Int. J. Sci. R. Tech., 2026 3(1)
A Multidisciplinary peer-reviewed Journal
www.ijsrtjournal.com [ISSN: 2394-7063]

Original Article

Digital Voting System with Face Recognition

Hayath T. M., Rajeev D. V.*, R. Nihanth, U. Venkata Tharun, R. Achutha

Department of Computer Science and Engineering, Ballari. Institute of Technology and Management, Ballari

ABSTRACT

The conduct of elections in many organizations and institutions continues to depend on traditional or semi-digital voting mechanisms, which are prone to impersonation, duplicate voting, operational delays, and human error. Critical processes such as voter authentication, vote casting, and result compilation often lack adequate security and transparency. Existing digital voting solutions provide partial automation but fail to ensure robust identity verification and secure handling of sensitive electoral data. This study presents the Digital Voting System with Face Recognition, an automated and secure platform designed to enhance the voting process through biometric-based voter authentication. The system employs face recognition techniques to verify voter identity before allowing vote casting, thereby ensuring the principle of "one person, one vote." Automated vote recording and result generation improve efficiency, accuracy, and transparency. Experimental evaluation demonstrates reduced voting fraud, faster processing, and increased reliability compared to conventional methods. Future enhancements include integration with national identity databases, blockchain-based vote storage, mobile application support, and cloud deployment to enable large-scale, secure, and scalable election management.

Keywords: Digital Voting, Face Recognition, Biometric Authentication, Secure Voting System, Election Automation

INTRODUCTION

Voting is a fundamental process in democratic systems, enabling individuals to express their choices in elections conducted by institutions, organizations, and governments. With the advancement of digital technologies, there is an increasing need to modernize traditional voting systems to improve efficiency, transparency, and security. Conventional voting methods, whether paper-based or basic electronic systems, often face challenges such as impersonation, duplicate voting, manual verification errors, and delayed result processing. In many existing voting systems, voter authentication relies on physical identity cards or manual verification, which can be inaccurate and vulnerable to misuse. These limitations reduce trust in the election process and increase administrative workload. To address these challenges, biometric authentication has emerged as a reliable solution for secure identity verification. This project proposes a **Digital Voting System with Face Recognition**, which integrates biometric technology into the voting process. The system verifies the voter's identity using facial recognition before allowing vote casting, ensuring that only authorized voters can participate and that each voter can vote only once. Automated vote recording and result generation further enhance efficiency and accuracy. The proposed system provides a secure, reliable, and user-friendly platform for conducting elections in academic institutions, organizations, and similar environments.

2. Related Work

The conduct of elections requires a secure, transparent, and well-coordinated process to ensure voter trust and democratic integrity. In institutions, organizations, and governmental settings, voting procedures involve voter registration, identity verification, vote casting, and result compilation. Despite technological advancements, many voting systems still rely on traditional or semi-digital approaches that are vulnerable to impersonation, duplicate voting, and operational inefficiencies.

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

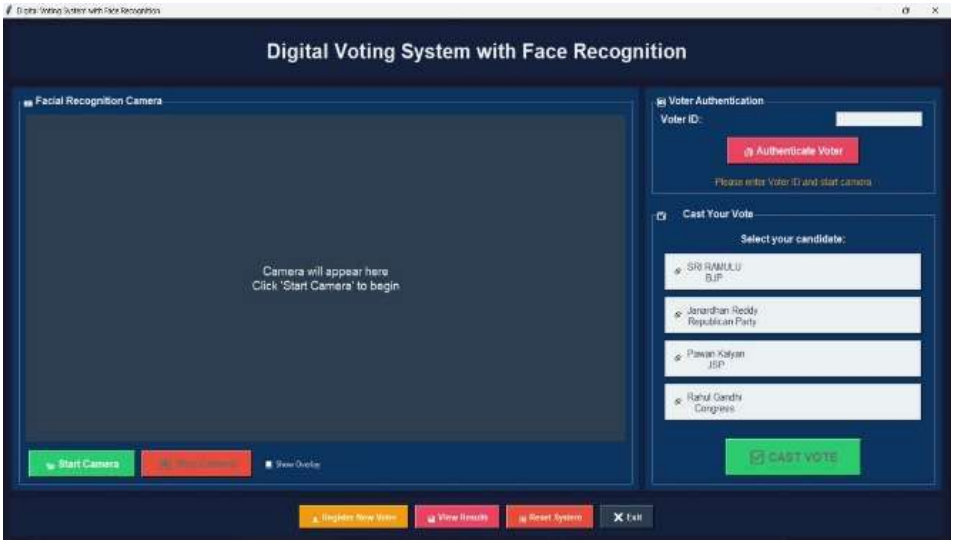

Fig 1 Landing Page of Digital Voting System with Face Recognition

Prior research highlights the importance of automation and biometric authentication in modern voting systems; however, existing implementations often address isolated components rather than providing a comprehensive, end-to-end secure voting solution. This section reviews existing research on traditional voting challenges, current digital voting systems, and the role of emerging technologies, thereby positioning the proposed **Digital Voting System with Face Recognition** within the broader context of secure election management.

