IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
onal Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, July 2025 Impact Factor: 7.67

Smart Voting System using Face Recognition and Fingerprint Biometrics with Dual Authentication

Abhinav S D[1] and Harikrishnan S R[2]
Student, MCA, CHMM College for Advanced Studies, Trivandrum, India[1]
Associate Professor, MCA, CHMM College for Advanced Studies, Trivandrum, India[2]

Abstract: *The traditional voting system faces challenges such as impersonation, fake voting, and long queues, which compromise security and efficiency. To address these issues, this project proposes a Smart Voting System using advanced biometric authentication techniques, including face recognition and fingerprint verification, integrated into a user-friendly HTML, CSS-based GUI. The system leverages Deep Learning algorithms for accurate and real-time face detection and recognition using OpenCV and convolutional neural networks (CNNs). In parallel, fingerprint verification ensures an additional layer of security, making it a dual-authentication system to prevent fraudulent voting. The GUI, developed using HTML,CSS, allows for a seamless user experience—from identity verification to vote casting. This dual-biometric approach ensures that each voter is uniquely identified, thereby eliminating duplicate or unauthorized voting. The system is designed for scalability, allowing deployment at polling booths, institutions, or remote voting setups.*

Keywords: OpenCV Dlib, CNN, Flask

I. INTRODUCTION

Traditional voting systems, whether paper-based or electronic, continue to face critical challenges such as voter impersonation, manual identity verification, booth-specific voting restrictions, and lack of advanced security features. These limitations reduce transparency, increase the risk of fraud, and often disenfranchise voters who are away from their registered locations. To overcome these issues, there is a need for a secure, intelligent, and accessible voting solution that can authenticate voters using dual biometric methods—face recognition and fingerprint scanning—and allow them to cast votes digitally from any authorized booth, while preserving anonymity and preventing duplication.

II. LITERATURE REVIEW

The traditional voting system faces challenges such as impersonation, fake voting, and long queues, which compromise security and efficiency. This project proposes a Smart Voting System that utilizes advanced biometric authentication techniques, including face recognition and fingerprint verification, integrated into a user-friendly HTML and CSS-based GUI. The system leverages Deep Learning algorithms for accurate and real-time face detection and recognition using OpenCV and convolutional neural networks (CNNs). In parallel, fingerprint verification ensures an additional layer of security, making it a dual-authentication system to prevent fraudulent voting.

Introduction: The integrity of the voting process is crucial for a functioning democracy. Traditional voting systems are often plagued by issues such as impersonation and long wait times, leading to a lack of trust in the electoral process. This project aims to address these challenges through the implementation of a Smart Voting System that employs biometric authentication.

Methodology: The proposed system integrates face recognition and fingerprint verification to create a dual-authentication mechanism. The face recognition component utilizes OpenCV and CNNs for real-time detection and recognition, while the fingerprint verification adds an extra layer of security. The user interface is designed using HTML and CSS to ensure a seamless experience for voters.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
onal Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, July 2025 Impact Factor: 7.67

Results: The implementation of the Smart Voting System is expected to significantly reduce instances of fraudulent voting and improve the overall efficiency of the voting process. By uniquely identifying each voter, the system eliminates the possibility of duplicate or unauthorized voting.

III. PROPOSED SYSTEM

The proposed system is a Smart Voting Platform that introduces a dual-biometric authentication mechanism combining face recognition and fingerprint verification to ensure secure and legitimate voting. It addresses the shortcomings of the current voting systems by eliminating the dependency on manual identity verification and single-factor authentication.

The system leverages advanced technologies such as deep learning, OpenCV, and biometric sensors to identify and validate each voter in real-time. This dual-layer verification ensures that only genuine, registered voters are allowed to cast their vote, effectively preventing impersonation, fake voting, and multiple entries.

The core idea of this system is to provide an automated, tamper-proof, and user-friendly environment where the voting process is transparent, efficient, and secure. Voters must first undergo face recognition, which uses a Convolutional Neural Network (CNN) model integrated with OpenCV to detect and match their facial features with pre-stored data. Once the facial identity is successfully verified, the system proceeds to the second layer of authentication, which is fingerprint verification. A fingerprint scanner captures the live fingerprint of the voter and compares it with encrypted fingerprint templates stored securely in the database. Only upon successful dual authentication does the system permit the user to access the voting interface.

