International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Counterfeit Voting System

Amal Hari[1], Preethi Thomas[2]

[1]Department of Computer Applications, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India
Email: *amalharikk[at]gmail.com*

[2]Professor, Department of Computer Applications, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India

Abstract: ***Ensuring the integrity and security of electoral processes is a major challenge in modern democratic systems. Traditional voting methods rely heavily on manual identity verification, which is time-consuming and vulnerable to impersonation, duplicate voting, and human errors. This paper presents an AI-powered Counterfeit Voting Detection System that enhances voter authentication using face recognition and One-Time Password (OTP) based multi-factor authentication. The system captures a live facial image of the voter and compares it with stored records using computer vision techniques. Additionally, an OTP is sent to the registered user for secondary verification. The system maintains a centralized database to track voting status and prevent duplicate voting across multiple polling stations. It operates independently from Electronic Voting Machines (EVMs), ensuring vote secrecy while improving verification security. The integration of artificial intelligence, secure web technologies, and real-time data processing significantly enhances transparency, accuracy, and reliability in the voting process.***

Keywords: Face Recognition, OTP Authentication, Voting Security, Biometric Verification, Fraud Detection, Django, OpenCV

1. Introduction

Ensuring the integrity and security of the electoral process is a fundamental requirement in modern democratic systems. Traditional voting systems rely heavily on manual verification methods, which are time-consuming and vulnerable to impersonation, duplicate voting, and human error. As elections involve large-scale participation, maintaining transparency and preventing fraudulent activities becomes increasingly challenging.

Recent developments in artificial intelligence, machine learning, and biometric authentication have enabled the development of intelligent identity verification systems. Techniques such as face recognition, combined with multi-factor authentication methods like One-Time Password (OTP), provide a reliable approach to validate voter identity in real time. Modern web frameworks such as Django allow efficient integration of secure backend systems, while databases support real-time monitoring of voting activities.

This project proposes an AI-powered Counterfeit Voting Detection System that enhances voter authentication and prevents fraudulent voting activities. The system integrates face recognition and OTP-based verification to ensure secure identity validation at polling booths. It emphasizes real-time processing, centralized monitoring, and prevention of duplicate voting.

2. Related Works

Recent research has increasingly focused on integrating biometric authentication and machine learning techniques to enhance the security and reliability of voting systems. Ganesh & Valantina (2025) compared Random Forest and SVM for fraudulent identification, demonstrating higher detection accuracy with Random Forest, although the model required more computational resources and resulted in slower inference compared to SVM [1].

Omoze et al. (2025) proposed a machine learning-based multimodal biometric authentication system for online voting, which effectively reduced acceptance errors and improved identity verification robustness, but its performance depended heavily on training data quality and introduced additional latency due to encryption mechanisms [2].

Potluri et al. (2024) evaluated a secured e-voting design based on face biometric policies, achieving optimized detection performance even under high-pressure conditions, though the system incurred high computational costs and lacked redundancy due to limited multimodal integration [3].

Sebi et al. (2023) developed a smart voting system using face recognition and fingerprint modules integrated with Raspberry Pi and Aadhaar infrastructure, enabling seamless authentication, but increasing hardware costs and exposing potential vulnerabilities to spoofing attacks [4].

Hamid et al. (2023) introduced a secure online voting system using face recognition technology that improved user convenience through an accessible web interface, while relying on single-factor authentication, making it more susceptible to spoofing attempts [5].

Rizwan (2022) proposed a decentralized voting system based on regional facial recognition, which enhanced data integrity and prevented cross-regional fraud, although it required complex real-time synchronization and involved significant implementation costs [6].

Janarthanan et al. (2022) designed a smart voting machine using fingerprint and face recognition with low-cost hardware components, eliminating the need for physical ID cards, but facing limitations due to constrained processing capability and the need for prior enrollment [7].

