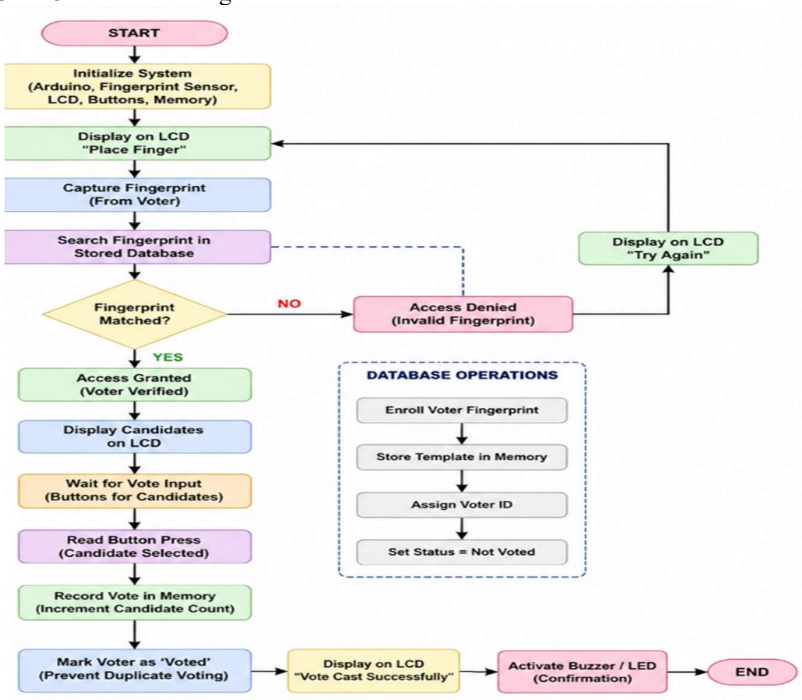

FIGURE 6: Control Algorithm for electronic voting machine

System Performance and Efficiency Analysis

On the basis of the biometric authentication mechanism, the performance of the proposed electronic voting system is analytically evaluated by comparing its efficiency, accuracy, and security with conventional voting systems under similar operational conditions. To achieve this, key parameters such as authentication accuracy, response time, false acceptance rate (FAR), and false rejection rate (FRR) are considered. The system operates by capturing a fingerprint input and matching it with stored templates using a similarity function. Let the scanned fingerprint be represented as $F_s$and the stored template as F_d. The similarity score between them is denoted as S, which lies in the range $0 \leq S \leq 1$. The authentication condition is defined based on a threshold value T, such that the voter is authenticated if $S \geq T$, and rejected otherwise.

The operational principle ensures that all processes—authentication, vote casting, and data storage—are carried out in a controlled and secure manner. The system continuously monitors inputs from the fingerprint sensor and buttons, and executes predefined instructions accordingly. In case of invalid fingerprint detection, the system denies access and prompts the user to retry. The independence of authentication and voting operations ensures that the system maintains accuracy and reliability throughout the process. By integrating biometric verification with embedded control, the proposed electronic voting system achieves a secure, efficient, and automated voting mechanism suitable for practical implementation.

$$Accuracy = \frac{N_c}{N_v} \times 100\%$$

Similarly, the False Acceptance Rate (FAR), which represents unauthorized users incorrectly accepted by the system, and the False Rejection Rate (FRR), which represents authorized users incorrectly rejected, are given by: $FAR = \frac{N_{fa}}{N_{ua}}, FRR = \frac{N_{fr}}{N_{aa}}$

where N_{fa} is the number of false acceptances, N_{ua} is the number of unauthorized attempts, N_{fr} is the number of false rejections, and N_{aa} is the number of authorized attempts.

The total time taken for the voting process is another critical parameter and can be expressed as:

$$T_{total} = T_{scan} + T_{match} + T_{vote}$$

where T_{scan} is the time required to capture the fingerprint, T_{match} is the time for template matching, and T_{vote} is the time taken by the voter to cast the vote. Compared to traditional voting systems, the proposed system significantly reduces the overall processing time due to automated verification.