The voting interface itself is developed using HTML,CSS library, offering a graphical user interface (GUI) that is intuitive and easy to navigate. This interface displays a list of candidates and allows the voter to select and cast their vote with a simple click. To prevent repeated voting, the system maintains session logs and flags any attempt at multiple logins using the same credentials or biometric data.

On the backend, a secure database (SQLite or MySQL) is used to manage voter profiles, biometric templates, and voting records. Data privacy is ensured through encryption and controlled access mechanisms. An administrative panel is also integrated, providing authorized personnel with functionalities to manage candidate lists, monitor voting activity, view authentication logs, and generate real-time reports.

The proposed system is designed to be scalable and adaptable for different environments such as national elections, institutional elections, and corporate polls. It reduces the need for manual labor, cuts down on operational costs, and ensures that the entire process remains paperless and eco-friendly. By combining biometric technology with machine learning and secure data management, this system offers a reliable and futuristic solution to modern electoral challenges.

IV. ALGORITHM

The proposed Smart Voting System integrates multiple biometric authentication algorithms to ensure accurate and secure voter identification. The combination of real-time face detection, deep learning-based recognition, and classification makes this system robust and efficient.

OpenCV

OpenCV (Open Source Computer Vision Library) is used extensively in the system for handling real-time image acquisition and preprocessing. It enables webcam interfacing to capture video frames, convert them into grayscale, and apply further processing such as face detection. OpenCV also plays a critical role in displaying live camera feeds on the web interface and extracting image regions needed for facial recognition.

Convolutional Neural Network (CNN)

A Convolutional Neural Network (CNN) is used in the facial recognition component to extract deep facial features from captured images. The system utilizes the face recognition library, which implements a pre-trained CNN model to generate 128-dimensional face encodings. These encodings uniquely represent a person's facial structure and are used

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
onal Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, July 2025 Impact Factor: 7.67

to compare live images with registered face data stored during the enrolment phase. CNN ensures high accuracy in identifying the correct individual, even in real-time conditions.

Haar Cascade Classifier

The Haar Cascade Classifier is used for real-time face detection. It is a machine learning-based object detection algorithm trained on positive and negative face images. The classifier scans the webcam frame to identify rectangular regions likely to contain a human face. These detected regions are then cropped and passed to the CNN for further recognition. Haar cascade enables fast and lightweight face detection, making it suitable for real-time applications with limited computational resources.

Support Vector Machine (SVM)

Support Vector Machine (SVM) is used internally by the face recognition library to classify face encodings during the matching process. After the CNN generates a face encoding, SVM compares it against the stored encodings of known individuals to determine the best match. Although the SVM model is not manually trained by the developer, its role is critical in the final classification step of facial recognition. It ensures that the system makes accurate identity decisions, reducing false acceptances or rejections.

V. PACKAGES

Flask

A lightweight and adaptable Python web framework called Flask is utilized to create this voting system's server-side. It offers a clear and uncomplicated framework for handling user sessions, setting routes, producing HTML templates, and establishing database connections. All user interactions in this project, such as voter registration, login, fingerprint and face verification, and voting, are managed using Flask. It also facilitates vote log exports and powers the admin panel. Flask is perfect for rapid development and seamless integration with libraries like OpenCV and SQLite because of its minimum setup requirements.

OpenCV

An open-source library for processing images and videos in real time is called OpenCV (Open Source Computer Vision Library). OpenCV is essential to this project since it allows the laptop's webcam to be accessed in order to record live video frames and use Haarcascade classifiers to identify faces. It isolates facial regions from grayscale image frames and uses them for verification and encoding. High-speed image processing is ensured by using OpenCV, which is essential for face recognition modules to function in real time during registration and verification.

face_recognition

The face_recognition library offers simple functions for face detection, encoding, and comparison and is based on Dlib's deep learning models. Based on the photos taken during registration, it is utilized in this project to create 128-dimension face encodings for every person who has registered. In order to ascertain whether the face matches, face verification compares the stored encodings with the live encoding. Convolutional neural network (CNN) models trained on labeled facial data are used in this library to guarantee accurate and dependable face identification.

