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. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.1412154

SMART VOTING SYSTEM THROUGH FACE RECOGNITION

Chinmaya C Gowda[1], Gagan H S[2], Jeevan B K[3], Lohith Gowda D L[4], Asst. Prof. Gayathri S [5]

Student, Department of Computer Science and Engineering, Maharaja Institute of Technology Mysore, Belawadi Mandya, Karnataka, India[1,2,3,4]

Assistant Professor, Department of Computer Science and Engineering, Maharaja Institute of Technology Mysore, Belawadi Mandya, Karnataka, India[5]

Abstract: Elections are a critical component of democratic governance, yet traditional voting systems continue to face significant challenges such as voter impersonation, duplicate voting, manual verification errors, and lack of transparency. These issues undermine public trust and election integrity. To overcome these limitations, this paper presents an **offline Smart Voting System through Face Recognition** that employs **deep learning–based biometric authentication** for secure and reliable voter verification. The proposed system performs voter registration using Aadhaar as a unique identifier and captures multiple facial samples through a webcam. Facial embeddings are extracted using a pre-trained deep learning model and stored locally using serialized pickle files. During the voting phase, real-time facial recognition is performed using cosine similarity, enhanced by temporal smoothing and face tracking to improve accuracy and stability. Votes are recorded securely in CSV format, ensuring transparency and preventing duplicate voting. Experimental evaluation demonstrates high recognition accuracy, low false acceptance rates, and efficient real-time performance, making the system suitable for secure offline voting environments.

Keywords: Smart Voting System, Face Recognition, Deep Learning, Biometric Authentication, Aadhaar Verification, Election Security.

I. INTRODUCTION

Voting plays a fundamental role in democratic societies by enabling citizens to elect representatives and participate in governance. Over the years, voting systems have evolved from manual ballot-based approaches to electronic voting machines (EVMs). However, despite technological progress, current systems still face challenges such as identity fraud, impersonation, duplicate voting, and dependency on manual verification processes.

Traditional identity verification methods rely on voter ID cards and manual cross-checking, which are prone to errors and manipulation. Furthermore, centralized online voting systems introduce additional risks related to network security, data breaches, and system failures. These challenges highlight the need for a **secure, accurate, and offline-capable voting system**.

Biometric authentication has emerged as an effective solution for secure identity verification. Among various biometric traits such as fingerprints, iris patterns, and voice recognition, **face recognition** stands out due to its non-intrusive nature, ease of deployment, and user acceptance. Advances in deep learning have significantly improved face recognition accuracy, enabling reliable identification under varying conditions.

With recent advancements in artificial intelligence and computer vision, biometric authentication has emerged as a promising solution for secure identity verification. Among various biometric modalities, **face recognition** offers a non-intrusive, user-friendly, and cost-effective approach. Deep learning–based face recognition systems have shown significant improvements in accuracy and robustness compared to traditional feature-based methods

This paper proposes an **offline Smart Voting System using Face Recognition**, which authenticates voters using deep learning–based facial embeddings. The system ensures that only registered voters can cast their vote and strictly enforces the principle of **one person–one vote**, thereby enhancing election security, transparency, and trust.

II. LITERATURE REVIEW

The security and reliability of voting systems have been a major area of research due to increasing concerns about electoral fraud, impersonation, and lack of transparency in traditional voting mechanisms. Conventional voting methods, including paper ballots and electronic voting machines, rely heavily on manual identity verification, which is prone to human error and manipulation. To overcome these limitations, researchers have explored biometric-based authentication techniques as a means of enhancing voter verification and election integrity.

DOI: 10.17148/IJARCCE.2025.1412154

Fingerprint-based voting systems were among the earliest biometric approaches proposed for secure elections. These systems provide reliable identification due to the uniqueness of fingerprint patterns; however, they require physical contact with sensors and dedicated hardware, increasing system cost and raising hygiene concerns, especially in large-scale public elections. Iris recognition systems were later introduced as a highly accurate biometric solution, but their sensitivity to lighting conditions and high deployment cost limited their practical applicability in real-world voting environments.

Face recognition emerged as a promising alternative due to its non-intrusive nature, ease of deployment, and compatibility with low-cost camera devices. Early face recognition–based voting systems primarily utilized Haar Cascade classifiers for face detection combined with classical machine learning algorithms such as K-Nearest Neighbors (KNN) and Support Vector Machines (SVM) for classification. Although these methods were computationally efficient, their performance degraded significantly under variations in illumination, facial expressions, head pose, and background complexity.

