IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Smart Voting System With Liveness-Aware Facial Biometrics And Multi-Level OTP Authentication

Dr.D.HariKrishna[1],P. Afiyad[2], P. Roja Veera Raghavamma[3], Ch. Bhramaramb[4], G. Indu[5]

1. Associate Professor(1).Dept Of CSE(CAI), KKR & KSR Institute Of Technology And Sciences
2,3,4,5 Students, Dept Of CSE(CAI), KKR & KSR Institute Of Technology And Sciences

1. Abstract

Voting is an essential part of democratic systems, but manual verification-based traditional voting procedures are laborious and susceptible to mistakes, fraud, and duplicate voting. Facial recognition has become a dependable and unobtrusive method of voter authentication with the development of biometric technologies. In order to prevent spoofing attacks, this paper presents a Smart Voting System Through Face Recognition that combines facial biometrics with liveness detection. A multi-level authentication method utilizing OTP with offline support is integrated to further improve security and dependability, producing a voting solution that is quicker, more secure, and useful for real-world implementation.

Keywords: Smart Voting System, Face Recognition, Biometric Authentication, Liveness Detection, Offline OTP.

2.Introduction

Elections are essential to democracy because they allow the general public to participate in decision-making. Conventional voting techniques rely on manual processes like ballot marking on paper, voter identity verification, and physical supervision. Despite being widely used, these approaches frequently have operational inefficiencies, lengthy wait times, and high labour requirements.

Ensuring that only eligible voters participate and that each voter casts a single ballot is a significant challenge in contemporary voting systems. As the number of voters rises, problems like impersonation and duplicate voting continue to undermine the validity of election results. Facial recognition is becoming more popular because it is contactless and easy to use, and biometric authentication has become a dependable method of voter identification. But facial recognition by itself is susceptible to spoofing attacks with pictures or videos. The suggested system incorporates liveness detection and extra

authentication layers to improve security and overall system dependability in order to overcome this restriction.

3. Problem Statement

Conventional voting methods are laborious, prone to mistakes, and vulnerable to fraud like impersonation, duplicate voting, and unauthorized access because they depend on manual verification and physical supervision. Many electronic voting systems rely on single-factor techniques like fingerprint or facial recognition, which are susceptible to spoofing attacks using photos or videos, even though biometric authentication increases efficiency. Additionally, their usability in remote or rural areas is limited by their reliance on constant internet connectivity for OTP or verification. A secure, dependable, and scalable voting system is therefore required in order to improve overall voting efficiency while guaranteeing accurate voter authentication, preventing fraudulent activity, supporting offline operation, and protecting voter privacy.

4. Objectives

The primary goals of the suggested Smart Voting System Through Face Recognition are:

- Using facial recognition technology to create a safe and dependable electronic voting system
- Using liveness detection to thwart spoofing and impersonation attacks
- To provide a scalable and user-friendly system appropriate for real-world deployment
- To enable offline OTP authentication for voting in low or no network conditions
- To guarantee one-person-one-vote integrity and eliminate duplicate voting
- To reduce manual intervention and speed up the voting process

5. Literature Review

The application of biometric technologies in electronic voting systems has been the subject of numerous studies, which have reported increases in security and efficiency. Early methods mostly relied on fingerprint-based authentication, which offered precise voter verification but necessitated physical contact and extra hardware. Researchers turned to facial biometrics to get around these restrictions and provide a more practical and contactless voting experience.

Computer vision methods for automated face detection and recognition in voter authentication have been the focus of recent research. To minimize human intervention and expedite the voting process, tools like OpenCV and feature-extraction algorithms have been widely utilized. Nevertheless, a lot of these systems are vulnerable to spoofing attacks using images or videos since they rely on single-factor facial recognition.

