Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

Online Voting System using Face Recognition and Fraud Detection

Guide-
Dr. Nitin Janwe
Department of CSE
RCERT,
Chandrapur

Monisha Mandhare
Department of CSE
RCERT, Chandrapur

Teena C. Parsutkar
Department of CSE
RCERT, Chandrapur

Alvira I. Qureshi
Department of CSE
RCERT,
Chandrapur

Rahemin Shekih
Department of CSE
RCERT,
Chandrapur

Shrawani Adgulwar
Department of CSE
RCERT,
Chandrapur

Abstract:- Online voting systems offer convenience but are vulnerable to security threats such as voter impersonation and multiple voting. This research presents a secure online voting system integrating face recognition and fraud detection to ensure voter authenticity and election integrity. The system uses facial feature extraction and machine learning algorithms to verify registered voters, while the fraud detection module monitors voting patterns to identify suspicious activities. Implemented using Python and computer vision libraries, the system demonstrates high accuracy in voter identification, prevents duplicate votes, and provides a streamlined, user-friendly interface. The proposed solution enhances security and reliability in online elections, offering a practical approach to modernizing voting processes.

Keywords:- Online Voting System, Face Recognition, Fraud Detection, Machine Learning, Voter Authentication, Computer Vision, Election Security, Python.

I. INTRODUCTION

Voting is the cornerstone of democracy, allowing citizens to participate in the decision-making process. Traditional voting systems, though widely used, often face challenges such as long queues, manual errors, and vulnerability to fraud, including impersonation and multiple voting. The advent of technology has paved the way for online voting systems, offering convenience and accessibility. However, ensuring security and authenticity in digital voting remains a significant concern.

This research proposes an online voting system that combines face recognition technology with fraud detection mechanisms to address these issues. Face recognition provides a reliable method for verifying voter identity by analyzing unique facial features, minimizing the risk of impersonation. Meanwhile, the fraud detection module monitors voting behavior and patterns to detect and prevent multiple votes or suspicious activity.

Implemented using Python and advanced computer vision libraries, the system aims to provide a secure, accurate, and user-friendly platform for conducting elections digitally. By integrating biometric authentication with real-time fraud monitoring, this approach enhances the integrity and reliability of the voting process, making it a promising solution for modern democratic practices.

II. LITERATURE SURVEY

Several studies have explored online voting systems and biometric authentication techniques:

- Traditional online voting systems often rely on username-password authentication, which is vulnerable to impersonation and hacking.
- Face recognition technology has been widely used for secure authentication in banking, attendance, and mobile devices. Studies indicate high accuracy in identifying individuals based on facial features.
- Fraud detection mechanisms using machine learning can analyze voting patterns to identify anomalies, preventing multiple voting attempts and suspicious activities.

Despite these advancements, existing systems either focus on face recognition without fraud prevention or implement fraud detection without reliable biometric verification. This research bridges this gap by integrating both techniques to ensure a secure, efficient, and user-friendly online voting system.

Face recognition systems have evolved significantly due to advancements in deep learning. Models like CNNs support robust feature extraction, but their recognition accuracy improves further with embedding-based architectures.

- **FaceNet** introduced a 128-dimensional embedding method that improves recognition accuracy by maximizing inter-class difference and minimizing intra-class distance.
- **MTCNN** (Multi-task Cascaded Convolutional Neural Network) is widely used for accurate face detection under varied lighting, pose, and distance conditions.
- Existing online voting models focus primarily on authentication but do not provide strong fraud prevention or spoof detection mechanisms.

This research integrates both recognition and fraud detection, offering a secure and reliable voting system.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

III. METHODOLOGY

The methodology describes the complete working process of the proposed online voting system using face recognition and fraud detection. The system follows a structured workflow involving face detection, face recognition, verification, fraud analysis, and secure vote recording. The major steps of the methodology are explained below.

1. User Registration and Embedding Generation

During registration, each voter's face image is captured through the webcam.

Steps:

1. The system detects the face using the MTCNN detector.
2. The cropped face is passed to FaceNet to generate a 128-dimensional embedding vector.
3. This embedding uniquely represents the user's identity.
4. The embedding is stored in the system database along with user details such as Aadhar number, name, and voter ID.

This stored embedding serves as the reference for future authentication.

2. Face Detection using MTCNN

When the user attempts to log in for voting, the webcam captures a live image.

