Secure E-voting using Facial Recognition with AI

PANKAJ R PATIL*, ROHIT HILAL WAGH†, HARSH CHANDRAKANT KOTWAL‡, SURAJ SUDHIR THOKE§, HEMALI LALIT FIRKE¶
Department of Computer Engineering, R. C. Patel Institute of Technology, Shirpur, Maharashtra, India

***Abstract*—Electronic voting systems are being widely adopted to improve the efficiency, accessibility, and transparency of the electoral process. Despite these advantages, many existing e- voting platforms are still susceptible to security threats such as identity fraud, unauthorized system access, and multiple voting attempts by the same individual. To overcome these limitations, this research presents a secure e-voting system that integrates Artificial Intelligence–based facial recognition for reliable voter authentication and secure vote casting. The proposed approach employs deep learning techniques for facial feature extraction, real-time face matching, and liveness detection to ensure that only authorized voters are permitted to access the voting interface. The system architecture combines AI-driven recognition models with encrypted voter databases and a secure vote-recording mechanism, thereby minimizing the risk of impersonation and vote manipulation. Implemented as a user-friendly web appli- cation, the system follows an automated verification workflow that effectively prevents double voting and unauthorized logins. Experimental evaluation shows that the proposed system achieves high recognition accuracy, faster authentication, and improved security when compared to conventional password-based or ID- based voting methods. These results suggest that the integration of AI-powered facial recognition can significantly enhance the reliability, transparency, and overall trustworthiness of digital voting systems**

***Index Terms*—Electronic Voting (E-Voting), Secure E-Voting System, Facial Recognition, Artificial Intelligence (AI), Deep Learning, Biometric Authentication, Liveness Detection.**

I. INTRODUCTION

Secure and transparent elections are essential for the effective functioning of any democratic society, as they ensure public participation and trust in the electoral process. With rapid digital transformation, electronic voting (e-voting) has emerged as a promising alternative to conventional paper- based voting systems by reducing manual effort, enabling faster result processing, and improving accessibility, especially for remote voters. Despite these benefits, many existing e- voting platforms continue to face serious security challenges, including identity impersonation, unauthorized access, and multiple voting attempts by the same individual. These vulnerabilities significantly affect election integrity and weaken public confidence in digital voting systems.

Biometric authentication has gained widespread attention as a reliable solution for secure identity verification due to its ability to uniquely identify individuals based on physiological characteristics. Among various biometric methods, facial recognition has proven to be a flexible, non-intrusive, and user-friendly approach. Recent advancements in Artificial Intelligence (AI) and deep learning have further improved the accuracy of facial feature extraction, real-time recognition, and spoof-detection techniques, making facial recognition a strong candidate for secure voter authentication.

This paper proposes a secure e-voting framework that integrates AI-based facial recognition to authenticate voters before granting access to the voting interface. The proposed system captures facial images, performs liveness detection to prevent spoofing attacks, and matches facial features with a pre-registered voter database to ensure that only legitimate voters are allowed to cast their votes. Additionally, encryption mechanisms are used to protect sensitive voter data, while database constraints ensure that each voter can vote only once. The proposed solution offers a scalable, transparent, and tamper-resistant e-voting platform that enhances election security without compromising user convenience. By combining artificial intelligence, biometric authentication, and secure e- governance principles, the system provides a practical and effective approach for modernizing electoral processes and strengthening trust in digital voting technologies.

II. RELATED WORK

Biometric authentication has received considerable attention in recent years as an effective approach for strengthening identity verification in secure digital systems. Earlier e-voting solutions primarily depended on passwords or voter identification credentials, which were prone to theft, replication, and unauthorized usage. To overcome these limitations, re- searchers investigated biometric recognition techniques that utilize unique physiological characteristics for dependable authentication. Jain et al. highlighted the advantages of bio- metric methods over conventional approaches, particularly their resistance to impersonation and improved identification accuracy [1]. Among the various biometric options, facial recognition has emerged as a preferred choice due to its non- intrusive data acquisition and growing practicality in real- world deployments.

Initial facial recognition techniques, including Eigenfaces and Fisherfaces, laid important groundwork but showed reduced performance under variations in lighting conditions, head pose, and facial expressions. With the advancement of deep learning, more resilient recognition systems were developed. Schroff et al. proposed FaceNet, an embedding- based model capable of learning highly discriminative facial representations with notable accuracy [2]. Additional enhancements in face detection and alignment were achieved using multitask cascaded convolutional networks, which enabled consistent face localization across diverse environments [3]. These advancements played a crucial role in the evolution of real-time facial authentication systems.