Some studies have added One-Time Password (OTP) verification as an extra security layer to improve authentication. However, OTP delivery via email or SMS relies on constant network connectivity, which might not be possible in some areas. Other strategies, like blockchain-based voting systems, seek to

increase data integrity and transparency but frequently encounter scalability and adaptability issues. These constraints spur the creation of voting systems that are more dependable and safe.

6. Research Gap

Biometric-based electronic voting systems that use blockchain technology, fingerprint recognition, OTP authentication, and facial recognition have been the subject of numerous studies. These methods have increased voter authentication and system effectiveness, but they have a number of drawbacks. While OTP-based systems typically rely on online SMS or email services, which limits their use in places with inconsistent internet connectivity, facial recognition-based systems frequently rely on single-factor authentication, making them susceptible to spoofing attacks using photos or recorded videos. While some sophisticated solutions emphasize data integrity, their practical deployment is limited by their high processing power or expensive infrastructure requirements. In order to guarantee safe, dependable, and accessible electronic voting without constant network connectivity, there is a research gap in the lack of a unified and affordable voting system that incorporates facial recognition, liveness detection, and offline-capable OTP authentication.

7. Proposed System and Advantages

Using biometric authentication, the suggested Smart Voting System Through Face Recognition is intended to offer a quick and safe voting procedure. The system eliminates the need for conventional manual identification techniques by taking a live picture of the voter's face during the voting session and comparing it with securely stored facial data to confirm the voter's eligibility.

Liveness detection, which uses natural facial movements like eye blinking and head rotation to confirm the presence of a legitimate voter, is incorporated into the authentication process to improve system reliability. This real-time verification greatly lowers identity fraud and successfully stops spoofing attempts using printed photos or recorded videos, enhancing the voting system's overall security.

The system uses One-Time Password (OTP) verification as part of a multi-level security strategy in addition to facial recognition. In order to ensure functionality in low or no network conditions, a time-bound OTP is generated following successful biometric authentication and can be verified even in offline mode. The suggested framework is a workable and dependable solution for contemporary voting systems since it minimizes manual supervision, avoids duplicate voting, permits quicker authentication, and guarantees secure vote recording.

8. Methodology

The put forth system we have designed is a structured solution for secure and accurate voter authentication. Our method is a multi step process that begins with voter enrolment and which also includes secure vote recording at the end. At each step we have included measures which are meant to reduce errors, to also include prevention of fraud and the which also protected voter privacy.

8.1 Voter Registration

In the registration phase we collect voter info which includes identification details as well as what we have which are several facial images of the voter captured in various settings. Those images are put through a process which extracts out unique features from the face which in turn are converted into numerical feature vectors which we call face encodings. We then put these encodings through an encryption process before we store them in the database to at the same time guarantee data confidentiality and to also prevent against unauthorized access.

8.2 Face Detection and Recognition

As the voting occurs, the system records the voting activity through a camera and captures video streams in real-time. To determine whether a face exists and where that face is located, face detection methodologies are employed on the video streams. When a face is located, the facial region is cropped and relevant features are captured through facial recognition. These features are used to determine the polarity of a match with the stored facial encodings of the facial features to determine who the voter is.

8.3 Liveness Detection

Since there may be attempts to fool the system, the authentication process has a step for liveness detection. The system checks for the existence of certain facial dynamics, such as slight head movement or blinking, which help to ensure a real person is supplying the input. If the system assigns a negative authentication to liveness, the system will end the authentication process immediately to safeguard against system breaches.

8.4 OTP Authentication and Voting

After we have successful face recognition and live scan of the individual's identity another authentication feature comes in through the use of a One Time Password (OTP). We have implemented both on and off line features for the OTP to report out that the system is reliable even when not connected to a network. Once the OTP is inputted correctly the person is given the go ahead to cast their vote. The vote is put into the database securely and at the same time the voter's status is updated to stop against repeat voting. Also results are made available to admin users as they are counted out.