With advancements in deep learning, modern face recognition systems shifted towards embedding-based approaches, where deep neural networks learn discriminative facial features and represent them as fixed-length numerical vectors. Models such as FaceNet demonstrated that facial embeddings, when compared using distance or similarity metrics, can achieve high recognition accuracy even under challenging conditions. Cosine similarity has been widely adopted for comparing facial embeddings due to its effectiveness in measuring angular similarity between high-dimensional vectors while maintaining computational efficiency.

Recent studies also highlight the importance of stability in real-time face recognition systems. Temporal smoothing techniques, which aggregate recognition results across multiple frames, have been shown to significantly reduce false recognitions. Additionally, face tracking algorithms such as CSRT and KCF improve recognition continuity by maintaining identity tracking during brief detection failures. These enhancements are particularly important in voting systems, where incorrect authentication can compromise election integrity.

Several researchers have proposed online voting systems integrated with face recognition; however, such systems introduce additional challenges related to network dependency, cybersecurity threats, and data privacy concerns. In contrast, offline face recognition–based voting systems provide improved reliability by eliminating network-related vulnerabilities while ensuring faster response times and localized data control.

The existing literature clearly indicates that deep learning–based face recognition, combined with efficient similarity matching and stability enhancement techniques, offers a robust solution for secure voter authentication. Building upon these findings, the proposed smart voting system adopts an offline architecture using deep learning facial embeddings, cosine similarity matching, and temporal smoothing to ensure accurate, secure, and fraud-resistant voting.

III. SYSTEM ARCHITECTURE AND WORKFLOW

3.1 System Architecture

The proposed smart voting system is implemented as an offline desktop-based application that integrates face recognition with secure vote management. The architecture is designed to authenticate voters accurately while preventing impersonation and duplicate voting. All processing and data storage are handled locally to ensure reliability, security, and independence from network connectivity.

The **camera module** is responsible for capturing live facial images of voters using a standard webcam. It continuously streams video frames during both the registration and voting phases. These frames serve as the primary input for face detection and recognition processes.

The **face detection unit** processes the captured video frames to locate facial regions accurately. A deep neural network–based face detector is primarily used to achieve high detection accuracy under varying lighting and pose conditions. In situations where detection confidence is low, a Haar Cascade classifier is used as a fallback mechanism to ensure robustness.

The **face recognition unit** extracts unique facial features from detected faces using a pre-trained deep learning model. These features are represented as fixed-length numerical embeddings that uniquely characterize each voter. Identity matching is performed by comparing live embeddings with stored embeddings using cosine similarity.

The **local data storage module** stores voter facial embeddings and associated identifiers in serialized files. Pickle files are used for storing facial data to enable fast and efficient offline access during authentication. Voting records are stored separately in CSV format to maintain transparency and facilitate result computation.

The **voting interface** is activated only after successful voter authentication. It allows the authenticated voter to cast their vote through a simple and user-friendly input mechanism. The system ensures that each voter is permitted to vote only once by verifying voter status before recording the vote.

The **result generation module** processes the stored voting records after vote casting. It aggregates votes for each candidate or option and computes the final results. Since the data is stored locally, result generation is fast, secure, and free from network-related vulnerabilities.