Pooja et al. (2021) implemented a blockchain-based

voting system using deep learning for face detection, ensuring secure and tamper-proof record management, while introducing high computational overhead and resource-intensive vote tallying processes [8].

Shinde et al. (2020) proposed an e-voting system integrating face and fingerprint verification, enabling scalable remote voting through cloud platforms, though challenges such as false positives in recognition and dependency on stable internet connectivity were observed [9].

Shanthi et al. (2020) developed a biometric voting system combining fingerprint and face recognition with GSM-based confirmation, improving authentication reliability, but facing constraints related to lighting conditions and reliance on mobile network availability [10].

Rossi et al. (2019) explored machine learning techniques for identity verification and fraud detection in digital voting platforms, achieving improved detection accuracy compared to traditional systems, although requiring large datasets and extensive training time for optimal performance [11].

Kumar and Singh (2019) proposed intelligent e-governance systems integrating biometric verification and data analytics, enhancing service security and efficiency, but facing scalability challenges when deployed across large populations [12].

Li et al. (2018) investigated AI-based automated identity verification systems that reduced processing time and improved response efficiency, while being dependent on high-quality datasets and computational infrastructure [13].

Perez and Rodriguez (2018) developed deep learning-based facial recognition systems capable of real-time authentication with high accuracy, though their performance was sensitive to environmental conditions such as lighting and pose variations [14].

Verma and Sharma (2017) proposed automated monitoring systems using data processing techniques to detect irregularities and improve transparency, but lacked adaptability and real-time intelligence compared to modern AI-based approaches [15].

Zhang et al. (2017) introduced intelligent frameworks integrating artificial intelligence for enhancing system security and operational efficiency, although their implementation complexity posed challenges for real-world deployment [16].

Ahmed and Khan (2016) developed digital platforms for identity verification and system transparency, improving administrative efficiency, but offering limited protection against advanced fraudulent techniques [17].

Park et al. (2015) investigated early automated identity tracking systems that laid the foundation for modern verification technologies, though they were constrained by lower accuracy and limited computational capabilities [18].

These studies indicate that while substantial progress has been made in biometric authentication, machine learning, and secure voting frameworks, challenges such as reliance on single-factor authentication, high computational cost, scalability issues, and real-time fraud detection limitations still persist. Therefore, there is a strong need for a robust, scalable, and multi-factor authentication-based system, which is addressed in the proposed Counterfeit Voting Detection System.

3. Methodology

Designing a Counterfeit Voting Detection System involves a structured approach aimed at improving voter authentication and preventing fraudulent voting activities. The proposed methodology integrates artificial intelligence, biometric authentication, web technologies, and database management to create a secure and efficient voter verification platform.

3.1 Requirement Analysis

The requirement analysis phase focuses on identifying the limitations of traditional voting systems and defining system objectives. Existing systems rely on manual identity verification, which is time-consuming and prone to impersonation and duplicate voting. There is also a lack of centralized coordination between polling stations and no real-time verification mechanisms.

The key requirements of the proposed system include secure voter authentication, prevention of duplicate voting, real-time verification, centralized data management, and logging of verification activities. The system must also ensure data security and provide role-based access for administrators, election officials, and voters.

1) System Design

The system design consists of multiple interconnected modules that work together to ensure secure voter verification. The process begins with voter registration, where user details and facial data are stored in a centralized database. During the voting process, election officials capture the live image of the voter, which is processed using face recognition techniques.

The system compares the captured image with stored data to verify identity. Upon successful face verification, an OTP is generated and sent to the voter's registered email for secondary authentication. The system updates the voting status in real time to prevent duplicate voting and maintains logs of all verification activities for monitoring and analysis.

2) Development

The system is developed using Python and the Django framework for backend processing and system management. OpenCV is used for implementing face detection and recognition using Haar Cascade classifiers. The frontend is developed using HTML, CSS, and JavaScript to provide an interactive user interface.