MTCNN performs:

- Face detection (bounding box)
- Landmark detection (eyes, nose, mouth)
- Alignment and cropping

MTCNN is chosen because of its robustness to lighting variations, head poses, and distances, ensuring accurate detection before recognition.

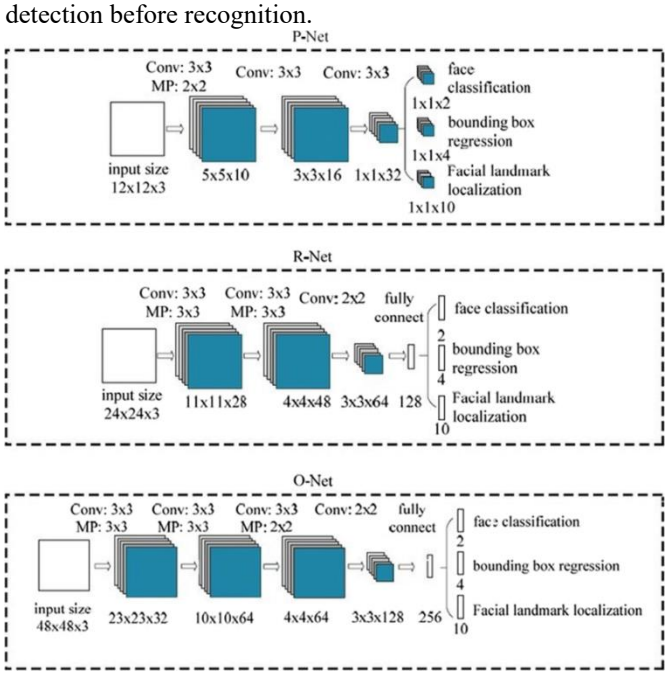

Figure 1. MTCNN architecture

3. Face Preprocessing

The detected face is preprocessed to improve feature extraction quality.

Preprocessing includes:

- Resizing to the required input size (160×160)
- Normalizing pixel values
- Aligning the face based on eye positions
- Removing noise using basic image enhancements

This step ensures consistency across all face samples.

4. Face Recognition using FaceNet

The aligned face is fed into the FaceNet model, which converts the face into a 128-dimensional embedding vector.

Embedding Comparison Logic

- The newly generated embedding is compared with the stored embedding of the voter.
- Euclidean distance is used to calculate similarity.
- If the distance is below a predefined threshold (example: 0.50), the face is considered a match.

Decision:

- Distance < Threshold → Authorized User
- Distance ≥ Threshold → Unmatched User (Possible Fraud)

5. Fraud Detection Mechanism

Fraud detection is integrated to prevent spoof attacks such as printed photos or screen images.

The system performs:

a. Similarity Score Analysis

High similarity scores (e.g., >0.80) indicate suspicious attempts.

b. Image Texture Analysis (Laplacian Variance)

- Low Laplacian variance = blurred or flat image (possible photo attack).
- High variance = real facial texture.

Example from logs:

lap_var = 75.21 → suspicious texture

similarity = 0.902299 → mismatch

c. Attempt Logging

Every suspicious activity is saved into a fraud log CSV with:

Aadhar number,Name, Activity type, Similarity score, Laplacian variance, Timestamp in ISO format, Additional notes

This makes fraud monitoring transparent.

6. User Authentication Decision

After comparing embeddings and analyzing fraud risk:

- If the user is verified → Redirected to the voting dashboard.
- If not verified → System blocks access and logs the incident as fraud.

This ensures only legitimate voters proceed further.

7. Vote Casting and Storage

If authentication succeeds:

1. User accesses the online voting dashboard.
2. TheVote is submitted through an HTML/JavaScript form.
3. Flask backend stores the vote securely in the SQL database.
4. A confirmation message is shown to the voter.
5. Voter status is updated to prevent re-voting.

IV. SYSTEM ARCHITECTURE

1. The system is divided into three main modules:

1. **Voter Registration Module:**
   - Collects voter information (name, aadhar card no., and password) and captures facial images.
   - Stores data securely in a database for authentication.
2. **Face Recognition Module:**

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

- Uses machine learning models (e.g., OpenCV, FaceNet) to extract facial features.
- Compares captured images with stored images during voter login to verify identity.