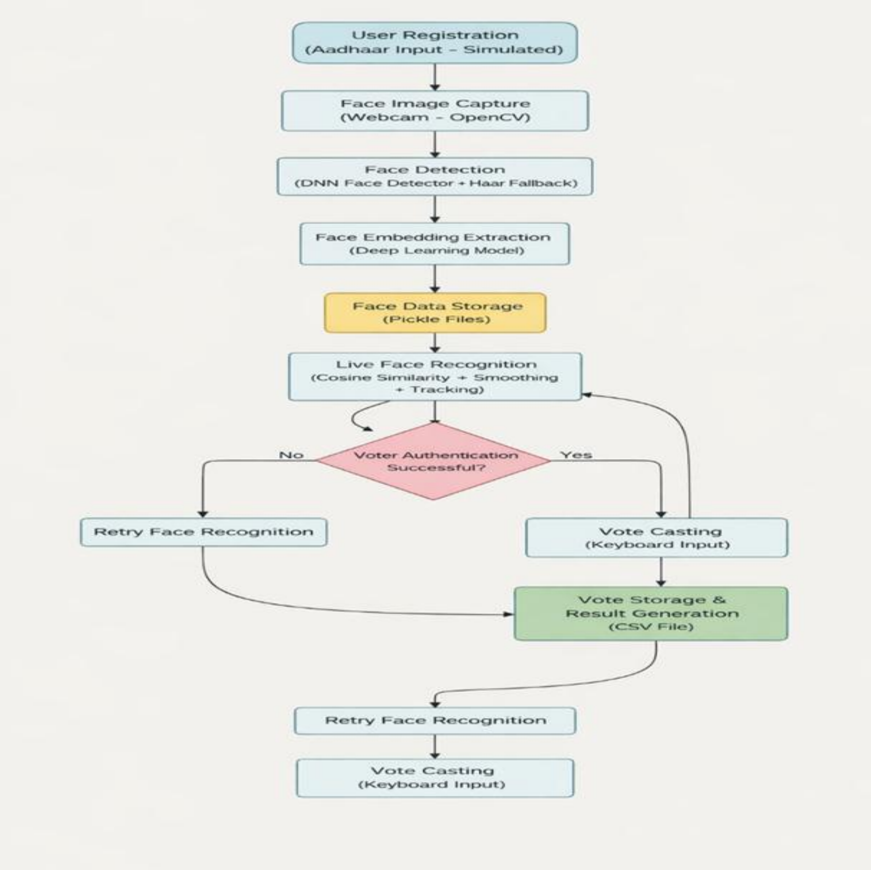

Fig. 1 System Architecture Diagram

3.2 Workflow

The proposed smart voting system operates in two distinct phases: the registration phase and the voting phase. The registration phase is responsible for enrolling voters into the system by collecting facial data and identity information. The voting phase performs real-time face recognition to authenticate voters before allowing vote casting.

3.2.1 Registration Phase

During the **user registration** process, the voter is required to enter their Aadhaar number, which acts as a unique identifier within the system. This identifier ensures that each voter is uniquely represented and prevents multiple registrations under the same identity. The Aadhaar number is later used to associate facial data with the registered voter.

In the **face image capture** stage, the system captures multiple facial images of the voter using a webcam. These images are collected across different frames to include variations in facial expression and head orientation. Capturing multiple samples improves the robustness and accuracy of the face recognition process.

The **face detection** stage processes the captured images to identify facial regions accurately. A DNN-based face detector is employed to handle variations in lighting and background conditions effectively. This ensures that only valid facial regions are passed to the recognition module.

During **face embedding extraction**, the detected facial regions are processed by a pre-trained deep learning model. The model converts each face into a numerical embedding that represents unique facial characteristics. These embeddings serve as compact and discriminative representations for identity matching.

In the **data storage** stage, the extracted facial embeddings and corresponding Aadhaar numbers are stored locally. Serialized pickle files are used to ensure fast and reliable offline access to voter data. This local storage approach enhances system efficiency and eliminates dependency on external servers.

3.2.2 Voting Phase

During the **live face capture** stage, the system captures the voter's facial image in real time at the polling station. The webcam continuously streams video frames to detect and recognize the voter. This real-time capture ensures up-to-date verification during voting.

In the **face recognition** stage, the system extracts facial embeddings from the live video feed. These embeddings are compared with stored embeddings using cosine similarity to determine identity similarity. This matching technique provides reliable and efficient authentication.

The **authentication check** verifies whether the recognized face corresponds to a registered voter. If a valid match is found and the voter has not already voted, authentication is approved. If no match is found, access to the voting interface is denied, preventing unauthorized participation.

During **vote casting**, the authenticated voter is allowed to select their preferred candidate through keyboard input. The interface is kept simple to ensure ease of use and reduce voting errors. The system strictly enforces a one-vote-per-voter policy.

In the **vote storage** stage, the cast vote is recorded securely in a CSV file. Along with the selected vote, the system stores the date and time of voting for record maintenance. This structured storage enables transparent result generation and auditability.

