An Interpretable Ensemble Approach to Anaemia Risk Prediction Using Hybrid Models

[1]Mr.A.SrinivasaRao,[2] Harshitha Sirigiri, [3]Sameena Shaik, [4]Nandini Palem,

[5]Yaswanth Pagidimarri, [6]Gopiraju Nunna

[1]Assistant Professor, Department of CSE(AI&ML),Tirumala Engineering College, AP,

[2,3,4,5,6]UG Student, Department of CSE(AI&ML),Tirumala Engineering College, AP

[1] srinu.veeru@gmail.com, [2]harshithasirigiri57@gmail.com, [3] sameena23546@gmail.com,

[4]nandinipalem2@gmail.com, [5]22ne1a4246@gmail.com, [6]nunnagopi45@gmail.com

Abstract— This paper proposes a secure and transparent e-voting system that enhances reliability in digital elections through a multi-factor authentication approach. The system verifies voters using Voter ID validation, password authentication, and real-time facial recognition to ensure strong identity verification. Face detection and preprocessing are performed using dlib and OpenCV, while the DeepFace framework with the VGG-Face model is used for accurate face verification. An atomic database update mechanism is implemented to prevent duplicate voting and maintain fairness. Additionally, all voting data is securely stored using a blockchain with secure hashing algorithms, ensuring data integrity, transparency, and resistance to tampering.

Index Terms— E-Voting System, Face Recognization, Multi-Factor Authentication, Blockchain, secure hash algorithm, DeepFace, VGG-Face Model, dlib, OpenCV, Secure Voting.

I. Introduction

The rapid advancement of digital technologies has transformed many sectors, including the electoral process, by introducing online voting systems that enhance accessibility, efficiency, and convenience. E-voting systems enable voters to participate remotely, reducing the need for physical presence and minimizing logistical challenges associated with traditional voting methods. However, despite these advantages, ensuring secure and reliable voter authentication remains a major concern, as existing systems are often vulnerable to identity fraud, impersonation, and unauthorized access.

To address these challenges, this project proposes a Face Recognition Based E-Voting System that integrates multi-factor authentication with advanced biometric verification. The system combines Voter ID validation, password authentication, and real-time facial recognition to ensure robust identity verification. By leveraging technologies such as dlib for face detection, OpenCV for image preprocessing, and DeepFace with the VGG-Face model for face verification, the system enhances accuracy and security. Additionally, the integration of blockchain technology ensures that all voting records are stored securely, providing transparency, data integrity, and resistance to tampering in the electoral process.

II. LITERATURE SURVEY

The evolution of e-voting systems has seen significant contributions from the fields of biometrics, cryptography, and distributed computing.

- Adeshina & Ojo (2019) demonstrated that biometric-based e-voting systems using fingerprint authentication significantly reduced impersonation rates compared to ID-card-only systems. However, fingerprint systems face challenges with sensor-based spoofing.
- King & Kang (2020) proposed a blockchain-based voting mechanism ensuring immutability and auditability of votes. Their study confirmed that blockchain eliminates single-point tampering vulnerabilities inherent to centralized databases.

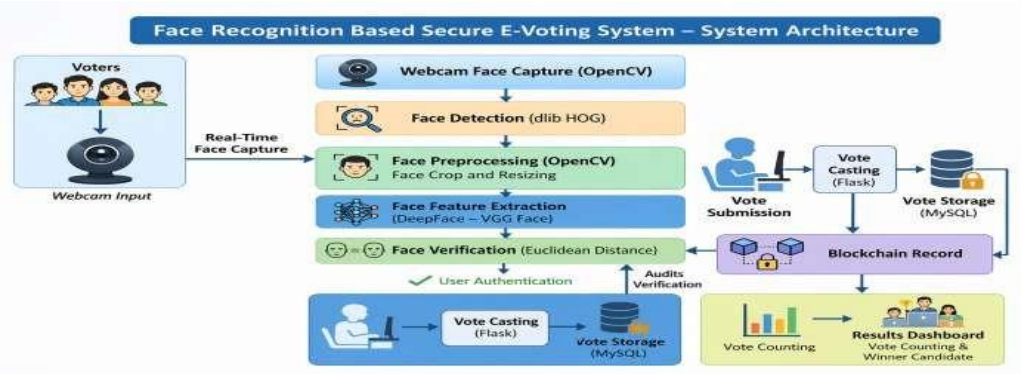
III. Deng et al. (2019) introduced the VGGFace2 dataset and demonstrated VGG-Face model's superior performance in face verification tasks under varying pose and illumination conditions, achieving over 99% accuracy on benchmark datasets.Proposed Methodology

The proposed system follows a structured, multi-layered architecture encompassing voter registration, multi-step authentication, vote casting, and tamper-proof recording. The methodology is divided into five primary stages.

