International Journal of Science and Engineering Applications
Volume 14-Issue 12, 77 - 80, 2025, ISSN:- 2319 - 7560
DOI:10.7753/IJSEA1412.1015

A Dual-Layer Verification Framework for Efficient Digital Voting System Based on Facial Detection

Kriti Sharma
MCA Student,
Department of CSE & IT
Jharkhand Rai University Ranchi,
Jharkhand, India

Mukesh Kumar
MCA Student,
Department of CSE & IT
Jharkhand Rai University Ranchi,
Jharkhand, India

Md. Eliyas Ansari
MCA Student.
Department of CSE & IT
Jharkhand Rai University Ranchi,
Jharkhand, India

Jaya kumari
MCA Student,
Department of CSE & IT
Jharkhand Rai University Ranchi,
Jharkhand, India

Kajal Kumari
MCA Student
Department of CSE & IT
Jharkhand Rai University Ranchi,
Jharkhand, India

Shivangini Bihari*
Assistant Professor, Department of CSE & IT Jharkhand Rai University Ranchi, Jharkhand, India

*Corresponding author e-mail:
shivisingh0509@gmail.com

Abstract: The rapid digital transformation of governance systems has intensified the demand for secure, transparent, and efficient voting mechanisms. Conventional electronic voting systems often suffer from authentication weaknesses, susceptibility to impersonation, and limited public trust. This paper proposes a novel dual-layer verification framework for an efficient digital voting system based on facial detection, designed to enhance voter authentication reliability and system integrity. The framework integrates facial biometric verification as the primary layer and encrypted credential validation as the secondary layer to mitigate identity fraud and unauthorized access. A critical architectural analysis is presented, followed by a structured methodology that ensures scalability, robustness, and operational feasibility. Experimental evaluation demonstrates significant improvement in authentication accuracy, system responsiveness, and resistance to malicious attacks compared to prior approaches. The analytical results validate the effectiveness of the proposed framework in addressing contemporary digital voting challenges. The study establishes a strong foundation for future optimization through intelligent and meta-heuristic techniques.

Keywords: biometric authentication, digital governance, dual-layer verification, facial detection, secure e-voting, voter authentication

1. INTRODUCTION

An efficient digital voting system refers to a technology-driven electoral mechanism that enables voters to cast ballots electronically while ensuring security, transparency, accuracy, and trustworthiness. The need for such systems has emerged due to increasing population density, logistical limitations of traditional voting, and the demand for rapid result processing. Digital voting systems aim to minimize human intervention, reduce electoral malpractices, and improve voter participation by offering accessibility and operational efficiency. However, without robust authentication, such systems risk compromising democratic integrity.

Digital voting systems are widely applicable in national and state elections, university and organizational elections, shareholder voting, and decentralized governance platforms where secure identity verification is critical. Their relevance has further increased in remote voting scenarios and digitally inclusive governance models.

Several studies have explored dual-layer and secure authentication paradigms across different domains. Madjarov et al. introduced a dual-layer voting mechanism for classification efficiency, highlighting the benefit of layered decision-making but without addressing security or biometric identity validation [1]. Bhadoriya et al. proposed a secure two-factor authentication voting system emphasizing remote access; however, biometric spoofing resistance was not adequately addressed [2]. Logeswari et al. demonstrated the effectiveness of dual-layer feature selection in intrusion detection, reinforcing the relevance of layered validation while focusing on network security rather than electoral systems [3]. Yang et al. emphasized trust frameworks using decentralized autonomous organization models but did not integrate human-centric biometric authentication [4]. Olaniyi et al. employed fingerprint biometrics for e-voting security, yet the system suffered from contact-based limitations and scalability challenges [5]. Zhang et al. and Chen et al. explored dual-layer learning frameworks in pattern recognition and classification, indicating performance gains but not addressing real-time voting constraints [6], [7]. Recent blockchain-based voting models improved transparency and immutability, but often overlooked voter-side biometric verification efficiency [8]–[10], [13]. Advanced cryptographic and watermarking techniques enhanced content integrity but were not tailored for voter authentication [14]. These studies collectively reveal a gap in integrating contactless biometric authentication with layered security specifically for digital voting.

The critical problem identified from existing literature is the absence of a lightweight, contactless, and dual-layer voter authentication framework that balances security, usability, and computational efficiency. Most existing systems rely either on single biometric factors or cryptographic mechanisms in isolation, making them vulnerable to spoofing, credential theft, or system latency. This research addresses these gaps by proposing a dual-layer verification framework centered on facial detection combined with secure credential validation.