8.5 Process Flow Diagram

The process flow diagram illustrates the secure workflow of the proposed Smart Voting System. The system performs facial recognition and liveness detection to authenticate the voter. A time-based OTP is then validated to ensure multi-level security. After duplicate checks, the vote is encrypted and securely stored to maintain integrity and one-person-one-vote enforcement.

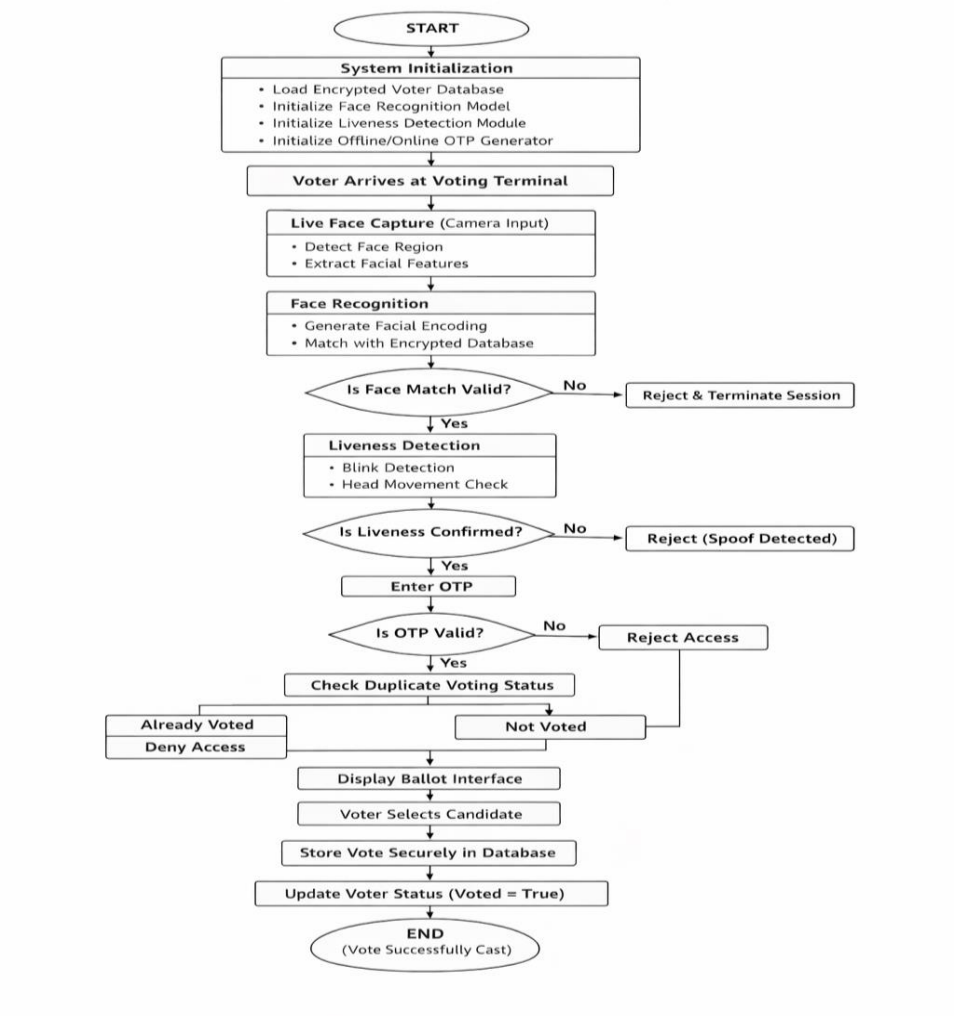

Fig: Process Flow Diagram of Proposed Smart Voting System

8.6 Algorithms Used in the Proposed System

8.6.1 HOG (Histogram of Oriented Gradients) – Face Detection Algorithm

Input: Live Vedio Frame

Output: Face bounding box coordinates

Algorithm Steps:

1. Capture video frame from camera.
2. Convert image to grayscale.
3. Divide image into small cells (8×8 pixels).
4. Compute gradient magnitude and orientation for each pixel.
5. Create histogram of gradient directions for each cell.
6. Normalize histograms over blocks.
7. Pass feature vector to trained classifier.
8. Detect and return face region coordinates.

