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 2, February 2026

DOI: 10.17148/IJARCCE.2026.15221

VOTEX

Prof. Veena Amit Mali[1], Aradhana Santosh Upadhyay[2], Arpita Ajit Taware[3], Gouri Chandrakant Sawant[4], Divya Rangnath Thombare[5], Neha Mahadev Patil[6]

Assistant Professor, Computer Science Engineering (Artificial Intelligence), DKTE Ichalkaranji[1]

Final Year B.Tech, Computer Science Engineering (Artificial Intelligence), DKTE Ichalkaranji[2-6]

Abstract: Elections are an essential part of democratic systems, but traditional voting methods still face challenges such as identity fraud, duplicate voting, and difficulties in voter verification. Manual authentication processes are time-consuming and may lead to errors, reducing transparency and efficiency during elections. With the advancement of biometric technologies and artificial intelligence, secure electronic voting systems can be developed to improve voter authentication and prevent unauthorized voting. This paper proposes VOTEX – One Person One Vote, a biometric-based voting system that combines fingerprint verification and face recognition to ensure secure and accurate identification. The system captures voter details and biometric data during registration, verifies identity through multi-level authentication, and prevents multiple voting by maintaining real-time vote status in the database. It also provides flexible authentication options for disabled voters to ensure accessibility and inclusiveness. By integrating technologies such as Flask, OpenCV, MTCNN, CNN-based face recognition, and MySQL, the proposed system aims to provide a reliable, secure, and user-friendly voting solution that enhances electoral transparency and trust.

Keywords: Biometric authentication, electronic voting system, face recognition, fingerprint verification, MTCNN, CNN, Flask framework, secure voting, voter authentication, one person one vote

I. INTRODUCTION

1.1 Background

Elections are an important foundation of democratic societies and ensuring fair and secure voting is essential for maintaining public trust. Traditional voting systems mainly depend on manual identity verification using voter cards and human supervision, which may lead to errors, impersonation, and duplicate voting. In recent years, biometric technologies such as fingerprint and face recognition have gained attention because they provide reliable identity verification based on unique human characteristics. At the same time, advances in artificial intelligence and web-based systems have made it possible to design smart electronic voting solutions that improve both security and efficiency. By integrating biometric authentication with modern software technologies, voting systems can become more transparent, accurate, and accessible to a wide range of users, including disabled voters.

1.2 Problem Statement

Existing voting systems face several challenges, including unauthorized voting, repeated vote casting, and long verification procedures that slow down the voting process. Systems that rely only on manual checks or a single biometric method may fail due to hardware limitations, environmental conditions, or human errors. Additionally, many voting systems do not provide proper accessibility options for disabled voters, which limits inclusiveness. There is a need for a secure and intelligent electronic voting system that can authenticate voters accurately using multiple biometric methods, prevent duplicate voting, and maintain clear activity logs while ensuring a smooth and user-friendly voting experience.

1.3 Research Objectives

This study aims to:

- Develop a secure biometric-based electronic voting system following the “one person, one vote” principle
- Implement dual authentication using fingerprint verification and face recognition for improved security
- Provide flexible authentication options for disabled voters to ensure accessibility
- Maintain secure voter data, authentication logs, and vote status using a database system
- Create a user-friendly web-based voting interface using Flask and modern web technologies

1.4 Significance

This research contributes to secure digital voting by introducing a system that combines biometric authentication, real-time verification, and accessibility-focused design. The proposed VOTEX system reduces the risk of

DOI: 10.17148/IJARCCE.2026.15221

impersonation and duplicate voting while improving transparency and reliability during elections. By integrating fingerprint verification, face recognition, and secure database management, the system offers a practical solution that can enhance voter trust and simplify the overall voting process. The project also highlights how AI-based biometric systems can be applied to real-world electoral applications, supporting the development of safer and more inclusive voting technologies.

II. LITERATURE REVIEW

2.1 Biometric-Based Electronic Voting Systems

Biometric authentication has been widely used in electronic voting systems to improve voter identification and reduce impersonation. Technologies such as fingerprint recognition, facial recognition, and iris scanning provide unique identity verification and help enforce secure voting practices. Many biometric voting systems successfully reduce unauthorized access; however, relying on a single biometric modality may cause authentication failures due to hardware limitations or environmental factors.

2.2 Fingerprint Authentication for Voting

Fingerprint-based voting systems are commonly adopted because fingerprints are unique and easy to capture. Several studies have shown that fingerprint authentication effectively prevents duplicate voting and improves voter verification accuracy. Despite its benefits, fingerprint-only systems can experience reduced performance when fingerprints are unclear, damaged, or when sensor quality is poor, highlighting the need for additional authentication mechanisms.