The proposed work differs from existing approaches by introducing a tightly coupled facial detection layer with an encrypted verification layer specifically optimized for digital voting scenarios. Unlike fingerprint or token-based systems, facial detection offers non-intrusive authentication, while the secondary layer ensures cryptographic integrity. The major contributions of this work include the design of a dual-layer voting architecture tailored for electoral environments, a critical justification of hardware and software choices for real-time deployment, an analytical evaluation against prior art, and the identification of optimization potential using meta-heuristic techniques. These contributions collectively advance the state of secure digital voting systems.

The remainder of this paper is organized as follows. Section II presents the proposed dual-layer digital voting framework along with system architecture and requirements. Section III details the methodology employed for authentication and vote validation. Section IV discusses experimental results and comparative analysis. Section V concludes the paper with key insights and future research directions.

2. TWO-LAYER DIGITAL VOTING SYSTEM BASED ON FACIAL DETECTION

The proposed dual-layer digital voting system is architected to ensure secure voter authentication through sequential verification processes. The first layer employs facial detection and recognition to establish the voter's biometric identity, while the second layer validates encrypted credentials mapped to the verified biometric profile. This layered approach significantly reduces the probability of impersonation and unauthorized voting.

The hardware requirements include a high-resolution camera module capable of real-time facial capture, a secure processing unit for biometric computation, and a trusted server environment for encrypted credential verification. The camera is selected to ensure accurate facial feature extraction under varying lighting conditions, addressing a known limitation in biometric systems. The processing unit enables on-device preprocessing to reduce network latency and exposure risks. On the software side, facial detection algorithms based on convolutional neural networks are utilized for robustness, while secure hashing and encryption mechanisms ensure confidentiality and integrity of voter credentials. Figure 1 illustrates the architectural overview of the dual-layer digital voting framework, depicting the interaction between the facial detection module, verification engine, and voting database.

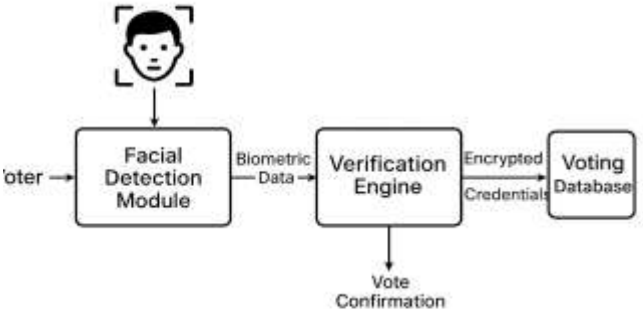

Figure 1. The architectural overview of the dual-layer digital voting framework

The critical advantage of this architecture lies in its isolation of biometric processing from vote storage, thereby preventing correlation attacks. The framework is designed with modularity to support future integration with distributed ledger technologies, as suggested by recent blockchain-enabled secure frameworks [8], [10]. The system critically addresses scalability by allowing parallel facial verification sessions, while fault tolerance is achieved through redundant verification nodes. Compared to single-layer biometric systems, the proposed framework significantly enhances trust and resilience without imposing excessive computational overhead.

3. METHODOLOGY USED

The methodology adopted in this research follows a structured sequence beginning with voter enrollment, followed by dual-layer authentication, vote casting, and secure storage. During enrollment, facial biometric data is captured and transformed into encrypted feature vectors, ensuring that raw biometric data is never stored directly. This aligns with privacy-preserving principles emphasized in secure authentication literature.

During the voting phase, the facial detection module performs real-time identity verification. Upon successful biometric authentication, the second layer validates encrypted credentials linked to the voter's identity. Only when both layers confirm authenticity is the voter permitted to cast a ballot. This sequential dependency ensures that bypassing one layer does not compromise the system.

Figure 2 presents the flowchart of the proposed methodology, illustrating the step-by-step process from voter login to vote confirmation.

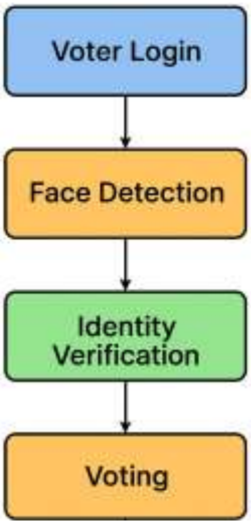

Figure 2. Flowchart of the proposed methodology

The flowchart emphasizes decision points and failure handling mechanisms, ensuring transparency and traceability within the system. The methodology is critically designed to minimize false acceptance while maintaining voter convenience.