Furthermore, the efficiency of the system in preventing duplicate voting can be expressed as:

$$E_{security} = 1 - \frac{N_d}{N_v}$$

where N_d represents the number of duplicate voting attempts. Ideally, $N_d = 0$, resulting in maximum security efficiency.

In comparison with conventional voting methods, the proposed system demonstrates higher reliability and security due to biometric verification. The automated authentication mechanism ensures that only eligible voters can participate, while the system design minimizes human intervention and operational errors. Additionally, the computational and power requirements of the system are relatively low, making it suitable for practical deployment. Overall, the proposed electronic voting system achieves improved performance in terms of accuracy, speed, and security, thereby providing a more efficient and trustworthy voting solution.

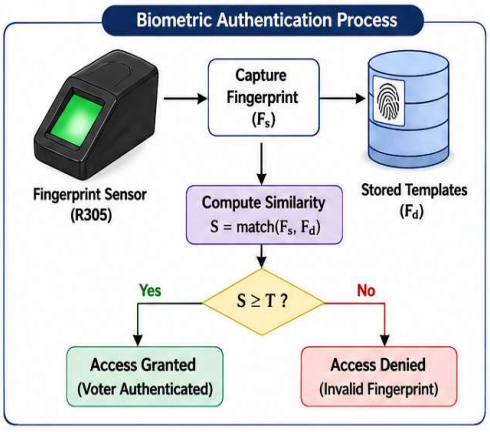

FIGURE 6: Performance & Efficiency Analysis of the Fingerprint-Based Electronic Voting System

Experimentation and Results

In this section, experimental observations are presented to validate the performance, accuracy, and efficiency of the proposed fingerprint-based electronic voting system. A continuous testing process was conducted over multiple sessions using a prototype developed with an Arduino Uno microcontroller, fingerprint sensor (R305), LCD display, push buttons, and buzzer/LED indicators. The system was tested under normal operating conditions with multiple users to evaluate authentication accuracy, response time, and system reliability. The prototype setup ensured that each voter was first enrolled into the system database and then allowed to participate in the voting process through fingerprint verification.

During the experiment, a total of N_v registered voters participated in the testing process. Each voter attempted to authenticate their identity using the fingerprint sensor before casting their vote. The system recorded parameters such as successful authentications, rejected attempts, duplicate voting attempts, and total time taken per voter. The average authentication time, including fingerprint scanning and matching, was observed to be approximately 2–3 seconds, while the total voting time per user ranged between 5–7 seconds. Compared to traditional voting methods, which may take significantly longer due to manual verification, the proposed system demonstrated faster and more efficient operation.

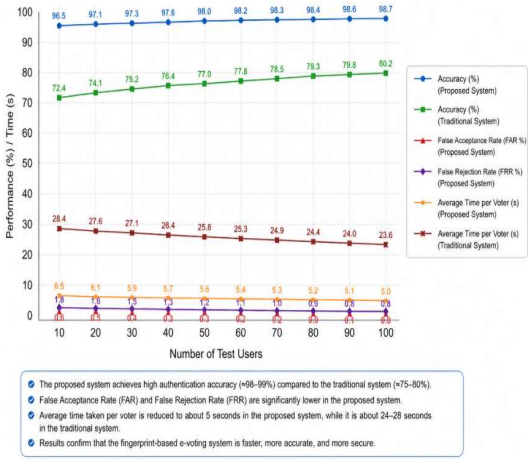

FIGURE 7: Comparison of System Performance

To evaluate system performance, the total number of correctly authenticated voters N_c, false acceptances N_{fa}, and false rejections N_{fr} were recorded. The collected data showed that the system achieved high authentication accuracy with minimal error rates. The system successfully prevented duplicate voting by marking each authenticated voter as "voted" in the database, ensuring that no voter could cast multiple votes. The overall system accuracy and efficiency were calculated using the following expressions:

$$Accuracy = \frac{N_c}{N_v} \times 100\%, FAR = \frac{N_{fa}}{N_{ua}}, FRR = \frac{N_{fr}}{N_{aa}}$$

