# Secure And Hassle Free EVM through Deep Learning Base Face Recognition

Shraddha N. Phad, Shital A. Mengal, Sanskruti S. Gangurde, Dhanashri K. Jadhav Ms. A.S. Sanap, Prof. M.P. Bhandakker
Department of Information Technology
*Student Matoshri Aasarabai Institute of technology and Research Centre Eklahare, Nashik, MH 422105*
*Lecturer, Matoshri Aasarabai Institute of technology and Research Center Eklahare, Nashik, MH 422105*
*HOD, Matoshri Aasarabai Institute of technology and Research Centre Eklahare, Nashik, MH 422105*

**Abstract—security, reduces manual intervention, election and increases public trust in the voting process. The solution is suitable for small-scale elections, institutional voting, and future smart governance applications. The Smart Electronic Voting Machine (EVM) using Facial Recognition improves is an intelligent and secure voting solution designed to enhance the integrity and transparency of the electoral process. The system integrates machine learning–based facial recognition techniques with electronic voting to ensure accurate voter authentication and prevent multiple voting by the same individual. A camera module captures the voter's facial image, which is processed using face recognition algorithms and compared with pre-registered voter data stored in the system.**

**The primary objective of the system is to eliminate voter impersonation, reduce election fraud, and enforce the principle of "one person, one vote." Once a voter's identity is successfully verified, the voting option is enabled. After the vote is cast, the system locks the voter's identity to prevent repeated voting attempts. All voting data is securely stored for counting and verification purposes.**

**By combining biometric authentication with electronic voting, the proposed system.**

**Index Terms—Smart EVM, Facial Recognition, Machine Learning, Biometric Authentication, Secure Voting System.**

## I. INTRODUCTION

Voting is a fundamental democratic process that allows citizens to select their representatives and participate in governance. Traditional voting methods and conventional Electronic Voting Machines (EVMs) face challenges such as voter impersonation, booth capturing, multiple voting, and manual verification errors. These issues raise concerns about election fairness and transparency.

Existing electronic voting machines improve counting efficiency but still rely on manual voter verification using identity cards or voter lists. Such methods are vulnerable to human error and fraudulent practices. Ensuring secure voter authentication remains a major challenge in modern electoral systems.

Facial recognition technology has gained significant attention due to its ability to uniquely identify individuals based on facial features. Integrating facial recognition with electronic voting machines can significantly enhance election security.

This project proposes a Smart EVM using facial recognition and machine learning to authenticate voters automatically and prevent repeated voting. The system ensures that only authorized voters can cast a vote and that each voter can vote only once.

### II-A. PROBLEM STATEMENT

The integrity, transparency, and security of the electoral process are critical for maintaining public trust in a democratic system. However, traditional voting systems and existing Electronic Voting Machines (EVMs) face several significant challenges that threaten the fairness and accuracy of elections.

One of the major issues is voter impersonation, where an unauthorized person casts a vote on behalf of another eligible voter. Since conventional systems mainly rely on voter ID cards and manual verification by polling officers, forged identity documents or

human errors can lead to fake voting. This compromises election authenticity.
Another major concern is duplicate or repeated voting. In some cases, weaknesses in voter verification mechanisms allow individuals to attempt voting more than once. Existing systems lack a strong automated biometric validation process to strictly enforce the "one person – one vote" rule.

II-B OBJECTIVES

Facial Recognition Authentication: -
The system verifies the voter's identity using facial recognition before allowing voting.
Eliminate Voter Impersonation: -
It prevents fake voting by matching the voter's face with stored records in the database.
Prevent Multiple Voting: -
After voting once, the system blocks the voter from voting again.
Reduce Manual Errors: -
Automated verification reduces mistakes that may happen during manual checking.
Secure Storage of Votes: -
All votes are stored safely in a secure database to avoid tampering or data loss.