2.3 Face Recognition Using Deep Learning

Face recognition has gained significant attention due to its contactless authentication capability and user convenience. Deep learning approaches, especially Convolutional Neural Networks (CNNs), have demonstrated strong performance in extracting facial features and improving recognition accuracy. Techniques such as MTCNN-based face detection combined with CNN models provide reliable face authentication, although lighting conditions and image quality remain important factors affecting system performance.

2.4 Research Gap

Existing research mainly focuses on fingerprint-based or face recognition-based voting systems independently, with limited work integrating both authentication methods into a unified system. Additionally, many solutions do not adequately address accessibility requirements for disabled voters or maintain proper authentication logs for audit purposes. This research addresses these gaps by proposing VOTEX – One Person One Vote, which combines fingerprint verification and CNN-based face recognition within a web-based voting system while ensuring secure database management, activity logging, and inclusive authentication pathways

III. METHODOLOGY

3.1 System Architecture

The proposed VOTEX system consists of five core modules designed to ensure secure voter authentication and reliable vote casting:

1. **Registration Module:** Collects voter personal details such as name, date of birth, gender, email, mobile number, address, and Aadhaar number along with biometric data including fingerprint and face images. OTP-based verification is used before storing data in the database.
2. **Biometric Authentication Module:** Performs voter verification using fingerprint matching and face recognition. Face detection is carried out using MTCNN, and facial embeddings are compared with stored database embeddings for identity verification. missing values, feature scaling, image resizing, normalization, and dataset splitting to ensure model robustness.
3. **Accessibility Module:** Provides adaptive authentication pathways for disabled voters by allowing either fingerprint or face recognition based on user capability, ensuring inclusiveness. Multiple machine learning algorithms for crop and fertilizer recommendations and a Convolutional Neural Network (CNN) for plant disease identification.
4. **Vote Casting Module:** Displays available parties and candidates after successful authentication and allows the voter to cast a vote. The system updates vote status to prevent duplicate voting.
5. **Logging and Monitoring Module:** Stores authentication results, timestamps, and access decisions such as success, failure, or access denial for auditing and transparency purposes.

DOI: 10.17148/IJARCCE.2026.15221

3.2 Mathematical Framework

3.2.1 Face Recognition Model

Face authentication is formulated as a similarity comparison problem. Given a face image input I, the system first detects faces using MTCNN and generates an embedding vector using a deep learning-based FaceNet model.

$$E = f(I)$$

where Erepresents the generated face embedding.
The similarity between input and stored embeddings is calculated using Euclidean distance:

$$D = \| E_{input} - E_{database} \|$$

If the distance is below a defined threshold, authentication is successful.

3.2.2 Fingerprint Verification Model

The Fingerprint authentication is performed using the Source AFIS library. The captured fingerprint template is matched against stored templates in the database, and access is granted only when a valid match is found. This ensures accurate voter identity verification before proceeding to vote.

3.3 Model Training and Optimization

3.3.1 Face Recognition Model

The face recognition module uses deep learning-based feature extraction:

- MTCNN for face detection
- FaceNet for embedding generation
- CNN-based architecture using Keras and TensorFlow

The model extracts meaningful facial features to achieve reliable authentication under real-world conditions.

3.3.2 Authentication Parameters

- Face detection confidence threshold: 0.95
- Face embedding similarity threshold: 0.9
- Maximum authentication attempts: 3
- Real-time webcam image capture using OpenCV

3.4 Experimental Design

3.4.1 Data Preprocessing

- Face image capture using webcam
- RGB color conversion and normalization
- Face region extraction using bounding boxes
- Feature embedding generation for storage
- Secure database indexing using voter ID

3.4.2 Authentication Logic

- Fingerprint verification performed first for normal users
- Face authentication performed as secondary verification
- Disabled users allowed flexible authentication options
- Voting denied if voter already marked as voted
- Maximum three retry attempts allowed in case of failure.