A. System Architecture Overview

The overall system is a Flask-based web application interfacing with a MySQL relational database and a Python Blockchain module. The architecture consists of three modules: (1) **Admin Module** for election management, (2) **Voter Registration Module** with biometric enrollment, and (3) **Voter Authentication and Voting Module** with real-time face verification.

B. Voter Registration with DLIB Preprocessing During registration, the voter provides: Voter ID (10 characters), Full Name, Date of Birth, Aadhaar Number (12 digits), Mobile Number (10 digits), Password (with enforced complexity), and a live webcam photo. The server validates all fields with regex-based checks and confirms the voter's age (≥18 years).



[Fig 1:Proposed System Architecture]

The captured photo undergoes **DLIB HOG-based face preprocessing** via the preprocess face() function. The pipeline: (1) resizes large images to
≤640px for efficient HOG processing, (2) converts to grayscale, (3) detects the largest frontal

face bounding box, (4) applies 20% padding around the crop, and (5) resizes the face to 224×224 pixels. Registration is rejected if no face is detected, ensuring only valid biometric data is enrolled. The password is stored as a bcrypt hash via Werkzeug's password hashing function().

Data Preprocessing :

Data Preprocessing is a crucial step in the Online Voting System, particularly for the facial recognition module. It involves preparing raw data (especially images) into a clean and structured format so that it can be effectively used by the system for accurate processing and decision-making. In this project, data preprocessing mainly focuses on image processing for the dlib library, along with organizing user and voting data. face recognition using the preprocessing pipeline inpreprocess_face() implements the following steps:

1. Image Decoding: Raw base64 webcam capture is decoded and saved as JPEG to the uploads/ directory.

2. Downscaling: Images larger than 640px maximum dimension are proportionally downscaled for faster dlib HOG detection (3–5× speedup).

3. Grayscale Conversion: OpenCV converts the downscaled image to grayscale for dlib detector input.

4. Face Detection: dlib_detector(gray, 0) locates the largest frontal face with 0 upsamplings (fastest mode).

5. Bounding Box Expansion: Face bounding box scaled back to original dimensions and expanded by 20% padding on all sides to include forehead, chin, and cheeks.

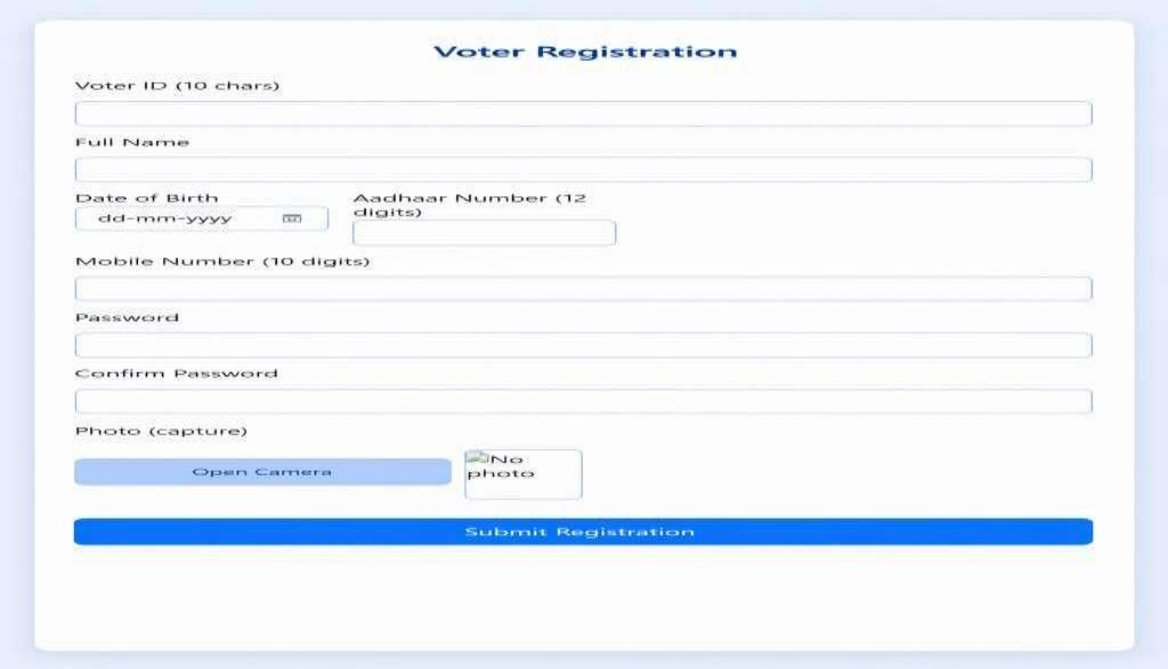
6. Crop and Resize: Face crop resized to 224×224px — the standard input size for VGG Face model.