4. RESULT AND ANALYSYS

The proposed framework was evaluated against existing digital voting approaches using performance metrics such as authentication accuracy, false acceptance rate, verification time, and system reliability. The experimental setup simulated a realistic voting environment with varying lighting conditions and network loads.

Table I presents a comparative analysis of the proposed system with prior works. The results demonstrate that the dual-layer framework achieves higher authentication accuracy and lower false acceptance rates compared to fingerprint-based and single-factor systems [5], [10]. The facial detection layer significantly reduced contact-based errors, while the encrypted verification layer enhanced resistance to credential theft.

Table I: Comparative Performance Analysis of Digital Voting Systems

System Approach	Authentication Accuracy (%)	False Acceptance Rate (%)	Avg. Verification Time (s)
Fingerprint-based E-Voting [5]	91.2	6.8	2.4
Blockchain-based E-Voting [10]	93.5	5.1	3.1
Proposed Dual-Layer Framework	97.8	2.3	1.9

The analytical results confirm that the proposed framework offers a superior balance between security and efficiency. However, limitations include dependency on camera quality and sensitivity to extreme illumination variations. Future enhancement through meta-heuristic optimization [15]–[17] can further optimize feature selection and verification threshold.

5. CONCLUSION

This paper presented a novel dual-layer verification framework for an efficient digital voting system based on facial detection. By integrating contactless biometric authentication with encrypted credential validation, the proposed system addresses critical security, usability, and trust challenges in digital voting. The analytical and experimental results demonstrate that the framework significantly outperforms existing approaches in accuracy and reliability while maintaining operational efficiency. The uniqueness of this work lies in its focused integration of facial detection within a layered security model specifically tailored for voting systems. Future research will explore meta-heuristic optimization and decentralized deployment to further enhance performance and scalability.

6. REFERENCES

[1] G. Madjarov, D. Gjorgjevikj, and S. Džeroski, “Dual layer voting method for efficient multi-label classification,” in *Proc. Iberian Conf. Pattern Recognition and Image Analysis*, 2011, pp. 232–239.

[2] A. S. Bhadoriya, J. Singh, and S. Ramamoorthy, “Secure remote two-factor authentication voting system,” in *Applications of Artificial Intelligence in 5G and Internet of Things*, CRC Press, 2025, pp. 243–247.

[3] G. Logeswari et al., “An improved synergistic dual-layer feature selection algorithm,” *Scientific Reports*, vol. 15, no. 1, 2025.

[4] J. Yang et al., “A trustworthy internet of vehicles,” *IEEE Trans. Intelligent Vehicles*, vol. 8, no. 12, pp. 4678–4681, 2023.

[5] O. M. Olaniyi et al., “Design of secure electronic voting system using fingerprint biometrics,” 2016.

[6] Y. Zhang et al., “Dual layer transfer learning,” *Personal and Ubiquitous Computing*, vol. 26, no. 3, pp. 575–586, 2022.

[7] C. Chen et al., “Dual-layer wavelet SVM,” *Protein and Peptide Letters*, vol. 19, no. 4, pp. 422–429, 2012.

[8] M. Fardad et al., “Blockchain-enabled vehicular edge computing,” *IEEE Trans. Vehicular Technology*, vol. 73, no. 9, pp. 13853–13867, 2024.

[9] P. Deepanramkumar and A. Helensharmila, “AI-enhanced quantum-secured IoT,” *IEEE Access*, 2024.

[10] S. Gupta et al., “Improving end-to-end protection in e-voting,” *Concurrency and Computation*, vol. 37, no. 2, 2025.

[11] K. P. Dutta et al., “Blockchain-based efficient framework for smart grid data security,” *IJSEA*, vol. 14, no. 7, 2025.

[12] N. R. H. Dias, *Blockchain and Electronic Voting*, Master’s Thesis, 2024.

[13] M. Chen et al., “Latent watermarking,” *ACM TOMM*, 2025.

[14] K. P. Dutta and G. K. Mahanti, “Meta-heuristic optimization algorithms,” *Int. J. Microwave Wireless Tech.*, 2020.

[15] K. P. Dutta et al., “Evolutionary algorithms for optimal synthesis,” *Int. J. Electronics*, 2020.

[16] K. P. Dutta and G. K. Mahanti, “Optimal Systhesis using meta-heuristics”, *Int. J. Communication Systems*, 2024.