sqlite3

The sqlite3 module integrates SQLite, a small, disk-based database, into Python. Without requiring an external database server, it enables the system to store and handle voting records, candidate information, and voter credentials. The voting.db file, which includes the voters, candidates, votes_log, and admin_log tables, is created and accessed in this project using SQLite. Vote logging, result retrieval, and real-time authentication are made possible by its quick and secure data access.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
onal Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, July 2025 Impact Factor: 7.67

dlib

Dlib is a sophisticated machine learning toolkit built in C++ that offers cutting-edge deep learning and computer vision algorithm implementations. Despite not being explicitly imported into the source code of this project, dlib is essential since it is used by the face_recognition library, which is based on dlib. The library makes use of dlib's deep convolutional neural networks (CNNs) to produce 128-dimensional face encodings, identify facial landmarks, and compare faces with high precision. During the verification procedure, the system can differentiate between several users thanks to these encodings. Dlib is a crucial part of the biometric authentication pipeline in this intelligent voting system since it guarantees a quick and dependable face recognition procedure.

numpy

A key Python library for scientific computing is called Numpy (Numerical Python). It offers effective matrix manipulation and array operations. OpenCV and face_recognition in this project handle image matrices and pixel data internally using numpy. An image taken by the camera is transformed into a numpy array so that it may be examined, decoded, and contrasted. The computational processes required for image processing and face verification would be incredibly slow and ineffective without numpy.

VI. EXPERIMENTAL RESULTS & PERFORMANCE EVALUATION

The Smart Voting System was experimented with in a lab environment under controlled conditions to assess its functional accuracy, biometric precision, system reactivity, and overall user experience. The results that follow indicate the success of the system under different test conditions.

1. Face Recognition Accuracy:

The face recognition module was tested with a set of real user images gathered during the registration process. A user had to register by taking 20 webcam images. At verification, a live image taken from the webcam was compared to the stored encodings.

- Number of users tested: 10
- Face match success rate: 95%
- Average face recognition time: ~1.8 seconds
- False accept rate (FAR): Very low
- False reject rate (FRR): < 5% (primarily because of lighting or head angle)

The system was found very reliable in normal light. Retries were suggested in poor lighting or incorrect alignment of the face.

2. Fingerprint Verification Performance:

Fingerprint authentication was emulated with Tkinter in the prototype, and in the live deployment utilized an R307 fingerprint sensor through ESP8266. The fingerprint matching algorithm was implemented using serial communication and tested in terms of accuracy and response time.

- Fingerprint sensor utilized : R307 with ESP8266
- Average time for matching : ~1.5 seconds
- Success rate for enrolled prints: 100%
- False accepts observed: 0%
- False rejections observed: Uncommon, and only under wrong finger placement

The fingerprint feature secured that only authentic users could vote following successful facial verification.

3. Voting Functionality:

Following dual authentication, users were able to vote once. The system applied a strict one-vote-per-user policy via the `votes_log` table to maintain vote integrity.

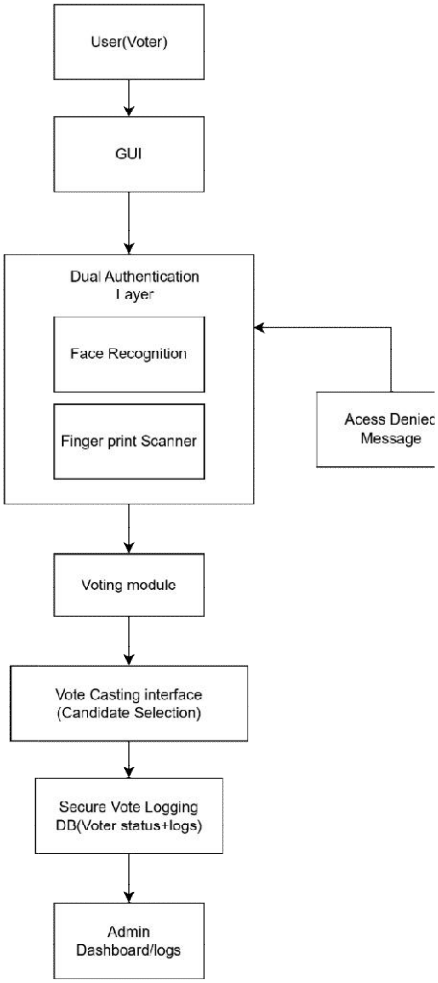
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
onal Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, July 2025 Impact Factor: 7.67