2.1 Challenges in Traditional Voting Systems

Traditional voting systems, including paper-based ballots and basic electronic voting machines, face numerous challenges related to security, accuracy, and scalability. Studies [1] indicate that manual voter identification methods are susceptible to impersonation, proxy voting, and human verification errors. Paper-based systems also demand extensive manpower and time for ballot distribution, vote counting, and result declaration, often leading to delays and inconsistencies. Furthermore, research in [2] highlights that reliance on physical voter identification cards does not guarantee authenticity, as such credentials can be forged or misused. Inadequate monitoring mechanisms increase the risk of duplicate voting, thereby compromising the principle of "one person, one vote." As discussed in [3], traditional voting processes lack real-time validation, traceability, and secure handling of sensitive electoral data. These limitations underscore the need for advanced authentication mechanisms and automated voting workflows to ensure reliability and public confidence.

2.2 Existing Digital Voting Solutions and Their Limitations

Several digital voting systems have been proposed to overcome the drawbacks of traditional paper-based elections. Many existing systems provide electronic vote casting and automated result calculation, reducing manual effort and time consumption. However, most of these systems rely on basic authentication methods such as voter ID numbers, passwords, or manual verification, which are vulnerable to impersonation and unauthorized access. As highlighted in prior studies, the absence of strong biometric verification mechanisms allows fake or duplicate voting, thereby reducing trust in the election process. Some biometric-based systems utilize fingerprint authentication, which improves identity verification but introduces issues related to hardware dependency, hygiene concerns, and sensor accuracy. Additionally, online voting platforms increase accessibility but often lack transparency and robust security mechanisms for safeguarding sensitive voter data. Existing systems also require significant human supervision and do not fully eliminate manual intervention. These limitations demonstrate that current digital voting solutions provide only partial automation and insufficient security, emphasizing the need for a more reliable and tamper-resistant approach.

2.3 The Role of Emerging Technologies in Exam Section

Recent advancements in automation, artificial intelligence, cloud computing, and secure communication technologies have demonstrated substantial potential for transforming digital voting systems. Blockchain-based voting models [3] introduce immutable and tamper-proof record keeping, thereby enhancing transparency and security of sensitive electoral data. AI-powered systems, particularly face recognition techniques discussed in [2], improve voter authentication accuracy and decision-making by analyzing unique facial features, although their adoption in large-scale voting environments is still evolving. Cloud-based frameworks [4] provide scalability and centralized data access, enabling institutions and organizations to manage voting processes across multiple locations efficiently. QR-based and IoT-enabled systems [5] further strengthen voter verification and access control, reducing impersonation risks. Moreover, secure communication protocols ensure safe transmission of voting data between system components. The integration of these technologies—biometric authentication, automation scripts, cloud-hosted databases, and secure communication mechanisms—presents a promising pathway for a fully automated digital voting system. Such technological convergence lays the foundation for platforms capable of authenticating voters accurately, preventing duplicate voting, and generating election results automatically with minimal human intervention.

METHODOLOGY

The methodology of the **Digital Voting System with Face Recognition** is designed to provide a secure, efficient, and automated voting process by integrating biometric authentication, digital workflows, and secure data handling. The system focuses on eliminating impersonation, reducing manual effort, and ensuring accurate and transparent election results.

- System Analysis and Requirement Identification: - An analysis of traditional and existing digital voting systems revealed several challenges such as manual voter verification, possibility of fake or duplicate voting, time-consuming vote counting, and lack of transparency. Based on these observations, the primary requirements identified include secure voter registration with facial data, face recognition-based authentication, controlled vote casting, secure storage of votes, and automatic result generation.

- System Design and Architecture: A modular, scalable, and secure architecture was adopted to ensure flexibility and reliability. The system comprises the following core components:

  - Voter registration module with facial data capture.
  - Face recognition authentication engine.
  - Secure digital vote casting module.
  - Secure vote casting and storage mechanism Automated vote counting and result generation module.

- Technology Stack Selection:

  - GUI: - Tkinter.
  - Back-End: Python.