II-C. SCOPE

College and University Elections: -
Can be used for student elections and campus voting systems.
Corporate Voting Systems: -
Useful for company-level voting such as board member selection or internal decisions.
Institutional Decision Making: -
Can be applied in schools, organizations, and committees for secure voting.
Small-Scale Local Elections: -
Suitable for societies or small community elections.

III. LITERATURE REVIEW

INSERT TABLE

| Sr. No. | Paper Name | Author Name | Year | Algorithm / Logic Used | Data base | |
|---|---|---|---|---|---|---|
| 1) | Facial Recognition Based Electronic Voting System | A.Sharma, R.Verma | 2023 | Eigenfaces, PCA | MySQL | |
| 2) | Secure Smart Voting System Using Machine Learning | P.Kumar ,S. Singh | 2023 | CNN,Face Encoding | Firebase | |
| 3) | Biometric Based Electronic Voting Machine | R.Mehta ,K. Joshi | 2021 | Face Detection + ID Mapping | SQLite | |
| 4) | Smart EVM Using Face Recognition and IoT | M.Desai ,N . Shah | 2022 | Haar Cascade, CNN | Cloud DB | |

IV. PROPOSED SYSTEM

The proposed system is a Smart Electronic Voting Machine that uses facial recognition and machine learning to authenticate voters automatically. Each voter's facial data is registered in advance and stored securely in the system database.
During voting, a camera captures the voter's facial image. The system compares it with stored records. If a match is found and the voter has not voted earlier, the system enables vote casting. After voting, the voter status is updated to prevent multiple voting attempts.

IV. METHODOLOGY

The methodology of the Smart Electronic Voting Machine (EVM) using Facial Recognition follows a systematic process to ensure secure and accurate voting:

• Voter Registration Voters are registered in advance by capturing their facial images along with unique identification details. This data is stored securely in the system database.

• Image Capture During voting, a camera module captures the live facial image of the voter at the polling unit.

• Face Detection and Processioning The captured image is processed to detect the face, remove noise, and normalize features such as size and orientation for better accuracy.

• Facial Recognition and Authentication Machine learning–based facial recognition algorithms compare the live image with the per-registered voter database to verify identity.

• Voting Authorization If authentication is successful, the voting interface is enabled. If verification fails, voting access is denied
• Vote Casting The authenticated voter selects a candidate. The vote is recorded electronically.

## V.WORKING METHODOLOGY

1. Voter Registration Phase
The authorized administrator registers voters by capturing facial images using a camera module connected to Raspberry Pi.
Multiple images of each voter are stored to improve recognition accuracy. The dataset is preprocessed using OpenCV.
2. Dataset Training Phase
Facial features are extracted using machine learning algorithms such as Local Binary Patterns (LBP).
The trained model generates unique face encodings for each voter.
3. Authentication Phase
When a voter arrives:
Live image captured
Face detected
Encoded and compared with database
Confidence score calculated
If match is above threshold → voting allowed.
4. Vote Casting Phase
User selects candidate using push buttons. Vote stored securely in encrypted format.
5. Vote Locking Phase
Database updates voter status to "Voted" to prevent duplicate voting.

## VI.ALGORITHM

A. Local Binary Pattern Histogram (LBPH) Algorithm LBPH is a face recognition algorithm that works by analyzing the texture of a face image. It compares each pixel with its neighboring pixels and creates a binary pattern. These patterns are converted into histograms and used for matching with stored images. It works well in different lighting conditions and is commonly implemented using OpenCV.

B. Convolutional Neural Network (CNN)
is a deep learning algorithm used for face detection and recognition. It automatically learns and extracts important facial features such as eyes, nose, and facial structure from images. CNN provides high accuracy, especially when working with large datasets, and is widely used in modern biometric security systems.