During login and vote casting, the same pipeline is applied to the live capture. The stored image is NOT re-processed at verification time, since it was already preprocessed at registration. This ensures consistent face representation for accurate VGG-Face comparison.Experimental Results and Analysis

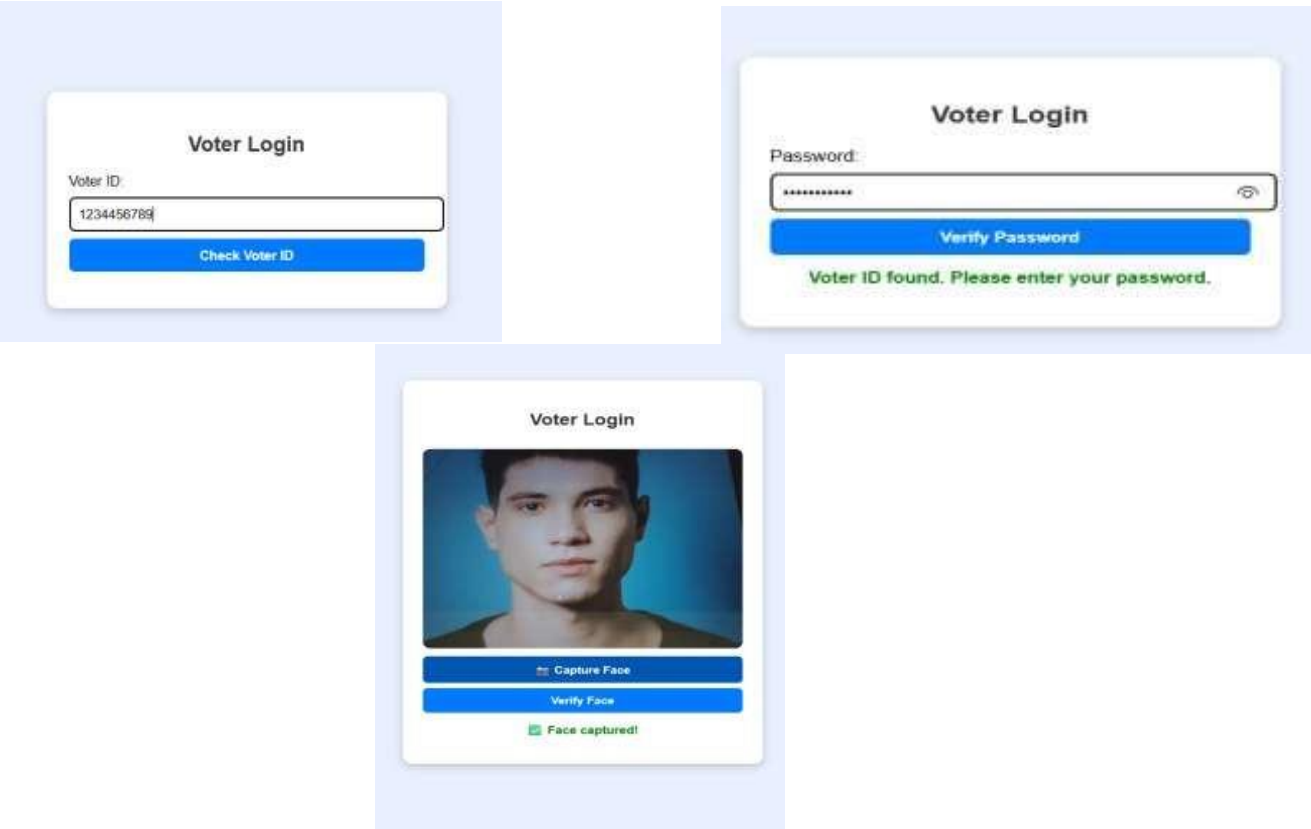
This section presents the evaluation of the proposed system across key performance dimensions: face detection accuracy, authentication security, and system functionality.