3.4.3 Evaluation Metrics

Model performance was evaluated using:

- Authentication Accuracy: Correct voter identification rate
- Precision: Correct successful authentications
- Recall: Ability to identify genuine voters
- False Acceptance / Rejection Rate
- Authentication Attempt Logs: Success and failure analysis

DOI: 10.17148/IJARCCE.2026.15221

3.5 Implementation Details

The VOTEX system was implemented using Python and the following tools:

- **Flask:** Backend framework and web routing
- **HTML, CSS, Bootstrap:** Frontend user interface
- **OpenCV:** Real-time video capture and image preprocessing
- **MTCNN:** Face detection
- **TensorFlow/Keras:** CNN-based face recognition
- **Source AFIS:** Fingerprint verification
- **NumPy:** Numerical operations and embedding comparison
- **PostgreSQL:** Database for voter data, biometrics, and vote logs

IV. EXPERIMENTAL SETUP

4.1 Dataset Requirements:

The proposed VOTEX system utilizes biometric and voter information datasets collected during the registration phase:

Voter Registration Dataset:

- Contains personal details such as name, date of birth, gender, email, mobile number, address, and Aadhaar number
- Each voter is assigned a unique voter ID for database indexing
- Data stored in MySQL database

Face Recognition Dataset:

- Captured face images during registration
- Converted into face embeddings using FaceNet
- Stored as numerical feature vectors for authentication
- Captured using webcam with real-time image processing

Fingerprint Dataset:

- Fingerprint templates captured using fingerprint scanner
- Templates stored securely and matched using Source AFIS library

4.2 Validation Strategy

- To ensure reliable and reproducible results, the following validation strategies were adopted:
- Real-time biometric matching against stored database records
- Threshold-based similarity comparison for face authentication
- Fingerprint template matching for identity confirmation
- Multiple authentication attempts (maximum three retries) to handle hardware or detection failures
- Independent verification for fingerprint and face authentication before vote casting

4.3 Comparative Analysis Protocol

The authentication process follows a structured protocol to ensure secure voting:

- Capture biometric input (fingerprint or face image)
- Preprocess data using OpenCV and detection models
- Match biometric features with stored database records
- Verify voter voting status to prevent duplicate voting
- Allow access only after successful authentication
- Store authentication results and timestamps for auditing

V. RESULTS AND DISCUSSION

5.1 Results Overview

The experimental implementation of the VOTEX system produced the following key outcomes:

- Successful voter registration with secure storage of personal and biometric data
- Accurate face detection and authentication using MTCNN and CNN-based feature extraction
- Reliable fingerprint verification using Source AFIS library

DOI: 10.17148/IJARCCE.2026.15221

- Prevention of duplicate voting through vote status tracking in the database
- Authentication logging with timestamps for audit and monitoring purposes
- The integrated biometric approach ensured that only verified users were allowed to access the voting panel.

5.2 Analytical Framework

5.2.1 Face Recognition Performance Analysis

The face authentication module successfully detected and verified faces in real-time using webcam input. MTCNN provided robust face detection, while deep learning-based embeddings improved matching accuracy. The threshold-based similarity comparison enabled effective identification of registered voters while rejecting mismatched faces. Multiple test cases showed stable performance under normal lighting conditions and standard camera quality.

5.2.1 Fingerprint Verification Analysis

The Fingerprint authentication demonstrated reliable voter identification by matching scanned fingerprints with stored templates. The use of Source AFIS provided accurate matching results and reduced unauthorized access attempts. However, recognition accuracy depends on fingerprint quality and sensor precision, which highlights the importance of proper hardware handling.

5.2.2 Combined Authentication Analysis

The dual-biometric authentication approach significantly improved system security compared to single-factor methods. By combining fingerprint verification with face recognition, the system minimized false acceptance cases and ensured stronger identity validation. The inclusion of a three-attempt retries mechanism improved usability by allowing genuine users additional chances during recognition failures

5.2.3 Discussion

The experimental results demonstrate that integrating biometric authentication into an electronic voting system enhances both security and transparency. The VOTEX system successfully enforced the "one person, one vote" principle by checking voter status before allowing vote casting and maintaining real-time authentication logs. The adaptive authentication pathway for disabled voters further improved system inclusiveness. Overall, the system shows that combining fingerprint verification, deep learning-based face recognition, and secure database management provides a practical and scalable solution for modern electronic voting applications.

VI. PRACTICAL APPLICATIONS

6.1 Use Cases

The proposed VOTEX system can be applied in several real-world voting scenarios, including:

- **Secure Election Voting:** Ensures that only authorized voters can cast votes through biometric authentication, reducing impersonation and fraudulent voting.
- **Duplicate Vote Prevention:** Maintains real-time vote status tracking to ensure that each voter can cast only one vote during an election cycle.
- **Accessible Voting for Disabled Users:** Provides flexible authentication options such as fingerprint or face recognition, improving inclusiveness and ease of use.
- **Automated Identity Verification:** Reduces dependency on manual verification and minimizes human errors during elections.
- **Audit and Monitoring:** Authentication logs with timestamps allow election authorities to monitor system activity and maintain transparency.