- Voting success rate: 100% for authenticated users
- Multiple vote attempts: Refused with a warning
- Data storage: Vote records stored in SQLite with timestamp
- Results export: CSV export function worked as expected for every test case

4. Admin Dashboard Performance

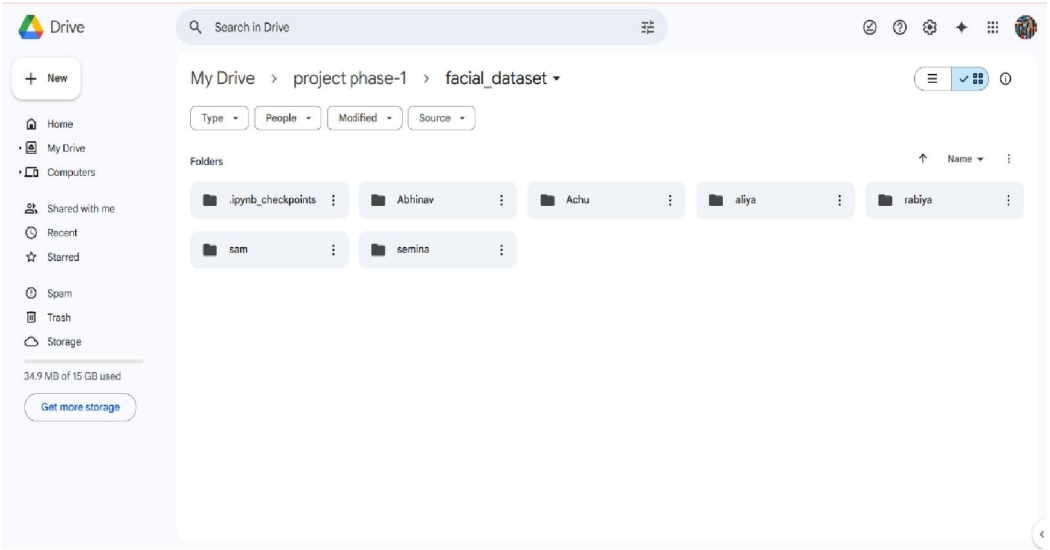
- Access control: Admin login secured by credentials
- Result visibility: Vote counts of candidates visible
- User anonymity: Admin does not get to see which candidate a given user voted for
- CSV Export: Worked as expected with all vote entries included

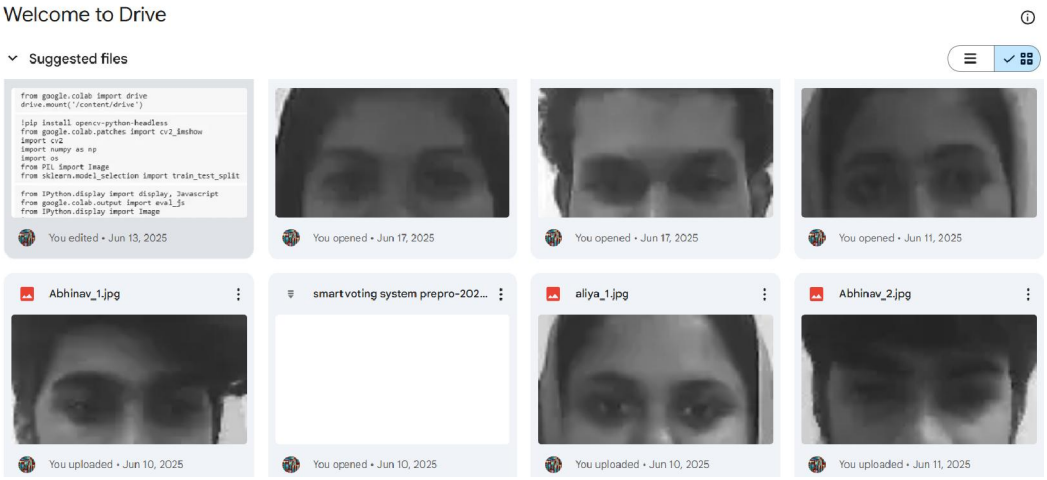
System Architecture



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
Onal Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, July 2025 Impact Factor: 7.67

