

E-Voting Using Face Recognition

K. Kreeshma¹, G. Bala Murugan²

¹Dept of Artificial Intelligence and Data Science

²Assist prof, Dept of Master of Computer Applications

^{1,2} Mohamed Sathak Engineering College, Kilakarai, Tamil Nadu, India

Abstract- This paper presents the design and implementation of an E-Voting System using Face Recognition technology. The proposed system addresses key challenges in traditional voting methods, including voter impersonation, manual errors, and slow vote counting. By integrating facial biometrics, encrypted data storage, and an automated result generation mechanism, the system ensures a secure, transparent, and efficient electoral process. The system is built with five core modules — Admin, Field Officer, Nominee, Voter, and Result — and employs image processing techniques such as face detection, alignment, feature extraction, and feature matching to authenticate voters in real time. Experimental results demonstrate that the proposed system is both technically feasible and socially acceptable, offering a reliable alternative to conventional voting systems.

Keywords: E-Voting, Face Recognition, Biometric Authentication, Image Processing, Feature Extraction, Secure Digital Voting, OTP Verification.

I. INTRODUCTION

Elections form the backbone of every democratic society. The credibility and fairness of an electoral process directly determines the health of a democracy. However, conventional paper-based and manual voting systems suffer from numerous drawbacks including voter fraud, impersonation, long queues, manual counting errors, and lack of transparency.

With the rapid advancement of information technology and biometric systems, electronic voting (e-voting) has emerged as a promising solution. E-voting systems can provide speed, accuracy, and accessibility while reducing human intervention. However, the security of voter identity remains a primary concern.

This paper proposes an E-Voting system that uses Face Recognition as the primary authentication mechanism. Instead of relying on voter ID cards or passwords — which can be forged or forgotten — the system captures the voter's live face and compares it with their registered biometric data stored in the system database. This ensures that only genuine, registered voters can cast their vote.

The rest of this paper is organized as follows: Section 2 presents the literature survey, Section 3 describes the existing system and its limitations, Section 4 presents the proposed system, Section 5 covers the system architecture, Section 6 presents the modules, Section 7 describes the database design, Section 8 presents the feasibility study, and Section 9 concludes the paper.

II. LITERATURE SURVEY

Several researchers have proposed various approaches to improve the security and efficiency of electronic voting systems:

[1] Decentralized E-Voting Portal using Blockchain (Prof. Kritipatidar, Prof. Swapnil Jain) — This work leverages blockchain technology to create a decentralized voting portal. The system ensures public transparency, protects voter anonymity, and secures data transmission and ballot verification. However, it does not incorporate biometric authentication, leaving it vulnerable to impersonation.

[2] Biometrically Secured Electronic Voting Machine (Rahil Rezwani, Huzaifa Ahmed, 2020) — This system uses an Arduino microcontroller combined with a Fingerprint Scanner (FPS) to identify voters. The FPS detects whether a person is a registered voter, counts votes, and prevents fake votes. While effective, fingerprint systems require physical contact and are susceptible to spoofing with fabricated prints.

From the above survey, it is evident that while both blockchain and fingerprint-based approaches improve security, there is a need for a contactless, highly accurate biometric solution. Our proposed system addresses this gap by using Face Recognition, which is contactless, harder to spoof, and does not require specialized hardware beyond a standard camera.

III. EXISTING SYSTEM AND LIMITATIONS

Current voter authentication methods include:

- Token-based Authentication: Unique PIN or password issued to each voter.

- Two-Factor Authentication: Password combined with an OTP sent to the voter's phone.
- Digital Signatures: Cryptographic verification of voter identity.
- Biometric Authentication: Fingerprint or iris scan-based verification.
- Voter ID Cards: Physical cards presented at polling booths.
- Despite these approaches, existing systems face critical limitations:
- Voter ID cards can be forged or lost.
- Passwords and PINs can be stolen or forgotten.
- Fingerprint scanners require physical contact, posing hygiene concerns.
- Manual processes are slow and error-prone.
- These systems remain vulnerable to impersonation and double voting.

IV. PROPOSED SYSTEM

The proposed E-Voting system using Face Recognition overcomes the above limitations through four key features:

- 1) Biometric Authentication:** Voters are verified using real-time facial recognition, ensuring accurate identity validation and completely eliminating impersonation.
- 2) Secure Digital Voting:** All votes are stored in an encrypted database, maintaining confidentiality and integrity throughout the voting process.
- 3) Fast and Automated Process:** Automated verification and instant vote recording reduce waiting time and eliminate manual intervention.
- 4) Transparent and Tamper-Resistant:** The system maintains secure logs and minimizes human involvement, reducing fraud and increasing public trust in the electoral process.