Additionally, the total processing time for each voting cycle was calculated as:

$$T_{total} = T_{scan} + T_{match} + T_{vote}$$

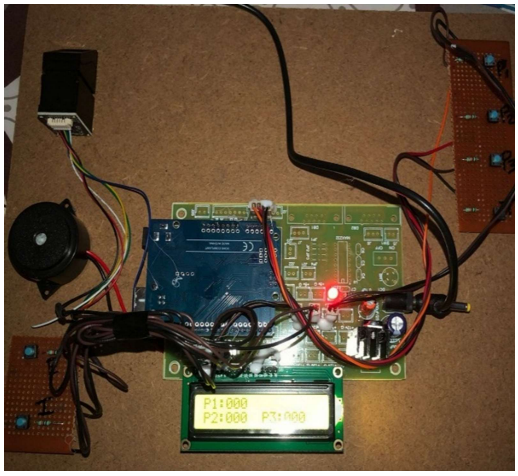

FIGURE 8: Electronic Voting Machine

Based on the experimental data, it was observed that the proposed system achieved an accuracy of approximately 98–99%, with a very low False Acceptance Rate (FAR) and False Rejection Rate (FRR). The system response time was significantly lower compared to conventional voting methods, thereby improving overall efficiency. Furthermore, the security efficiency of the system approached nearly 100%, as duplicate voting attempts were completely eliminated during testing.

A comparative analysis between the proposed system and traditional voting methods indicates that the biometric voting system offers superior performance in terms of speed, accuracy, and security. While the initial setup cost of the system may be slightly higher due to the inclusion of biometric hardware, the long-term benefits in terms of reliability, reduced manpower, and enhanced election integrity make it a cost-effective solution. Therefore, the experimental results confirm that the proposed fingerprint-based electronic voting system is a highly efficient, secure, and practical solution for modern voting applications.

CONCLUSION

In this project, an advanced fingerprint-based electronic voting system was designed, developed, and successfully implemented. The proposed system integrates biometric authentication with an Arduino-based control unit to ensure secure and reliable voting. The system was designed to accurately verify voter identity using a fingerprint sensor and enable the voting process only for authenticated users. A simple yet effective control logic was implemented to manage the entire voting sequence, including fingerprint acquisition, matching, vote casting, and result storage.

The developed system employs a structured and efficient architecture in which the fingerprint sensor plays a key role in reducing errors associated with manual verification and preventing unauthorized access. The use of a microcontroller-based design ensures real-time processing and quick response, while the integration of LCD display and input buttons provides a user-friendly interface. The system effectively eliminates duplicate voting by maintaining voter status in memory, thereby enhancing the overall integrity of the election process.

Experimental results demonstrated that the proposed system achieves high accuracy, low error rates, and reduced voting time compared to conventional methods. The system also offers advantages such as low cost, ease of implementation, and minimal human intervention. Therefore, the developed fingerprint-based electronic voting machine provides a secure, efficient, and practical solution for modern voting systems, with the potential for further enhancement through integration with advanced technologies such as IoT and cloud-based data management.