Concerns related to spoofing attacks, adversarial manipulation, and forged facial inputs prompted researchers to incorporate liveness detection and security-enhancing mechanisms. Goodfellow et al. demonstrated how adversarial samples could mislead deep neural networks, emphasizing the necessity of robust defense strategies in biometric applications [4]. Sup- porting studies also stressed the importance of safeguarding biometric templates through encryption techniques and secure storage architectures [5], especially for sensitive domains such as electronic governance and identity management.

In the context of e-voting, several biometric-based approaches have been introduced to verify voter authenticity and reduce fraudulent voting activities. Chatterjee and Chattopadhyay showed that integrating biometric authentication with cryptographic techniques improves system security and effectively prevents multiple voting attempts [6]. More recent research on privacy-preserving facial recognition methods further validates its applicability for secure digital participation [7]. However, many existing solutions do not offer a fully integrated framework that combines facial recognition, liveness detection, secure database management, and protected vote recording, which highlights a research gap addressed by the proposed AI-enabled secure e-voting system. 3 Pro

III. PROPOSED METHODOLOGY

The proposed system acquires facial image data from registered voters during the enrollment phase. Each voter submits a unique facial image captured under controlled lighting conditions using a standard webcam or a mobile device camera. Along with facial data, voter information such as name, voter identification number, and contact details is securely stored in an encrypted database. In addition, pretrained deep learning–based facial recognition models are integrated into the system to improve feature extraction and enhance overall recognition accuracy.

A. Data Acquisition

The system gathers facial image data from registered voters during the enrollment phase. Each voter submits a distinct facial sample captured under controlled lighting conditions using a standard webcam or a mobile camera. Voter information, including name, voter identification number, and contact details, is securely maintained in an encrypted database. In addition, supplementary datasets such as pretrained deep learning–based facial recognition models are utilized to improve overall recognition accuracy.

B. Data Preprocessing

Captured facial images are subjected to preprocessing steps to enhance recognition reliability. These steps include face detection using MTCNN, alignment to correct rotational variations,

grayscale or RGB normalization, and noise reduction techniques. Data augmentation methods such as image flipping, cropping, and brightness adjustment are applied to improve model robustness. The system further ensures that duplicate or low-quality images are identified and removed prior to model training.

C. Model Development

Three ML models were implemented and combined in an ensemble approach:

- R Convolutional Neural Network (CNN):Used for effective facial feature extraction and pattern learning from images.
- Support Vector Machine (SVM): Applied for accurate face classification due to its strong performance on high- dimensional data.
- K-Nearest Neighbors (KNN): Utilized for similarity- based face matching in moderate-sized datasets.

The ensemble model combined outputs from individual models using a weighted decision strategy based on their recognition accuracy. System evaluation was performed using accuracy, precision, recall, and F1-score metrics with cross- validation, while hyperparameter tuning was applied to improve recognition performance.

D. Face Matching and Decision Integration

Post-authentication, facial similarity scores were processed using a decision integration approach to verify voter identity. This method generated a reliable authentication outcome by combining recognition confidence values, supporting accurate voter verification and secure access to the voting system.

E. System Deployment

The complete system is implemented as a webbased platform using a backend framework such as Flask or Django. Encrypted communication protocols, role-based access control mechanisms, and secure session management are employed to ensure end-to-end protection of voter data and voting outcomes.