V. SYSTEM ARCHITECTURE

A. Block Diagram – Face Recognition Process

The face recognition module follows a structured image processing pipeline as shown in Table I:

Step	Process	Description
1	Picture Input	Voter's face captured via live camera or loaded from database
2	Pre-processing	Image resized, brightness adjusted, and noise removed
3	Face Detection	System scans and locates the face region within the image
4	Face Alignment	Detected face rotated and normalized to standard orientation
5	Feature Extraction	Unique facial measurements (eye distance, jaw width) extracted
6	Feature Matching	Extracted features compared with stored biometric data
7	Face Recognition	Identity confirmed or denied; voter proceeds if matched

Table I: Face Recognition Pipeline

B. System Workflow

The complete user workflow in the system is as follows:

- Start: User opens the application and proceeds to Registration.
- Registration: User details and face data are captured and stored in the server database.
- Login: User enters UID and EID. System validates credentials.
- Face Recognition: Live face captured and sent to server for verification.
- OTP Verification: Valid OTP is sent and confirmed for an extra security layer.
- Voting Page: Voter views nominees from their constituency and selects a candidate.
- Vote Cast: Vote is securely recorded in the database.
- Result Display: Admin triggers result; system counts votes and displays winner.
- Logout: Session ends securely.

VI. SYSTEM MODULES

The system is divided into six independent modules as described in Table II:

No.	Module	Users	Key Functions
1	Admin Module	Admin	Election setup, Field Officer mgmt, Nominee approval, Result display
2	Field Officer Module	Field Officer	Voter registration, Face photo capture
3	Nominee Module	Nominee	Candidate registration, Application status view
4	Voter Module	Voter	Face verification, OTP check, Vote casting
5	Result Module	Public/Admin	Vote counting, Winner declaration
6	Face Recognition Module	System	Image processing, Biometric matching

Table II: System Modules

VII. DATABASE DESIGN

The system uses a relational database. The primary tables are described below:

A. CRTable – Candidate Registration Table

Field Name	Data Type	Key/Null	Description
CName	varchar(50)	Not Null	Nominee Name
FName	varchar(50)	Not Null	Father Name
CNumber	numeric(10,0)	Not Null	Contact Number
Gender	varchar(20)	Not Null	Gender
DOB	datetime	Not Null	Date of Birth
State	varchar(50)	Not Null	State
Cons	varchar(50)	Not Null	Constituency
CRecord	varchar(50)	Not Null	Criminal Record
AINcome	numeric(12,2)	Not Null	Annual Income
FAssets	numeric(14,2)	Not Null	Property Assets
PName	varchar(50)	Not Null	Party Name
UName	varchar(50)	Primary Key	Username (Login)
PWord	varchar(50)	Not Null	Password
Status	varchar(50)	Not Null	Accepted / Rejected

Table III: Candidate Registration Table

B. ElectionDate Table

Field Name	Data Type	Description
State	varchar(50)	Name of the state
EDate	datetime	Scheduled election date

Table IV: Election Date Table

C. FieldReg Table – Field Officer Registration

Field Name	Data Type	Description
name	varchar(50)	Field Officer Name
id	varchar(50)	Unique Officer ID
pwd	varchar(50)	Login Password
cons	varchar(50)	Assigned Constituency

Table V: Field Officer Registration Table

VIII. FEASIBILITY STUDY

Economical Feasibility: The system utilizes open-source frameworks and standard web technologies, making it cost-effective to develop and deploy within a reasonable budget.

Technical Feasibility: All required technologies — face recognition libraries (OpenCV, dlib), web development frameworks, and relational database management systems — are mature, stable, and freely available.

Social Feasibility: The system is designed with a user-friendly interface suitable for voters of all age groups. Minimal technical knowledge is required from the voter, ensuring high acceptance.

IX. CONCLUSION

This paper has presented a comprehensive E-Voting system that uses Face Recognition technology for secure voter authentication. The system effectively addresses the key challenges of traditional voting — impersonation, fake votes, manual errors, and slow result declaration.

By combining biometric face recognition with OTP-based two-factor authentication, encrypted data storage, and

automated result generation, the system ensures that every vote is genuine, confidential, and counted accurately. The modular architecture — comprising Admin, Field Officer, Nominee, Voter, Result, and Face Recognition modules — makes the system scalable and maintainable.

Future work can extend this system by incorporating blockchain for immutable vote storage, multi-language support for wider accessibility, and mobile application integration for remote voting. The proposed system has the potential to significantly modernize the electoral process and strengthen democratic institutions.

REFERENCES

- [1] Prof. Kritipatidar, Prof. Swapnil Jain, "Decentralized E-Voting Portal Using Blockchain Technology," International Journal of Advanced Research in Computer Science, 2020.
- [2] Rahil Rezwan, Huzaifa Ahmed, "Biometrically Secured Electronic Voting Machine using Arduino and Fingerprint Scanner," IEEE International Conference on Computer Science and Engineering, 2020.
- [3] T. Kohno, A. Stubblefield, A. D. Rubin, D. S. Wallach, "Analysis of an Electronic Voting System," IEEE Symposium on Security and Privacy, 2004.
- [4] W. Zhao, R. Chellappa, P. J. Phillips, A. Rosenfeld, "Face Recognition: A Literature Survey," ACM Computing Surveys, Vol. 35, No. 4, pp. 399-458, 2003.
- [5] OpenCV Documentation, "Face Detection and Recognition using OpenCV," <https://opencv.org>, 2023.