## VII.SECIRITY ANALYSIS

* Biometric authentication prevents impersonation
* Encrypted vote storage prevents tampering
* No internet dependency reduces cyber attacks
* One-time voting lock prevents duplication

## VIII.ADVANTAGES AND DISADVANTAGES

A. Advantages
1)Automated Authentication – Verifies voter identity using facial recognition.
2)Prevents Duplicate Voting – Allows voting only once per voter.
3)Less Human Intervention – Reduces manual errors and bias.
4)Improved Security – Stores votes securely in digital form.
B. Disadvantages
1)Depends on Lighting – Poor lighting may affect accuracy.
2)Needs Proper Training Data – Incorrect data may cause errors.
3)High Cost – Requires camera and hardware setup.
4)Privacy Issues – Facial data storage may raise concerns.

## IX.APPLICATIONS

1)Trade Union Elections
Helps conduct fair and transparent elections for selecting union leaders.
2)Residential Society Elections
Societies can use it for committee elections to avoid duplicate or unauthorized voting.
3)NGO Elections
Non-government organizations can implement it for secure and transparent internal voting processes.

## X.HARDWARE AND SOFTWARE

A. HARDWARE
Camera: -

Used to capture the voter's facial image for authentication. It helps in identifying and verifying the voter using facial recognition.

PC (Computer System): -

Acts as the main processing unit. It runs the facial recognition software, stores voter data, and records votes.

Display Unit (Monitor): -

Displays instructions, candidate list, and voting confirmation messages to the voter.

B. SOFTWARE

OpenCV: -

Open-source computer vision library used for face detection and facial recognition.

Programming Language (Python / Java): -

Used to develop the application logic, database connectivity, and voting system interface.

## XI. SYSTEM ARCHITECTURE

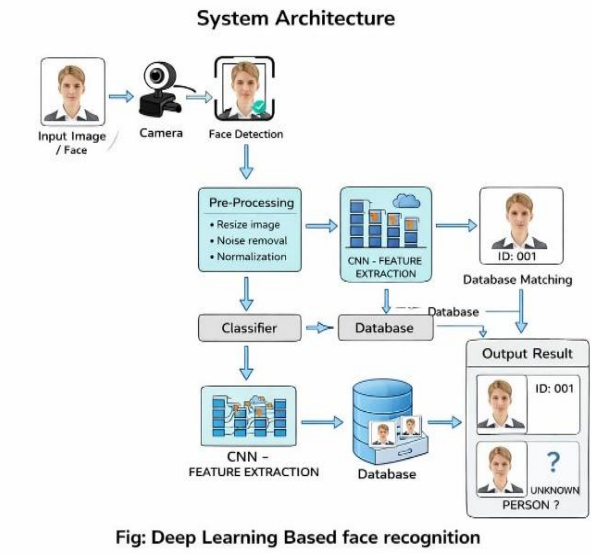


Fig: Deep Learning Based face recognition

## XII.FUTURE ENHANCRMENTS

* Integration with Aadhaar-based biometric database

In the future, the proposed system can be integrated with the Aadhaar-based biometric database to strengthen voter authentication. By combining facial recognition with Aadhaar biometric verification (such as fingerprint or iris recognition), a multi-factor authentication mechanism can be implemented. This would significantly reduce the chances of identity fraud, duplicate voting, and impersonation. However, such integration would require strong encryption protocols, secure API communication, and strict compliance with data privacy regulations. Government authorization and secure data handling mechanisms would be essential to ensure ethical and lawful implementation.

* Blockchain integration for tamper-proof vote storage

Blockchain technology can be incorporated to ensure secure and immutable vote storage. Once a vote is recorded on the blockchain ledger, it cannot be altered or deleted, ensuring transparency and data integrity. Distributed ledger technology minimizes the risk of hacking and centralized data manipulation. By implementing cryptographic hashing and end-to-end encryption, the voting system can become tamper-resistant and fully auditable. This enhancement would increase public trust in electronic voting systems.