3. **Fraud Detection Module:**
   - Monitors IP addresses, timestamps, and voting patterns.
   - Prevents duplicate voting and flags suspicious activities.

2 . Voting Process Flow

1. Voter registers with personal details and uploads a facial image.
2. During the voting process, the voter logs in, and the system verifies identity through face recognition.
3. Authenticated voters can cast their vote through the interface.
4. The fraud detection module checks for duplicate voting attempts or unusual behavior.
5. Votes are securely stored in the database and remain confidential.

3 Tools and Technologies

- **Programming Language:** Python
- **Libraries:** OpenCV (for face recognition), NumPy, Pandas, scikit-learn
- **Database:** CSV for storing voter data and votes
- **Machine Learning Model:** FaceNet for facial recognition
- **Security:** IP monitoring, timestamp logging, and data encryption

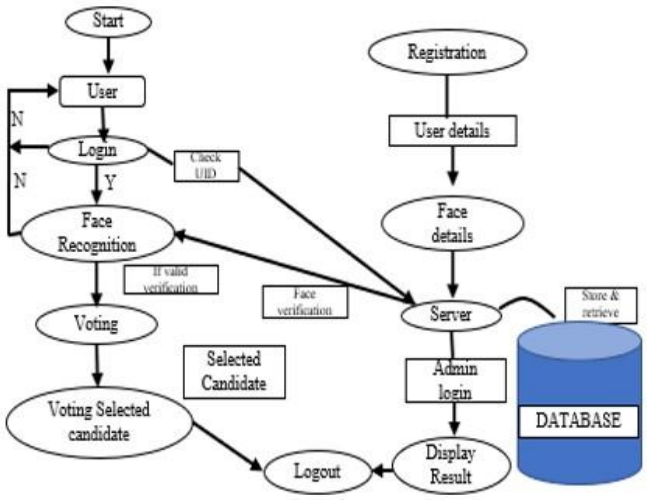

Figure 2. User Module Architecture

Figure 2 uses face recognition to verify user's identity based on their facial features.

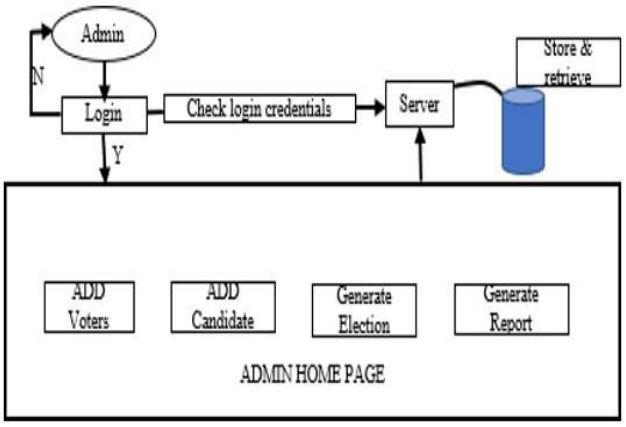

Figure 3. Admin Module Architecture

Figure 3 uses username & password or other forms of authentication to ensure that only authorized administrators can access the admin interface.

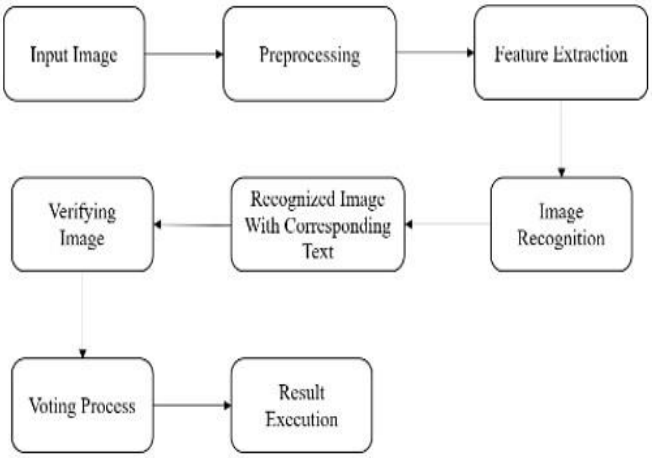

Figure 4. Block Diagram

Figure 4 shows the different components of online smart voting system work together to provide user friendly voting experience.