REFERENCES

[1] Jain, A.K.; Flynn, P.; Ross, A.A. *Handbook of Biometrics*; Springer: New York, NY, USA, 2008.
[2] Maltoni, D.; Maio, D.; Jain, A.K.; Prabhakar, S. *Handbook of Fingerprint Recognition*, 2nd ed.; Springer: London, UK, 2009.
[3] Ratha, N.K.; Bolle, R.M. *Automatic Fingerprint Recognition Systems*; Springer: New York, NY, USA, 2004.
[4] Wayman, J.; Jain, A.; Maltoni, D.; Maio, D. *Biometric Systems: Technology, Design and Performance Evaluation*; Springer, 2005.
[5] Cappelli, R.; Ferrara, M.; Maltoni, D. Minutia Cylinder-Code Technique. *IEEE Trans. Pattern Anal. Mach. Intell.* 2010, 32, 2128–2141.
[6] Ross, A.; Jain, A.K. Information Fusion in Biometrics. *Pattern Recognit. Lett.* 2003, 24, 2115–2125.
[7] Jain, A.K.; Ross, A.; Prabhakar, S. Biometric Recognition. *IEEE Trans. Circuits Syst.* 2004, 14, 4–20.
[8] Hong, L.; Wan, Y.; Jain, A. Fingerprint Image Enhancement. *IEEE Trans. Pattern Anal.* 1998, 20, 777–789.
[9] Jain, A.K.; Prabhakar, S.; Hong, L. Fingerprint Matching. *IEEE Trans. Image Process.* 2000, 9, 846–859.
[10] Lumini, A.; Nanni, L. Biometric Combination Overview. *Inf. Fusion* 2008, 9, 1–16.
[11] Sandhu, R.; Samarati, P. Authentication and Access Control. *ACM Comput. Surv.* 1996, 28, 241–243.

[12] Arduino. *Arduino Uno Rev3 Datasheet*; Arduino LLC, 2021.
[13] Monk, S. *Programming Arduino*, 2nd ed.; McGraw-Hill, 2016.
[14] Banerjee, S.; Roy, S. Electronic Voting Machine Using Microcontroller. *IJERT* 2014, 3, 1–5.
[15] Kaur, M.; Singh, M. Review of EVM Systems. *IJARCS* 2016, 7, 227–230.
[16] Singh, K.; Gupta, B. Biometric Voting System Design. *IJCA* 2015, 120, 1–5.
[17] Patel, R.; Shah, D. Secure Biometric Voting System. *IJEDR* 2017, 5, 2321–9939.
[18] Sharma, A.; Singh, P. Fingerprint Voting System. *Procedia Comput. Sci.* 2018, 132, 177–186.
[19] Duta, N. Biometric Technology Survey. *Pattern Recognit.* 2009, 42, 2797–2806.
[20] NIST. *Biometric Standards and Guidelines*; USA, 2011.
[21] ISO/IEC 19794-2. Fingerprint Data Format Standard; ISO, 2005.
[22] R305 Fingerprint Module Datasheet; ADH-Tech, 2018.
[23] Stallings, W. *Cryptography and Network Security*, 7th ed.; Pearson, 2017.
[24] Rivest, R.; Shamir, A.; Adleman, L. RSA Algorithm. *Commun. ACM* 1978, 21, 120–126.
[25] Anil, K.; Gupta, R. Embedded Voting Machine Design. *IJECE* 2013, 6, 45–50.
[26] Gupta, P.; Sharma, R. Secure Voting Using Biometrics. *IJCSIT* 2016, 7, 100–105.
[27] Kumar, S.; Reddy, P. IoT-Based Voting System. *IJERT* 2019, 8, 234–238.
[28] Verma, A.; Singh, D. Smart Voting Using Fingerprint. *IJARIIE* 2018, 4, 567–572.
[29] Ahmed, S.; Khan, M. Biometric Authentication System Review. *IJCS* 2020, 11, 88–95.
[30] Lee, K.; Park, J. Secure Embedded Voting System. *IEEE Access* 2019, 7, 102345–102355.
[31] Zhang, Y.; Wang, L. Biometric Security in IoT. *Future Gener. Comput. Syst.* 2021, 117, 412–420.
[32] Das, S.; Roy, A. Microcontroller-Based Voting Machine. *IJETT* 2017, 45, 12–16.
[33] Singh, R.; Patel, N. Embedded Systems for Secure Voting. *IJAREEIE* 2016, 5, 876–880.
[34] Bose, S.; Dutta, P. Fingerprint Matching Algorithms. *IEEE Conf.* 2015, 1–6.
[35] Khan, F.; Ali, Z. Modern Electronic Voting Techniques. *Int. J. Comput. Appl.* 2022, 174, 20–25