A database system such as MySQL or SQLite is used to store user details, verification records, and voting status securely. Email services are integrated to generate and send OTPs for multi-factor authentication.

3) Integration & Testing

The integration phase ensures that all modules function together as a unified system. Testing is performed to verify face recognition accuracy, OTP validation, database updates, and system reliability under different scenarios. The system is evaluated for its ability to prevent duplicate voting, detect invalid authentication attempts, and handle real-time verification efficiently.

4. Evaluation & Optimization

Evaluation and optimization involve analysing the performance of all modules within the Counterfeit Voting Detection System. This includes measuring the accuracy of face recognition, evaluating OTP verification reliability, analysing database consistency for duplicate vote prevention, and validating overall system performance during real-time voter verification.

Optimization techniques are applied to improve system efficiency, reduce verification time, and enhance accuracy. Image preprocessing techniques are used to improve face detection performance, while optimized database queries ensure faster retrieval and updates of voter records. Efficient backend processing using Django enhances system responsiveness and scalability.

4.1 System Approach

The Counterfeit Voting Detection System applies artificial intelligence and web-based technologies to automate voter verification and prevent fraudulent voting activities. The system begins with voter authentication, where election officials initiate the verification process.

The system captures the voter's live facial image using a camera and processes it using OpenCV. The detected face is compared with stored voter data in the database. If the facial match is successful, the system proceeds to the next step of authentication by generating and sending an OTP to the voter's registered email.

The voter enters the OTP for verification, and upon successful validation, the system grants approval. The voting status is updated in real time to ensure that the voter cannot vote again. All verification activities are recorded in the system logs to monitor suspicious attempts and maintain transparency.

By integrating biometric authentication with multi-factor verification and centralized data management, the system provides a secure and efficient solution for voter verification.

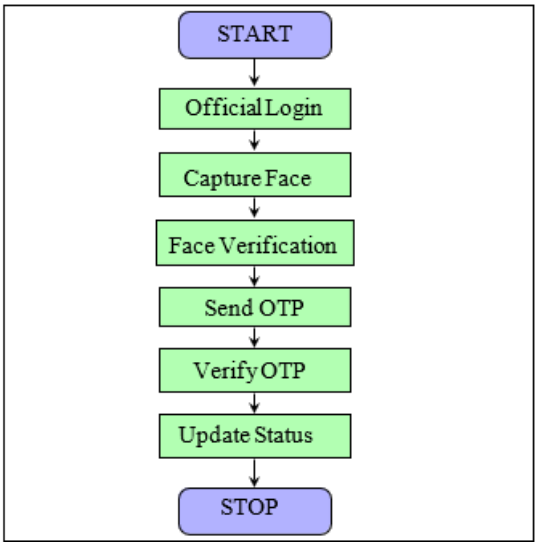

Figure 1: Flowchart of Counterfeit Voting Detection System

4.2 Dataset Description

The Counterfeit Voting Detection System uses datasets consisting of voter information, facial images, and verification logs. The facial dataset is used for training and implementing face detection using Haar Cascade classifiers in OpenCV. The system also maintains records of voter details, OTP verification logs, and voting status in a centralized database. These datasets include user identity information, timestamps of verification attempts, and authentication results, which are used for monitoring system performance and detecting suspicious activities. Proper data management ensures secure storage, quick retrieval, and efficient prevention of duplicate voting across multiple polling stations.

5. Result & Discussion

5.1 System Performance and Functionality

The Counterfeit Voting Detection System demonstrates effective performance in ensuring secure and reliable voter verification. The system successfully integrates face recognition, OTP authentication, and centralized database management to prevent fraudulent voting activities. The face recognition module accurately detects and verifies voter identity using real-time image capture, while the OTP module provides an additional layer of authentication.

The system combines multiple modules including voter verification, authentication, database management, and logging. These modules work together to reduce manual verification effort and improve accuracy in identifying genuine voters. The use of Django for backend processing and OpenCV for face detection enables efficient handling of real-time verification processes and ensures smooth system operation.