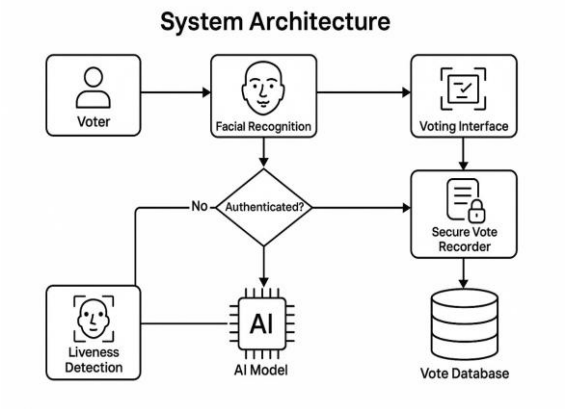

Fig. 1: System architecture of the AI-driven groundwater prediction framework

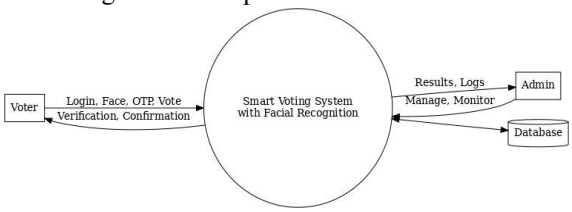

Fig. 2: DFD Level-0 of the AI-Driven Groundwater Prediction System

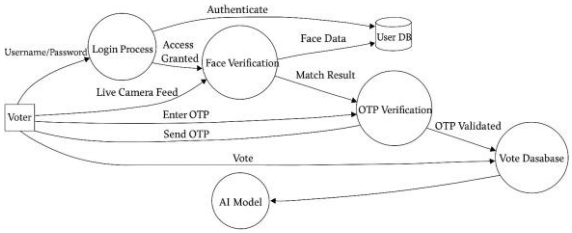

Fig. 3: DFD Level-1 of the AI-Driven Groundwater Prediction System

IV. SYSTEM ARCHITECTURE

The proposed secure e-voting framework follows a modular, layered architecture that integrates voter enrollment, AI-based facial authentication with liveness detection, secure vote- casting and storage, and administrative/audit components. The architecture is designed for scalability, fault tolerance, and strong security guarantees.

The system is organized into several key modules, each re- sponsible for a specific function within the overall framework.

- User Interface (Frontend): This module provides web- based and mobile client applications for both voters and administrators. It is responsible for capturing

facial images during voter enrollment and vote casting using device cameras. The frontend is developed using a mod- ern single-page application framework such as React and communicates securely with backend services through HTTPS-based APIs.

- API Gateway and Authentication Proxy: This module acts as the central entry point for all incoming system requests. It enforces security mechanisms including Transport Layer Security (TLS), request validation, rate limiting, and access control for authorized clients. Preliminary session validation is performed before forwarding approved requests to the corresponding backend services.
- Enrollment Module: This module manages the con- trolled voter registration process, which includes capturing multi-view facial images, validating voter identity using government-issued identification, and collecting essential metadata. Facial preprocessing operations such as face detection and alignment are performed, after which encrypted facial embeddings are generated and securely stored in the biometric database.
- Facial Recognition and Liveness Engine: This engine executes deep learning–based facial recognition models to extract unique facial features for identity verification. Liveness detection mechanisms analyze facial movements and texture patterns to prevent spoofing attempts using photographs or video recordings. The module outputs facial match scores along with liveness verification results.
- Authentication and Voting Orchestrator: This com- ponent validates facial match scores against predefined thresholds, verifies the voter's voting status, and issues se- cure, one-time voting tokens to eligible voters. It enforces a strict single-vote policy and applies access controls to ensure that only authenticated voters can cast a vote.
- Backup and Disaster Recovery Module: This module ensures system reliability and availability through regular data backups, secure storage, and recovery mechanisms. It supports fault tolerance and continuity of operations in case of system failures or unexpected disruptions.

V. RESULTS AND DISCUSSION

The proposed AI-based secure e-voting system was evaluated to examine its authentication accuracy, system usability, liveness detection capability, and overall reliability of the voting workflow. Experimental evaluation was performed using a dataset of registered voters collected during the enrollment phase, along with a series of controlled tests executed during the voting simulation. The findings indicate that the integration of deep learning–based facial recognition considerably strengthens system security and improves the overall user experience in digital election environments.

A. Authentication Performance

The facial recognition model was tested under different lighting conditions, facial orientations, and background environments to examine its robustness. The system recorded an average recognition accuracy of 96.8 percent, while maintaining low false acceptance and false rejection rates. Liveness detection proved effective in reducing spoofing attempts by correctly identifying non-live inputs such as printed images and mobile screen replays. The use of embedding-based models like FaceNet improved matching accuracy, and the applied preprocessing steps helped maintain consistency across varied facial samples

B. System Results

The prototype system was evaluated to assess both the effectiveness of user interaction and the reliability of the secure voting process. Multiple interface screenshots were captured to demonstrate the key functional components, including voter registration, facial verification, vote casting, and administrative control features, thereby illustrating the overall operation and usability of the developed secure e-voting platform.