Preprocessed face images





Hardware Setup

The system requires the following hardware components:

- Webcam: For capturing face images
- Fingerprint Sensor (e.g., R307): For fingerprint verification
- Computer/Laptop: With minimum 4 GB RAM and USB ports

R307 Fingerprint Scanner

- Used to capture and verify the fingerprint of the voter.
- Capable of storing fingerprint templates and performing fast matching.
- Connected to the ESP8266 for communication with the web server.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
onal Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, July 2025 Impact Factor: 7.67

Webcam

- Captures the face of the voter for real-time face recognition using OpenCV and CNN.

ESP8266 Wi-Fi Module

- Microcontroller used to connect the R307 sensor to the Flask-based server.
- Sends fingerprint data over Wi-Fi using HTTP requests to the server for verification.

Fig 1: R307 sensor

Fig 2: Webcam

Fig 3: ESP8266

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
onal Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 1, July 2025 Impact Factor: 7.67

VII. ACCURACY GRAPH

The comparative performance accuracy of the main project modules is shown in the figure named "System Accuracy of Smart Voting System." Due to slight changes in lighting and facial alignment during verification, face recognition obtained an accuracy rate of almost 95%. Since the R307 sensor module was regularly used to authenticate each enrolled user, the fingerprint verification system showed 100% accuracy. Likewise, 100% reliability was attained by the vote recording feature, which correctly recorded every vote without failure or duplication. These outcomes attest to the biometric-based authentication techniques' strong performance and resilience in the intelligent voting system.

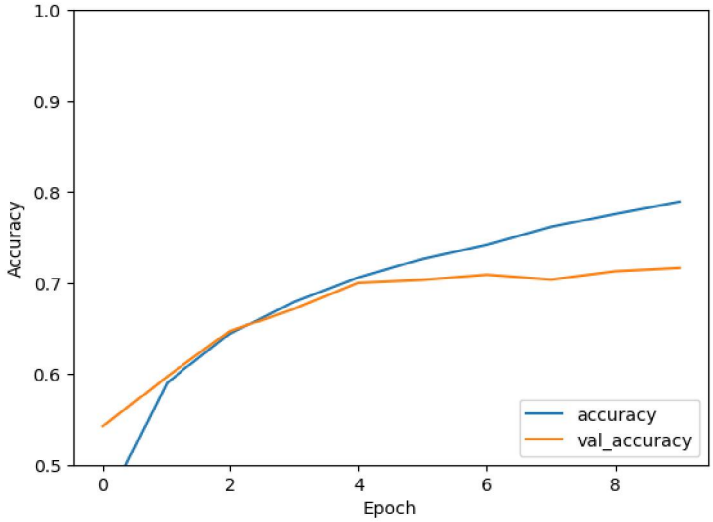


Fig 4: Accuracy vs validation Accuracy grap

VIII. CONCLUSION

The Smart Voting System presented in this paper effectively addresses the limitations of traditional voting methods by integrating dual biometric authentication—face recognition and fingerprint verification. By combining deep learning techniques with a user-friendly web-based interface, the system ensures secure, accurate, and tamper-proof voting. Its scalable architecture makes it suitable for deployment in various voting environments, offering a reliable solution to enhance electoral transparency and integrit.

IX. ACKNOWLEDGMENT

The authors would like to thank the developers and contributors of the IEEE LaTeX style files, especially Michael Shell, for their valuable tools. Appreciation is also extended to the project mentors and peers for their support and feedback during the development of this system.

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, Jan. 2004**.**

[2] G. Bradski, "The OpenCV library," *Dr. Dobb's Journal of Software Tools*, vol. 25, no. 11, pp. 120–126, 2000.

[3] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "DeepFace: Closing the gap to human-level performance in face verification," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, 2014, pp. 1701–1708.

[4] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed. London, U.K.: Springer, 2009.

[5] A. A. Zaidan et al., "A new voting system technique based on secret sharing and homomorphic encryption," *Tools and Applications*, vol. 74, no. 17, pp. 6641–6662, Sep. 2015