* Large-scale deployment for state and national elections

Currently developed as a prototype, the system can be expanded for large-scale deployment in state and national elections. Scalable cloud infrastructure and optimized server architecture can enable the system to handle millions of voters simultaneously. Load balancing, backup servers, and redundancy mechanisms would be necessary to prevent system failure. Efficient database management and high-speed processing techniques would ensure minimal latency and smooth voting operations during peak usage.

* Improved deep learning models for higher accuracy

Future improvements may include the use of advanced deep learning architectures such as Convolutional Neural Networks (CNNs) and transformer-based models to enhance facial recognition accuracy. The system can be trained on diverse datasets to reduce bias and improve recognition under varying lighting conditions, facial expressions, angles, and occlusions (e.g., masks or glasses). Real-time face recognition can be improved through GPU acceleration and model optimization techniques, resulting in faster and more accurate voter verification.

* Offline secure embedded system without internet dependency

To further enhance security, the system can be redesigned as a secure offline embedded system. An

air-gapped architecture can reduce vulnerabilities associated with internet-based cyberattacks. Data can be securely stored locally and later transmitted to a central server through encrypted channels when necessary. Implementation of secure microcontrollers and hardware-level encryption can increase system reliability and protect against unauthorized access.

## XIII.CONCLUSION

The Smart Electronic Voting Machine using Facial Recognition and Machine Learning provides a highly secure, efficient, and modern solution for digital voting systems. By integrating biometric authentication with electronic voting technology, the system ensures that only authorized voters can cast their votes. Facial recognition technology verifies the identity of each voter by matching their live facial image with the stored database, thereby eliminating the possibility of voter impersonation.

The use of Machine Learning, especially deep learning algorithms such as Convolutional Neural Networks (CNN), improves the accuracy of face detection and recognition. The system continuously learns and improves its performance, making it more reliable over time. This reduces false identification and increases overall system efficiency.

One of the major advantages of the proposed system is the prevention of duplicate or repeated voting. Since each voter's facial data is uniquely stored and verified before allowing access to the voting interface, the principle of "one person, one vote" is strictly maintained. Once a vote is cast, the system updates the database immediately, preventing any further voting attempts by the same individual.

Additionally, the system enhances transparency and reduces manual errors that may occur in traditional voting methods. Automation minimizes human intervention, thereby lowering the risk of manipulation, counting mistakes, and fraud. The electronic storage of voting records also ensures faster vote counting and instant result generation.

Furthermore, the integration of biometric and machine learning technologies demonstrates the potential of advanced digital solutions in strengthening democratic processes. It improves security, increases voter confidence, saves time, and reduces operational costs in the long run.

In conclusion, the Smart Electronic Voting Machine using Facial Recognition and Machine Learning represents a significant step toward secure, transparent, and technology-driven electoral systems, ensuring fairness, accuracy, and trust in modern democracy.

## REFERENCES

[1] A. Sharma and R. Verma, "Facial Recognition Based Electronic Voting System International Journal of Computer Applications," vol. 174, no. 5, pp. 12–18, 2022

[2] P. Kumar and S. Singh, "Secure Smart Voting System Using Machine Learning," International Journal of Advanced Research in Computer Science, vol. 14, no. 2, pp. 45–52, 2023.

[3] R. Mehta and K. Joshi, "Biometric Based Electronic Voting Machine", Journal of Information Security and Applications, vol. 59, pp. 102–109, 2021.

[4] M. Desai and N. Shah, "Smart EVM Using Face Recognition and IoT," International Journal of Engineering Research and Technology (IJERT), vol. 11, no. 6, pp. 350–356, 2022.

[5] L. Patel and A. Gupta, "Face Recognition-Based Voting System Using OpenCV," International Journal of Innovative Research in Computer Science and Technology (IJIRCST), vol. 8, no. 4, pp. 112–118, 2020.

[6] T. Brown and E. Wilson, "Secure Voting Using Biometric Authentication," Proceedings of the IEEE International Conference on Smart Systems, pp. 180–185.