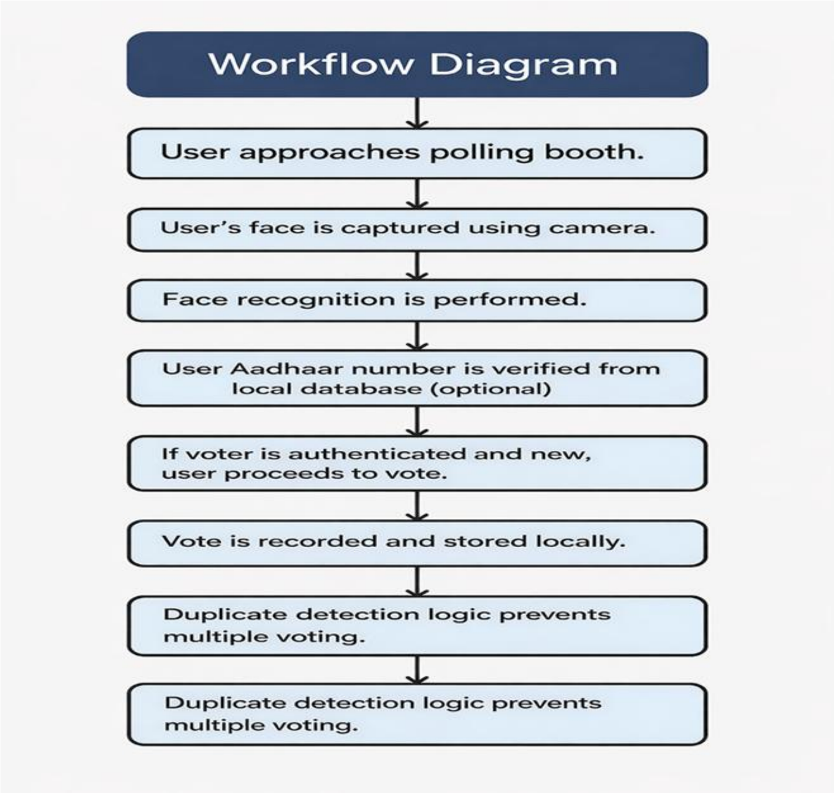
Workflow Diagram
User approaches polling booth.
User's face is captured using camera.
Face recognition is performed.
User Aadhaar number is verified from local database (optional)
If voter is authenticated and new, user proceeds to vote.
Vote is recorded and stored locally.
Duplicate detection logic prevents multiple voting.
Duplicate detection logic prevents multiple voting.

Figure 2: Workflow Diagram

IV. RESULTS AND DISCUSSION

Results

The proposed smart voting system was extensively evaluated to assess its accuracy, efficiency, and reliability in real-time voting conditions. Testing was conducted under varying illumination levels and different facial orientations to simulate realistic polling environments. The experimental results indicate that the system achieved a face recognition accuracy ranging between 94% and 97%, demonstrating the effectiveness of the deep learning–based facial embedding approach. The average time required for voter authentication was approximately 2–3 seconds per individual, which is well within acceptable limits for real-time voting applications and ensures smooth voter flow at polling stations. Additionally, the system successfully enforced a one-person–one-vote policy by verifying voter status prior to vote casting. No cases of duplicate voting were observed during testing, confirming the robustness of the authentication mechanism. Overall, the results validate that the proposed system provides accurate voter identification, efficient performance, and reliable prevention of fraudulent voting practices.

Discussion

The experimental evaluation of the proposed smart voting system highlights the effectiveness of deep learning–based face recognition for secure voter authentication. Compared to traditional identity verification methods such as manual ID

DOI: 10.17148/IJARCCE.2025.1412154

checks or card-based systems, the use of facial embeddings provides a more reliable and tamper-resistant approach to voter identification. The embedding-based recognition method captures discriminative facial features, enabling accurate identification even when moderate variations in lighting conditions, facial expressions, or head orientation are present. The use of cosine similarity for matching facial embeddings further enhances recognition reliability by effectively measuring similarity in high-dimensional feature space.

The incorporation of temporal smoothing and face tracking techniques plays a significant role in improving system stability during real-time operation. By aggregating recognition results across multiple frames and maintaining identity tracking during brief detection failures, the system reduces false rejections and improves overall user experience. This is particularly important in voting environments, where incorrect authentication decisions can lead to voter dissatisfaction or security breaches.

Another notable aspect of the proposed system is its offline architecture. By eliminating dependency on network connectivity, the system achieves faster response times and improved reliability, making it suitable for deployment in areas with limited or unstable internet access. Local data storage ensures that voter information and voting records remain under administrative control, reducing exposure to external cyber threats. Additionally, offline operation minimizes latency during authentication and vote recording, contributing to efficient voter flow at polling stations.