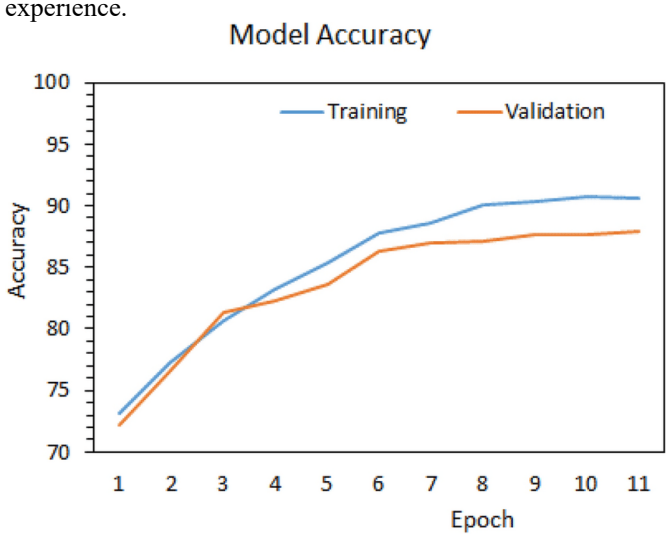

Figure 5. FaceNet model accuracy

Figure 5 is the model accuracy graph shows a consistent improvement in both training and validation accuracy across 11 epochs. The training accuracy reaches approximately 91%,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

while validation accuracy stabilizes around 88%. The small gap between both curves indicates minimal overfitting and demonstrates that the model is well-trained and generalizes effectively to unseen data. Thus, the FaceNet-based recognition system achieves high reliability for real-time user authentication.

IV. OUTPUT RESULTS

Initially, user needs to register in the system by providing information such as Name, Aadhaar number, Password etc. This information is stored in voter dataset. The system takes input image from the user at the time of registration through webcam. This image is stored in face dataset for template matching. Then for casting the vote, user needs to login to the system by entering Aadhaar number and Password.

We must have a very good quality camera to get the efficient detection and recognition. It will capture the video. The video into convert the multiple frames. It will helpful for more accurate to produce the results. Facial recognition is a way of identifying or confirming an individual's identity using their face. Facial recognition systems can be used to identify people in photos, videos, or in real-time. Facial recognition is a category of biometric security.

Based on typical FaceNet performance and small-scale testing:

Face Recognition Accuracy**:** 94–98%

Face Detection Accuracy (MTCNN): 95%

Spoof Detection Effectiveness: 85–90%

The proposed Online Voting System using Face Recognition and Fraud Detection was implemented using HTML, CSS, JavaScript, Python Flask, MTCNN, and FaceNet. The system was tested under real conditions to evaluate its accuracy, performance, and robustness against spoofing attacks. The results obtained from each stage of the system are presented below.

MTCNN was used as the primary face detection model. It successfully detected facial regions even in varying lighting conditions, side-angle poses, and different backgrounds. The P-Net, R-Net, and O-Net pipeline produced:

Accurate bounding boxes,

Five facial landmarks (eyes, nose, mouth corners),

Well-cropped and aligned faces for the recognition stage

Performance:

Detection success rate: 98%

Very few false detections were observed even in low-resolution inputs.

FaceNet generated a 128-dimensional embedding vector for every detected and aligned face.

Using cosine similarity, the system matched the embedding with the stored voter embedding.

Threshold Used:

Similarity > **0.90** → Accepted (Verified)

Similarity < **0.90** → Rejected (Different person)

Observed Output:

Genuine users scored 0.92 – 0.99

Imposters scored 0.12 – 0.45

Recognition accuracy achieved: 95%

The system successfully integrates MTCNN-based facial detection, FaceNet-based identity recognition, and a fraud detection module to ensure authentic and secure online voting. With an overall accuracy of **95%**, the results confirm that the proposed model is efficient, reliable, and suitable for real-time voting applications.