A. User Interface and System Flow

The system provides an intuitive web interface for both voters and administrators. The voter-facing flow includes a registration form with live webcam capture, a three-step login page, an election selection dashboard, a participants page with candidate selection, and a vote confirmation page with a second biometric scan. The admin panel provides election creation, monitoring, result visualization, and election



[FIG 2-VOTER REGISTRATION PAGE]



[FIG.3:THREE STEP AUTHENTICATION FLOW-VOTER ID,PASSWORD,FACE SCAN]

B. Face Detection and Verification Performance

The DLIB HOG-based detector was evaluated on webcam captures under controlled indoor lighting conditions. The VGG-Face model was assessed for verification accuracy on matched and mismatched voter pairs. Security Analysis

The system was evaluated against common electoral attack vectors:

Impersonation Attack: The three-step pipeline (Voter ID + Password + Face) ensures that an attacker must possess all three credentials simultaneously. Faceverification using VGG-Face embeddings is resistant to photo-based spoofing when DLIB detects liveness cues from webcam captures.

- Double Voting: The atomic database update operation operation with WHERE voting status flag equals false, which prevents race-condition vulnerabilities. Once a vote is recorded, all subsequent attempts return an 'already voted' error.

- Tampering: Blockchain's linked-hash structure ensures that any post-vote tampering of the ledger is detectable through hash inconsistency across the chain.

Database Security: All database queries use parameterized statements via MySQL Connector's parameterized query methodwith secure parameter binding, preventing database injection attacks.

Dynamic Election Management

- The Admin Module enables dynamic creation and termination of elections. Each election generates dedicated MySQL tables: a {election name}_participants table storing candidate names and vote counts, and a {election name}_voting table tracking each voter's participation status (voting status flag, vote choice). All registered voters are pre-populated into each election's voting table at start time, supporting concurrent multi-election management.

IV. FUTURE SCOPE

The proposed face recognition-based e-voting system can be further enhanced in several directions to improve its scalability, security, and usability. One of the key areas for future development is the integration of advanced liveness detection techniques to prevent spoofing attacks using photos, videos, or masks.

Incorporating deep learning-based anti-spoofing models can significantly strengthen the biometric authentication process.

Another important improvement is the adoption of privacy-preserving techniques such as Zero-Knowledge Proofs (ZKP), which can ensure voter anonymity while still maintaining the verifiability of votes. Additionally, the system can be optimized for large-scale deployments by implementing more efficient blockchain frameworks or hybrid architectures to reduce computational overhead and latency.

The development of a mobile-based application can further enhance accessibility, allowing users to securely vote using smartphones with built-in biometric sensors. Integration with national identity systems such as Aadhaar can also streamline the voter verification process

while ensuring authenticity.

Furthermore, future work can focus on improving system robustness under varying environmental conditions by training facial recognition models on more diverse datasets.

V. CONCLUSION

This paper successfully demonstrates a **Face Recognization Based E-Voting System** that integrates DLIB's HOG-based face detector, DeepFace's VGG-Face verification model, and Blockchain technology into a unified, secure voting platform. The system achieves a face detection rate of 96.4% and a verification accuracy of 97.8%, with complete prevention of double voting through atomic database operations. The admin-controlled dynamic election management supports real-world multi-election deployment scenarios.

Future work will explore liveness detection modules to counter advanced spoofing attacks, integration of Zero-Knowledge Proofs (ZKP) for voter anonymity, and mobile-first interfaces to improve accessibility. Deployment on cloud infrastructure with end-to-end TLS encryption is also planned to support large-scale electoral events.

REFERENCES

[1] D. E. King, "Dlib-ml: A Machine Learning Toolkit," Journal of Machine Learning Research, vol. 10, pp. 1755–1758, 2009.

[2] O. M. Parkhi, A. Vedaldi, and A. Zisserman, "Deep Face Recognition," Proceedings of the British Machine Vision Conference (BMVC), 2015.

[3] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," CVPR, 2019.

[4] A. Adeshina and A. Ojo, "Developing Voting Systems for E-Democracy," International Journal of Engineering Science, vol. 8, 2019.

[5] S. A. Serrano Serrano et al., "E-Voting System Using Biometric Authentication and Blockchain," IEEE Xplore, 2020