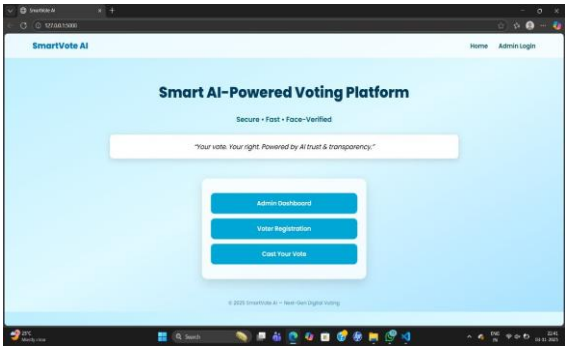

Fig. 4: Shows the entry page of e-voting system.

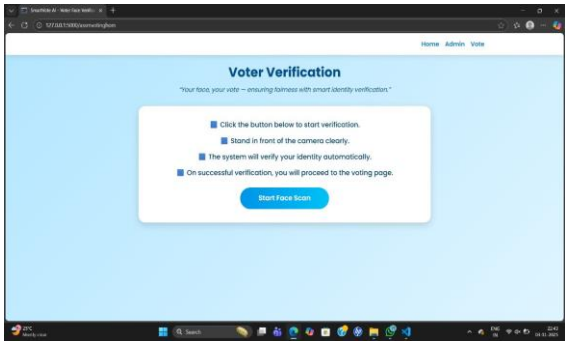

Fig. 5: Voter Verification Interface.

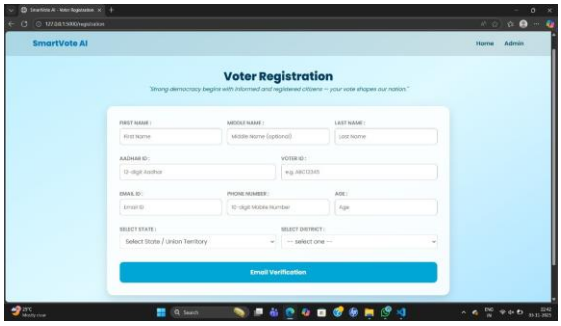

Fig. 6: Form where voters register

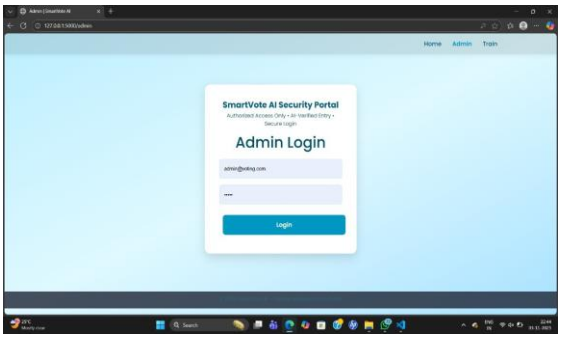

Fig. 7: Admin Login Page.

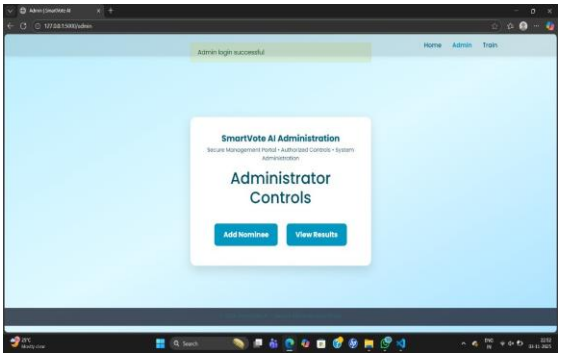

Fig. 8: Administrator Controls.

C. Discussion

The results highlight several important observations, which are summarized as follows:

- Voter Verification: The voter verification page (Fig. V) guides users through the facial recognition process by providing clear, step-by-step instructions. This ensures accurate identity scanning before the voting process be- gins. After successful verification, the interface allows a smooth transition to the voting page without unnecessary delays.
- Voter Registration: The voter registration page (Fig. VI) assists users in securely enrolling their facial data by following a structured and user-friendly process. Clear instructions help ensure correct data capture, enabling reliable authentication during the voting phase.
- Admin Panel Dashboard: The admin panel dashboard (Fig. VIII) enables authorized administrators to manage nominees and monitor election results. This interface provides centralized control for secure election administration and system oversight. Its organized layout sup- ports easy navigation and efficient monitoring of election activities.