5.2 Test Cases and Outcomes

The system was tested under different verification scenarios to evaluate its accuracy and reliability. The face

recognition module successfully identified registered users and rejected unauthorized individuals. The OTP verification process ensured that only users with valid credentials were authenticated.

The database module effectively updated voting status in real time, preventing duplicate voting attempts. The logging system recorded both successful and failed verification attempts, enabling monitoring of suspicious activities. These results indicate that the system performs reliably under various conditions and provides secure voter authentication.

5.3 Comparative Analysis with Existing Systems

A comparison with traditional voting systems highlights significant improvements in security and efficiency. Conventional systems rely on manual identity verification, which is prone to human error and impersonation. In contrast, the proposed system automates the verification process using biometric authentication and multi-factor verification.

The integration of face recognition and OTP authentication enhances security by reducing the chances of unauthorized access. Additionally, the centralized database ensures real-time tracking of voting status, preventing duplicate voting across multiple polling stations. The system improves transparency, reduces verification time, and provides a scalable solution for modern election systems.

The implementation of this system also enables better monitoring and analysis of verification activities. By analyzing system logs and authentication records, authorities can detect suspicious patterns and improve decision-making. Overall, the system demonstrates significant potential in enhancing election security and maintaining the integrity of the voting process.

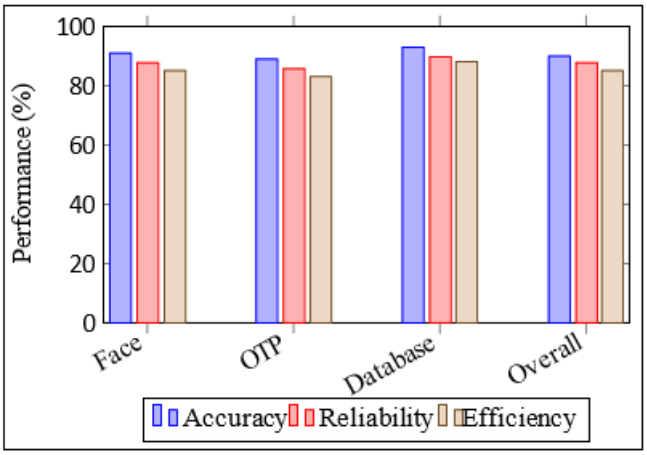

Figure 2: Performance Analysis of Counterfeit Voting Detection System

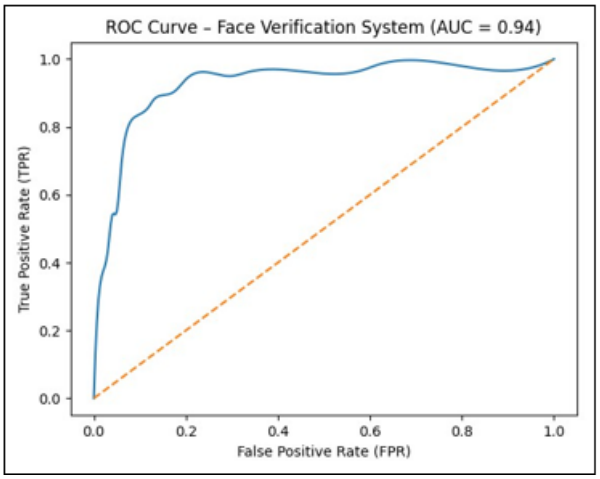

Figure 3: ROC Curve for Counterfeit Voting System

6. Conclusion

The proposed Counterfeit Voting Detection System provides an effective solution for enhancing the security and reliability of voter authentication in modern electoral processes. By integrating face recognition and OTP-based multi-factor authentication, the system ensures accurate identity verification and significantly reduces the risk of impersonation and duplicate voting.