Table I: Comparative Analysis with Existing Systems

Feature	Traditional Voting System	Existing Digital System	Proposed Face Recognition System
Voter Verification	Manual checking	ID / password-based	Face recognition-based
Impersonation Risk	High	Moderate	Very low
Vote Casting	Manual	Digital	Secure and automated
Vote Counting	Time-consuming	Semi-automatic	Fully automatic

- Implementation and Development: The system was developed using an iterative approach to allow continuous improvement and testing. Flask routes manage voter registration, face authentication, vote submission, and result processing. Face recognition ensures that only verified voters are allowed to cast a vote, and each voter can vote only once.

- Testing and Validation: Testing was carried out at multiple levels, including unit testing, integration testing, and functional testing. User Acceptance Testing confirmed the system's ability to accurately authenticate voters, prevent duplicate voting, and generate correct results. The system was tested in simulated election scenarios to validate its reliability and effectiveness.

MODULES

The **Digital Voting System with Face Recognition** is designed as a unified web-based platform that supports both **Administrator** and **User (Voter)** functionalities within a single interface. Role-based access control ensures that administrative operations and voter actions are logically separated while maintaining ease of use and system security. and control system operations such as The **Admin module** enables election authorities to manage the complete election lifecycle. Administrators can register voters by securely capturing personal information and facial biometric data, which is later used for authentication. The module also allows administrators to manage candidate details, configure election parameters, and monitor voting activity in real time through a centralized dashboard. Additionally, the admin can control election phases, prevent unauthorized access, and automatically generate election results once voting is concluded. These features reduce manual effort, eliminate errors, and improve transparency in election management.

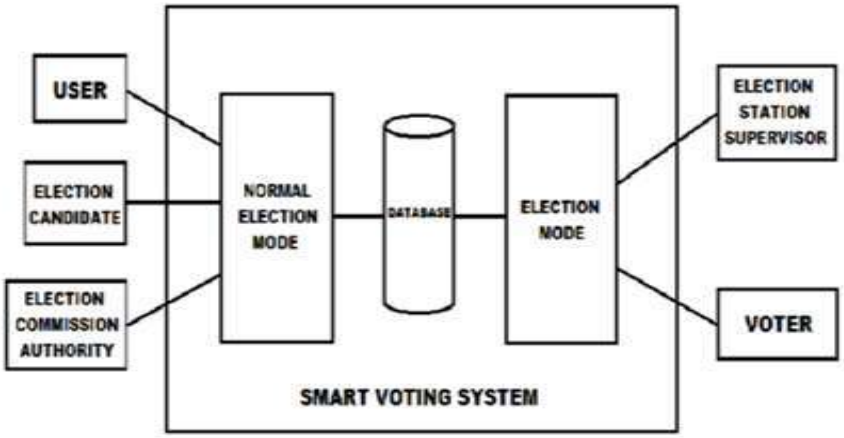

Fig 2: Proposed Methodology

The User (Voter) module allows registered voters to participate in the election securely and conveniently. Voters authenticate themselves using a combination of Voter ID and real-time face recognition, ensuring accurate identity verification and preventing impersonation. Once authenticated, voters are allowed to cast their vote anonymously through a secure digital interface. A confirmation step ensures intentional vote submission, and the system automatically restricts further voting attempts by the same voter to enforce the principle of *one person, one vote*. All voting data, biometric records, and election details are stored securely in the database layer, ensuring data integrity and confidentiality. The overall methodology ensures a robust, transparent, and fraud-resistant digital voting system that leverages face recognition technology to modernize the electoral process.

RESULTS AND ANALYSIS

The implementation of the Digital Voting System with Face Recognition resulted in significant improvements in election efficiency, security, and user experience. The system evaluation highlights enhanced voter authentication accuracy, reduced processing time, and improved transparency in the voting process. The results are discussed in the following subsections.

5.1 Time-Saving Analysis

The automated voting system considerably reduces the time required for voter verification, vote casting, and result generation when compared to traditional voting methods

Table II: Time Saving Analysis

Task	Manual Processing Time	Automated Time	Improvement
Voter Verification	2–3 minutes per voter	< 5 seconds	95% reduction
Vote Casting	1–2 minutes	< 30 seconds	70-85% reduction
Result Generation	Several hours	Instant	100% automation

5.2 Mathematical Model

To quantify time optimization, the following Model is applied:

$$Tsaved = Tmanual \left(1 - \frac{Tautomated}{Tmanual}\right)$$

5.3 System Performance and User Experience

The system exhibits high responsiveness, accuracy, and reliability. Administrators reported improved control over voter management and instant access to results, while voters benefited from a secure, simple, and fast voting process. The unified interface ensured ease of use, minimized confusion, and increased overall trust in the election process.