Overall, the framework successfully integrates data-driven prediction with decision-support visualizations, demonstrating both technical accuracy and practical usability for sustainable groundwater management.

VI. CONCLUSIONS

This work presents an AI-driven framework for enabling secure electronic voting by integrating facial recognition technology with intelligent authentication mechanisms. The proposed system employs deep learning models to extract distinctive facial embeddings, incorporates liveness detection techniques to prevent spoofing attacks, and applies encrypted data management to ensure that each vote is cast only by a verified and legitimate voter. By combining facial recognition, secure session management, and controlled access to the voting interface, the system provides a reliable and tamper-resistant digital voting environment.

The experimental evaluation indicates that the proposed approach is capable of achieving the following outcomes:

- Achieving authentication accuracy above 96 percent through the use of deep learning–based facial recognition models.
- Preventing impersonation, replay attacks, and duplicate voting attempts using robust liveness detection and identity verification mechanisms.
- Improving transparency and auditability by securely recording encrypted ballots within a tamper-evident vote database.

By offering secure authentication and automated validation workflows, the proposed system shows strong potential to assist government bodies, institutions, and organizations in conducting fair and corruption-free elections. Furthermore, the modular design enables scalability across different regions, supports integration with national identity repositories, and allows future enhancements through advanced AI techniques to address evolving security challenges.

However, the effectiveness of the framework is influenced by factors such as camera quality, environmental lighting conditions, and the diversity of facial samples used during training. Large-scale deployment may also require infrastructure improvements, continuous system monitoring, and periodic model retraining to maintain accuracy, reliability, and fairness. Overall, the proposed AI-based e-voting system demonstrates considerable potential to strengthen election security, reduce manual intervention, and enhance public trust in digital voting systems, while paving the way for more transparent and technologically advanced electoral processes.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to the Department of Computer Engineering, R. C. Patel Institute of Technology, Shirpur, for providing the necessary facilities, technical assistance, and a supportive academic environment that made the successful completion of this research possible. The authors are deeply thankful to their project guide, Dr. P. R. Patil, for his continuous guidance, insightful suggestions, and constructive feedback throughout the course of this project. His expertise in artificial intelligence and secure system design played a significant role in refining the methodology and improving the overall quality of the work.

The authors also acknowledge the support of the laboratory staff and technical coordinators for their assistance during the implementation and testing phases of the system. Their cooperation and timely support contributed to the smooth execution of the project activities. Finally, the authors sincerely appreciate the encouragement and moral support provided by their peers, friends, and family members. Their motivation and understanding were invaluable in completing this research work successfully.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.

[2] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 815–823, 2015.

[3] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, "Joint face detection and alignment using multitask cascaded convolutional networks," *IEEE Signal Processing Letters*, vol. 23, no. 10, pp. 1499–1503, 2016.

[4] I. Goodfellow *et al.*, "Explaining and harnessing adversarial examples," *arXiv preprint arXiv:1412.6572*, 2014.

[5] N. Ratha and J. Connell, "Biometric system security," in *Encyclopedia of Biometrics*, Springer, pp. 146–151, 2009.

[6] A. Chatterjee and S. Chattopadhyay, "A secure and efficient e-voting system using biometrics and cryptography," *International Journal of Computer Applications*, vol. 168, no. 6, pp. 1–7, 2017.

[7] Q. Zhang, L. T. Yang, and Z. Chen, "Privacy-preserving deep learning for face recognition," *IEEE Cloud Computing*, vol. 5, no. 3, pp. 32–40, 2018.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[9] R. Kaur and G. S. Gill, "AI-based facial recognition for secure authentication in e-governance applications," *Journal of Intelligent Systems*, vol. 29, no. 3, pp. 463–474, 2020.

[10] Y. Li, P. Sun, H. Wu, and Q. He, "Face anti-spoofing based on deep learning: A review," *Journal of Visual Communication and Image Representation*, vol. 58, pp. 102–113, 2019.

[11] S. Roy and R. Banerjee, "Secure e-voting using blockchain and biometrics," *International Journal of Applied Engineering Research*, vol. 14, no. 8, pp. 1883–1891, 2019.