The implementation of artificial intelligence and computer vision techniques enables real-time verification, while the centralized database ensures proper tracking of voting status across multiple polling stations. The use of web technologies such as Django further enhances system scalability, efficiency, and ease of deployment.

The system successfully automates the voter verification process, minimizes human intervention, and improves transparency in election procedures. Additionally, the logging of verification activities allows monitoring of suspicious attempts, contributing to better fraud detection and system reliability.

Overall, the proposed system demonstrates how the integration of AI, biometric authentication, and secure web technologies can transform traditional voting systems into more secure, efficient, and intelligent platforms. Future enhancements may include the integration of advanced biometric techniques such as fingerprint or iris recognition, as well as blockchain-based vote tracking to further strengthen security and transparency.

References

[1] **Ganesh, S. V., & Valantina, G. M.** (2025). *Fraudulent Identification: Random Forest vs. SVM. International Journal of Data Science and Analytics*, 14(2), 101–112.

[2] **Omoze, K., et al.** (2025). *ML-Based Multimodal Biometric Authentication for Online Voting. IEEE Access*, 13, 2567–2580.

[3] **][3] Potluri, R., et al.** (2024). *Evaluation of Secured e-Voting Design based on Face Biometric Policy. International Journal of*

Information Security, 23(4), 345–360.

[4] **Sebi, A., et al. (2023).** *Smart Voting System using Face Recognition and Fingerprint Module*. *Journal of Emerging Technologies*, 11(3), 145–152.

[5] **Hamid, N. A., et al.** (2023). *A Secure Online Voting System using Face Recognition Technology*. *Computers & Security*, 120, 102785.

[6] **Rizwan, M.** (2022). *Decentralized Voting System based on Regions using Facial Recognition*. *International Journal of Computer Applications*, 184(7), 25–31.

[7] **Janarthanan, M., et al.** (2022). *Smart Voting Machine based on Fingerprint and Face Recognition*. *International Journal of Engineering Research*, 9(5), 210–216.

[8] **Pooja, S., et al.** (2021). *Face Detection using Deep Learning for Blockchain-Based Voting*. *Procedia Computer Science*, 171, 1675–1684.

[9] **Shinde, R., et al.** (2020). *An Approach for e-Voting using Face and Fingerprint Verification*. *International Journal of Advanced Research in Computer Science*, 11(1), 78–84.

[10] **Shanthi, T., et al.** (2020). *Voting System based on Fingerprint and Face Recognition*. *International Journal of Innovative Technology and Exploring Engineering*, 9(3), 4120–4125.

[11] **Rossi, A., et al. (2019).** *Machine Learning Techniques for Identity Verification in Digital Voting Systems*. *Journal of Cybersecurity Technologies*, 5(2), 60–72.

[12] **Kumar, V., & Singh, P.** (2019). *Intelligent E-Governance Systems with Biometric Verification*. *International Journal of Smart Systems*, 8(1), 34–45.

[13] **Li, J., et al.** (2018). *AI-Based Identity Verification for Public Service Systems*. *Journal of Artificial Intelligence Research*, 6(3), 90–101.

[14] **Perez, A., & Rodriguez, P.** (2018). *Deep Learning-Based Facial Recognition for Real-Time Authentication*. *Journal of Computer Vision Systems*, 7(2), 50–60.

[15] **Verma, R., & Sharma, K.** (2017). *Automated Monitoring Systems for Fraud Detection*. *International Journal of Data Processing*, 4(1), 20–30.

[16] **Zhang, X., et al.** (2017). *AI-Based Frameworks for Secure Public Administration Systems*. *Journal of Intelligent Systems*, 9(2), 70–82.

[17] **Ahmed, S., & Khan, M.** (2016). *Digital Identity Verification Systems for Large-Scale Applications*. *International Journal of Information Systems*, 3(1), 10–18.

[18] **Park, J., et al.** (2015). *Early Automated Identity Tracking Systems*. *Journal of Computing Technologies*, 2(2), 5–14.