IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15106

KNN-Powered Online Voting System to Improve Accuracy and Transparency Election Process

Thillai Nayagi S[1], Shreya G[2], Shrusti K[3], Al-Mateenu Jan[4]

Guide, Computer Science and Engineering, East West College of Engineering, Bangalore, India[1]

Computer Science and Engineering, East West College of Engineering, Bangalore, India[2-4]

Abstract: The proposed system aims to create a safe online voting system by developing a face recognition-based authentication model using K-Nearest Neighbors (KNN). The system verifies voters through unique credentials and a real-time photo captured via webcam. It strictly enforces a one-vote-per-user policy by comparing live images with stored database records. Results are updated every minute, ensuring transparency and efficiency while reducing long queues at polling stations.

Keywords: Face recognition, KNN, Online Voting System, Machine Learning.

I. INTRODUCTION

In democratic systems, voting is an essential operation, but conventional procedures frequently encounter problems including fraud, voter impersonation, and inefficiencies in logistics. Facial recognition technology integration provides a clear, safe, and effective way to overcome these problems. This project replaces traditional methods with a machine learning-based system that uses facial image data to verify identities. The administrator manages the process by adding executives via 12-digit Aadhaar numbers, who then facilitate candidate and voter registration.

II. LITERATURE REVIEW

Current research on biometric and electronic voting systems highlights several gaps:

- Prabhu et al. (2021): Identified that systems are prone to fictitious email addresses, allowing multiple votes from one person.
- Chovancová et al. (2023): Noted that the complexity and high expense of blockchain technology make it less accessible to the general public.
- Mallike et al. (2023): Found that fingerprint sensor systems can lack flexibility in data entry.
- Kandan et al. (2021): Utilized facial recognition but lacked secondary verification methods like Aadhaar integration.

III. METHODOLOGY

The proposed system uses a multi-step authentication process to ensure integrity.

A. Face Detection and Feature Extraction OpenCV captures webcam footage while a Haar Cascade classifier detects faces. The algorithm identifies facial features and processes images by resizing and converting them to grayscale for easier analysis.

B. K-Nearest Neighbors (KNN) Classification The system recognizes voters using the sci-kit-learn KNN classifier. Face data from .pl files are used to train the model, categorizing individual voters based on registered face data.

C. Voting Procedure

1. **Registration:** Users provide a username and password associated with a validated email address to prevent duplicate accounts.
2. **Authentication:** A live picture is captured during login and contrasted with saved face data.
3. **One-Vote Enforcement:** The system records each user's voting status in a secure database; access is blocked if a user tries to cast a second ballot.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026
DOI: 10.17148/IJARCCE.2026.15106

IV. RESULT AND DISCUSSION

Performance metrics demonstrate the system's robustness across three main categories:

A. Face Recognition Metrics Precision, Recall, and Accuracy values are consistently high, reflecting reliable authentication. Face detection works effectively with high accuracy in normal illumination.

B. System Performance Metrics highlight fast response times, near-perfect system availability, and exceptional scalability to handle large user loads.

C. Comparison with Traditional Models The proposed model offers remote accessibility from any location, whereas the traditional model requires physical presence at polling places. Vote tallying is fully automated in real-time, eliminating manual counting errors.

V. CONCLUSION

The primary goal of this system is to provide a safe and secure online voting environment. By utilizing multi-step authentication involving usernames, passwords, and real-time KNN-based facial recognition, the system identifies false voters and ensures election integrity. This online approach is superior to previous systems due to its efficiency and transparency.

REFERENCES

[1]. S. G. Prabhu et al., "Smart Online Voting System," 2021.
[2]. C. J. Lakshmi and S. Kalpana, "Secured and Transparent Voting System Using Biometrics," 2018.
[3]. D. Malik et al., "Enhancing the Security of Online Voting System Using Defined Biometrics," 2023.
[4]. N. Bhubaneswar et al., "Smart Voting Machine Using Fingerprint Sensor and Face Recognition," 2022.
[5]. P. Nagaraj et al., "Voting System Using Facial and Fingerprint Authentication," 2022.