Fig 3: - Ready to Vote

Fig 4: - Cast Vote

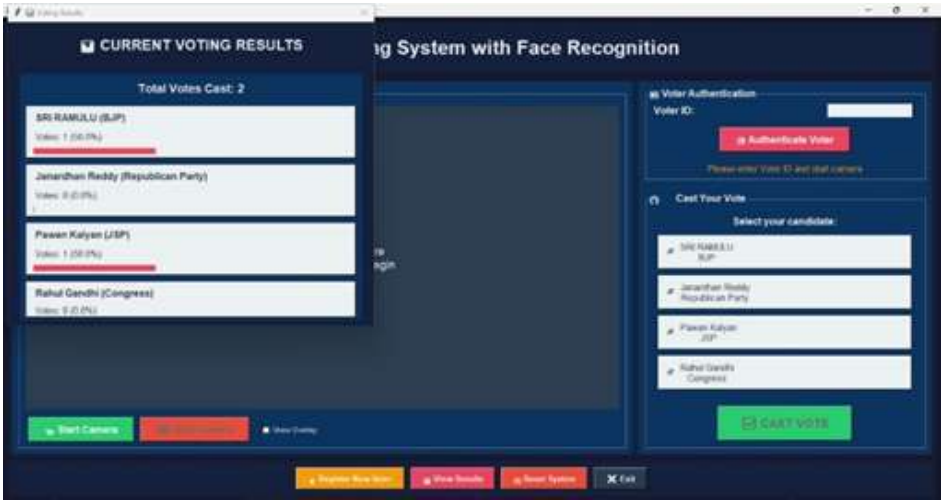

Fig 5: - Result Notification

CONCLUSION AND FUTURE SCOPE

The **Digital Voting System with Face Recognition** provides a secure and efficient solution for conducting elections. By using facial authentication, the system prevents impersonation and duplicate voting while reducing manual effort and human error. The automated voting and result generation process improves accuracy, transparency, and ease of use for both administrators and voters. Future enhancements may include integration with national ID systems, blockchain-based vote security, mobile application support, and cloud deployment to enable scalable and large-scale election management.

REFERENCE

1. M. T. Rahman, M. R. Islam, and M. A. Hossain, "A Secure Online Voting System Using Facial Recognition," International Journal of Information Security, 2023.
2. S. Gupta, M. Verma, and R. Yadav, "Blockchain-Based Secure Electronic Voting System with Biometric Authentication," IEEE Access, vol. 11, pp. 45678–45689, 2023.
3. R. Kumar, A. Singh, and R. Malhotra, "Face Recognition-Based Real-Time Electronic Voting System," International Journal of Computer Applications, vol. 185, no. 12, pp. 15–22, 2023.
4. H. Al-Mutairi and M. Al-Shehri, "A Secure Biometric-Based Voting Management Portal," Journal of Theoretical and Applied Information Technology, 2023.
5. A. Singh, P. Verma, and S. Nair, "Deep Learning-Based Face Recognition for Secure E-Voting," Journal of Artificial Intelligence and Data Science, 2024.
6. N. Patel and K. Shah, "Cloud-Based Digital Voting System with Facial Authentication," International Journal of Cloud Applications and Computing, 2024.
7. M. Hossain, T. Rahman, and S. Ahmed, "Multi-Factor Secure Digital Voting Using Face Recognition," IEEE Conference on Smart Computing, 2024.
8. Y. Zhang, L. Chen, and H. Wang, "AI-Driven Monitoring and Fraud Detection in Electronic Voting Systems," Future Generation Computer Systems, 2024.
9. A. Ahmed, R. Khan, and S. Malik, "Secure Mobile Voting System Using Face Recognition," International Journal of Mobile Computing, 2024.
10. P. Reddy and S. Kumar, "Biometric Authentication in Large-Scale E-Voting Systems," International Journal of Information Systems and Governance, 2025.
11. X. Chen, Y. Li, and Z. Wu, "Security, Privacy, and Ethical Challenges in Biometric-Based Voting Systems," ACM Computing Surveys, 2025.

HOW TO CITE: Hayath T. M., Rajeev D. V.*, R. Nihanth, U. Venkata Tharun, R. Achutha, Digital Voting System with Face Recognition, Int. J. Sci. R. Tech., 2026, 3 (1), 80-85. https://doi.org/10.5281/zenodo.18147625