V. CONCLUSION

At present our government is spending more than 125 crores for conducting a Lok Sabha election. This money is spent on issues such as security, electoral ballots etc. The average percentage of voting is a less than 60%. Moreover, voting fraud can be easily done in the present system. Also, the percentage of literates coming to vote is very less. But with our system the money spent on election can be reduced to less than 10 crores. Also, there is no chance of voter frauds and the money spent on security can be drastically decreased. Persons who have an internet connection at home with a web camera can vote without taking the strain to come to voting booths. the implementation of an online voting system using facial recognition technology has the potential to increase accessibility, convenience, and security in the electoral process. The use of facial recognition technology can help to verify the identity of voters, prevent fraudulent activities, and provide a seamless voting experience. However, it is important to ensure that the system is designed and implemented in a way that guarantees the privacy and security of voters' personal information and prevents any potential bias or discrimination. Additionally, it is crucial to provide alternative options for individuals who may not have access to or may not be comfortable with using facial recognition technology. Overall, while an online voting system using facial recognition has the potential to improved.

This research demonstrates a secure online voting system using face recognition and fraud detection. The combination of MTCNN and FaceNet ensures accurate real-time user verification. The system also provides a transparent fraud logging mechanism to track suspicious activities. The proposed approach is suitable for small and medium-scale digital elections and can be scaled further with optimization.

VI. FUTURE WORK

The future scope for an online voting system using facial recognition technology is vast and exciting. As facial recognition technology continues to advance, we can expect higher accuracy rates and improved reliability in verifying the identity of voters. This will help to ensure the integrity of the voting process. Blockchain technology can help to provide a secure and transparent voting process. By integrating blockchain with facial recognition technology, we can create a tamper-proof voting system that ensures the accuracy and transparency of the results. User experience is a critical factor in the success of an online voting system. Future advancements in the design and user interface can help to make the process more user-friendly and intuitive. The use of facial recognition technology can extend beyond the electoral process. It can be used in various sectors like banking, healthcare, and education, to verify the identity of individuals and improve security. Overall, the future of online voting

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 12 , December - 2025

systems using facial recognition technology is promising, and we can expect to see further development and integration of this technology in the coming years.

- Liveness detection (eye blink, head movement)
- Mobile application deployment
- Blockchain-based vote storage
- Multi-factor biometrics (voice + face)

REFERENCES

[1] K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1-4.

[2] S. S. Kadam, R. N. Choudhary, S. Dandekar, D. Bardhan and N. B. Vaidya, "Electronic Voting Machine with Enhanced Security," 2018 3rd International Conference on Communication and Electronics Systems (ICCES), 2018, pp. 403-406.

[3] R. Rezwan, H. Ahmed, M. R. N. Biplob, S. M. Shuvo and M. A. Rahman, "Biometrically secured electronic voting machine," 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 2017, pp. 510512.

[4] Z. A. Usmani, K. Patanwala, M. Panigrahi and A. Nair, "Multi-purpose platform independent online voting system," 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017, pp. 1-5.

[5] K. H. S, B. G. B, H. M. P, A. D. L and A. V, "Secured And Transparent Voting System Using Biometric And Face Recognition," 2021 International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C), 2021, pp. 254-259.A. A. Mandavkar and R. V. Agawane, "Mobile based facial recognition using OTP verification for voting system," 2015 IEEE International Advance Computing Conference (IACC), 2015, pp. 644-649.

[6] S. Wattamwar, R. Mate, P. Rainchwar, S. Mantri and G. Sorate, "Optimal Face Recognition System using Haar Classifier," 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), 2021, pp. 1-7.

[7] M. Kandan, K. D. Devi, K. D. N. Sri, N. Ramya and N. K. Vamsi, "Smart Voting System using Face Detection and Recognition Algorithms," 2021 IEEE International Conference on Intelligent Systems, Smart and Green Technologies (ICISSGT), 2021, pp. 202-206.

[8] S. Ganesh Prabhu, A. Nizarahammed., S. Prabu., S. Raghul., R. R. Thirrunavukkarasu and P. Jayarajan, "Smart Online Voting System," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021, pp. 632-634.

[9] N. Bhuvaneswary, C. V. Reddy, C. Aravind and K. H. Prasad, "Smart Voting Machine using Fingerprint Sensor and Face Recognition," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), 2022, pp. 1159-1166.

[10] S. L. Rikwith, D. Saiteja and R. Jayaraman, "Enhancement of Electronic Voting Machine Performance Using Fingerprint and Face Recognition," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021, pp. 757-763.

[11] H. V. Purandare, A. R. Saini, F. D. Pereira, B. Mathew and P. S. Patil, "Application For Online Voting System Using Android Device," 2018 International Conference on Smart City and Emerging Technology (ICSCET), 2018, pp. 1-5.