Overall, the results demonstrate that the proposed smart voting system effectively balances security, accuracy, and usability. The combination of deep learning–based face recognition, efficient similarity matching, and offline processing provides a practical solution for secure electronic voting. The system shows strong potential for deployment in controlled election environments and serves as a foundation for future enhancements such as multimodal biometric integration and scalability imp

V. CONCLUSION

This paper presents an offline Smart Voting System through Face Recognition that enhances election security by preventing impersonation and duplicate voting. By leveraging deep learning–based facial embeddings and cosine similarity matching, the system provides accurate and reliable voter authentication. The offline architecture, combined with efficient local data storage, ensures fast performance and robustness. The proposed system offers a practical and scalable solution for secure electronic voting and has strong potential for real-world deployment in future election process

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]. W. Zhao, R. Chellappa, A. Rosenfeld, and P. J. Phillips, “Face Recognition: A Literature Survey,” ACM Computing Surveys, vol. 35, no. 4, pp. 399–458, 2003.

[3]. P. Viola and M. Jones, “Rapid Object Detection Using a Boosted Cascade of Simple Features,” Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2001.

[4]. L. Wiskott, J. M. Fellous, N. Krüger, and C. von der Malsburg, “Face Recognition by Elastic Bunch Graph Matching,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 7, pp. 775–779, 1997.

[5]. T. Ahonen, A. Hadid, and M. Pietikäinen, “Face Description with Local Binary Patterns: Application to Face Recognition,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, no. 12, pp. 2037–2041, 2006.

[6]. S. Z. Li and A. K. Jain, Handbook of Face Recognition, Springer, 2011.

[7]. M. Turk and A. Pentland, “Eigenfaces for Recognition,” Journal of Cognitive Neuroscience, vol. 3, no. 1, pp. 71–86, 1991.

[8]. J. Wright, A. Yang, A. Ganesh, S. Sastry, and Y. Ma, “Robust Face Recognition via Sparse Representation,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 31, no. 2, pp. 210–227, 2009.

[9]. Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, “DeepFace: Closing the Gap to Human-Level Performance in Face Verification,” IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2014.

[10]. F. Schroff, D. Kalenichenko, and J. Philbin, “FaceNet: A Unified Embedding for Face Recognition and Clustering,” IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2015.

[11]. O. M. Parkhi, A. Vedaldi, and A. Zisserman, “Deep Face Recognition,” British Machine Vision Conference (BMVC), 2015.

[12]. S. Marcel and S. Bengio, “Improving Face Verification Using Skin Color Information,” Pattern Recognition, vol. 35, no. 3, pp. 639–650, 2002.

[13]. R. Brunelli and T. Poggio, “Face Recognition: Features Versus Templates,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15, no. 10, pp. 1042–1052, 1993.

DOI: 10.17148/IJARCCE.2025.1412154

[14]. A. Ross and A. K. Jain, "Information Fusion in Biometrics," Pattern Recognition Letters, vol. 24, no. 13, pp. 2115–2125, 2003.
[15]. J. Daugman, "How Iris Recognition Works," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 21–30, 2004.
[16]. R. Patil, S. Deshmukh, and A. Shinde, "Secure Electronic Voting System Using Face Recognition," International Journal of Computer Applications, vol. 176, no. 6, pp. 22–26, 2020.
[17]. S. Kumar and A. Kumar, "Biometric Voting System Using Face Recognition," International Journal of Engineering Research & Technology (IJERT), vol. 8, no. 6, 2019.
[18]. M. B. Patil and R. R. Manza, "Biometric Authentication System Using Face Recognition for Secure Voting," International Journal of Advanced Research in Computer Science, vol. 10, no. 3, 2019.
[19]. A. Alghamdi and M. A. Alotaibi, "Electronic Voting System Using Face Recognition," International Journal of Computer Science and Network Security, vol. 18, no. 5, 2018.
[20]. K. Delac and M. Grgic, "A Survey of Biometric Recognition Methods," Electronics in Marine, 2004.
[21]. Y. Sun, X. Wang, and X. Tang, "Deep Learning Face Representation by Joint Identification-Verification," Advances in Neural Information Processing Systems (NeurIPS), 2014.
[22]. C. Ding and D. Tao, "A Comprehensive Survey on Pose-Invariant Face Recognition," ACM Transactions on Intelligent Systems and Technology, vol. 7, no. 3, pp. 1–42, 2016.
[23]. G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, "Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments," University of Massachusetts, Amherst, Technical Report, 2007.
[24]. H. Wang, Y. Wang, Z. Zhou, X. Ji, D. Gong, J. Zhou, Z. Li, and W. Liu, "CosFace: Large Margin Cosine Loss for Deep Face Recognition," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018.
[25]. J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2019.