6.2 Deployment Considerations

The VOTEX system is designed for deployment in real-world voting environments through a web-based architecture Key deployment considerations include:

- Integration with biometric hardware such as fingerprint scanners and webcams
- Secure database storage for voter data and authentication logs
- Reliable network and system infrastructure for smooth voting operations
- Scalability to handle large numbers of voters during election periods
- Easy system maintenance and updates using Flask-based web deployment

DOI: 10.17148/IJARCCE.2026.15221

VII. LIMITATIONS AND FUTURE WORK

7.1 Current Limitations

Although the proposed VOTEX system shows promising results, certain limitations still exist:

- The accuracy of face recognition depends on lighting conditions and camera quality.
- Fingerprint authentication performance may vary based on sensor quality or unclear fingerprints.
- The system currently requires biometric hardware availability at voting locations.
- Recognition performance may reduce when handling very large voter databases without optimization.
- Secure storage and management of biometric data remain critical challenges that require strong security measures.

7.2 Future Enhancements

Future improvements to the VOTEX system can include:

- Liveness Detection: Adding anti-spoofing techniques to prevent fake face or fingerprint attacks.
- Improved Face Recognition Models: Using advanced deep learning architectures for higher accuracy under different lighting and angles.
- Cloud-Based Deployment: Enabling scalable voting infrastructure for large-scale elections.
- Blockchain Integration: Providing transparent and tamper-proof vote tracking mechanisms.
- Mobile-Based Authentication: Allowing secure remote identity verification where applicable.
- Performance Optimization: Enhancing processing speed for large voter datasets and real-time authentication.

VIII. CONCLUSION

This research presents VOTEX – One Person One Vote, a secure biometric-based electronic voting system designed to improve electoral transparency and prevent unauthorized voting. The proposed system integrates fingerprint verification and deep learning-based face recognition to ensure accurate voter authentication before allowing vote casting. By combining multiple authentication methods, the system reduces the chances of impersonation and duplicate voting while maintaining reliability during real-time voting operations. The inclusion of adaptive authentication pathways also ensures accessibility for disabled voters, making the system more inclusive and user-friendly. The implementation of authentication logging, vote status tracking, and secure database management further strengthens the overall integrity of the voting process. Experimental results demonstrate that the integration of biometric technologies with a web-based framework provides an efficient and practical solution for modern electronic voting systems. Although certain limitations related to hardware dependency and environmental factors exist, the proposed system establishes a strong foundation for future improvements. Overall, VOTEX contributes toward building a secure, transparent, and scalable voting framework that can enhance public trust and support the evolution of digital election technologies.

The proposed framework offers a practical and scalable solution for precision agriculture by supporting informed decision-making, early disease detection, and optimized resource utilization. Its modular architecture and web-based implementation enhance accessibility and usability for farmers and agricultural stakeholders. Overall, the system contributes to sustainable farming practices, improved crop productivity, and enhanced food security, while providing a strong foundation for future advancements in intelligent agricultural systems.

REFERENCES

[1]. R. Haenni, E. Dubuis, and U. Ultes-Nitsche, “Research on e-voting technologies." Bern University of Applied Sciences, Technical Report 5, 2008.

[2]. Sanjay Kumar, Manpreet Singh, “DESIGN OF A SECURE ELECTRONIC VOTING SYSTEM USING FINGERPRINT TECHNIQUE”, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013

[3]. V. Kiruthika Priya, V. Vimaladevi, B. Pandimeenal, T. Dhivya, “Arduino based smart electronic voting machine”, 2017 International Conference on Trends in Electronics and Informatics (ICEI) Year: 2017, conference Paper, Publisher: IEEE

[4]. R. K. Pandey, R. R. Vohra, and S. Ghosh, “A Study on the Use of Biometric Systems in E-Voting for Voter Authentication,” International Journal of Computer Science and Technology, vol. 9, no. 2, pp. 150 - 156, 2021

[5]. J. Srikanth, M. S. Chetana, J. Tarachand, V. Hanumanth and P. Sagar, “Smart Voting System Utilizing Iris Recognition Technology,” 2024 5th International Conference on Image Processing and Capsule Networks (ICIPCN), Dhulikhel, Nepal, 2024, pp. 73 - 77, doi: 10.1109/ICIPCN63822.2024.00021.