8.6.2 Deep Learning 128-D Face Embedding Algorithm – Face Recognition

Input: Detected face image

Output: 128-dimensional feature vector

Algorithm Steps:

1. Detect face from image.
2. Align and preprocess the face.
3. Resize image to model input size.
4. Pass image into pre-trained deep learning model.
5. Extract 128-dimensional embedding vector.
6. Store or compare embedding for verification.

8.6.3 Euclidean Distance Algorithm – Face Matching

Input: Live face embedding & stored embedding

Output: Match / No Match

Formula:

$$Distance = \sqrt{\sum_{i=1}^{128} (x_i - y_i)^2}$$

Algorithm Steps:

1. Take embedding of live captured face.
2. Retrieve stored voter embedding from database.
3. Compute Euclidean distance between both vectors.
4. Compare distance with predefined threshold.
   - If Distance < Threshold → Identity Verified
   - Else → Authentication Rejected

8.6.4 Other Supporting Algorithms Used

Apart from the main 3 core algorithms, the system also uses:

- **Facial Landmark Detection** – To detect eye coordinates
- **Aspect Ratio (EAR) Algorithm** – For liveness detection (blink detection)
- **OTP Generation & Validation Algorithm** – For second-layer authentication
- **Database Constraint Logic** – To prevent duplicate voting

9. Technologies Used

The proposed Smart Voting System is implemented using Python as the primary programming language due to its extensive support for computer vision and machine learning applications. The backend of the system is developed using the Flask web framework, which manages routing, authentication workflows,

and communication between the user interface and server-side components. OpenCV is employed for real-time video capture, face detection, and image preprocessing operations. The face_recognition library, built upon Dlib's deep learning models, is utilized to generate 128-dimensional facial embeddings for precise voter identification. NumPy is used for efficient numerical computations, particularly for performing similarity comparisons between facial encodings using distance-based metrics.

For secure authentication, a One-Time Password (OTP) mechanism is implemented using secure random generation with time-bound validation. The system supports both online and offline OTP verification to ensure functionality in environments with limited or unstable network connectivity. Voter details and voting records are securely stored in relational databases such as MySQL, while additional metadata and system logs can be maintained using MongoDB. Proper session management mechanisms are implemented to maintain authentication integrity and structured data handling suitable for institutional-level deployment.

10. Results and Discussion

When compared to conventional voting techniques, the analysis of the suggested Smart Voting System suggests that it may offer better security and dependability. Facial recognition technology is used to verify voter registration and is anticipated to drastically lower identity theft and illegal voting. Furthermore, liveness detection is used to detect and stop attempts to spoof images or recorded videos.

Voting operations can be carried out even in the absence of internet connectivity thanks to the system's support for offline One-Time Password (OTP) verification. Because of this feature, the proposed system can be deployed in remote and rural areas with limited network availability, guaranteeing voting process accessibility and continuity.

A qualitative and analytical evaluation was carried out based on system architecture, algorithmic capabilities, and observations reported in related studies because the system has not yet been fully implemented. The following is a summary of the anticipated performance attributes of the suggested system.

The proposed system is anticipated that the automated vote collection and result computation supported by the suggested system architecture will lessen manual labour and human error during vote counting. The system preserves election integrity and transparency by guaranteeing that each voter is only permitted to cast one ballot. All things considered, the analytical results indicate that the suggested method provides a safe, quick, and dependable framework for electronic voting.

11. Outcomes

The suggested smart voting system is expected to produce the following results:

- A scalable and reasonably priced voting solution appropriate for both urban and rural areas
- A notable decrease in voter impersonation, spoofing attacks, and duplicate voting
- Faster voter verification and shorter election wait times

- A decrease in manual labour and human error in vote verification and counting

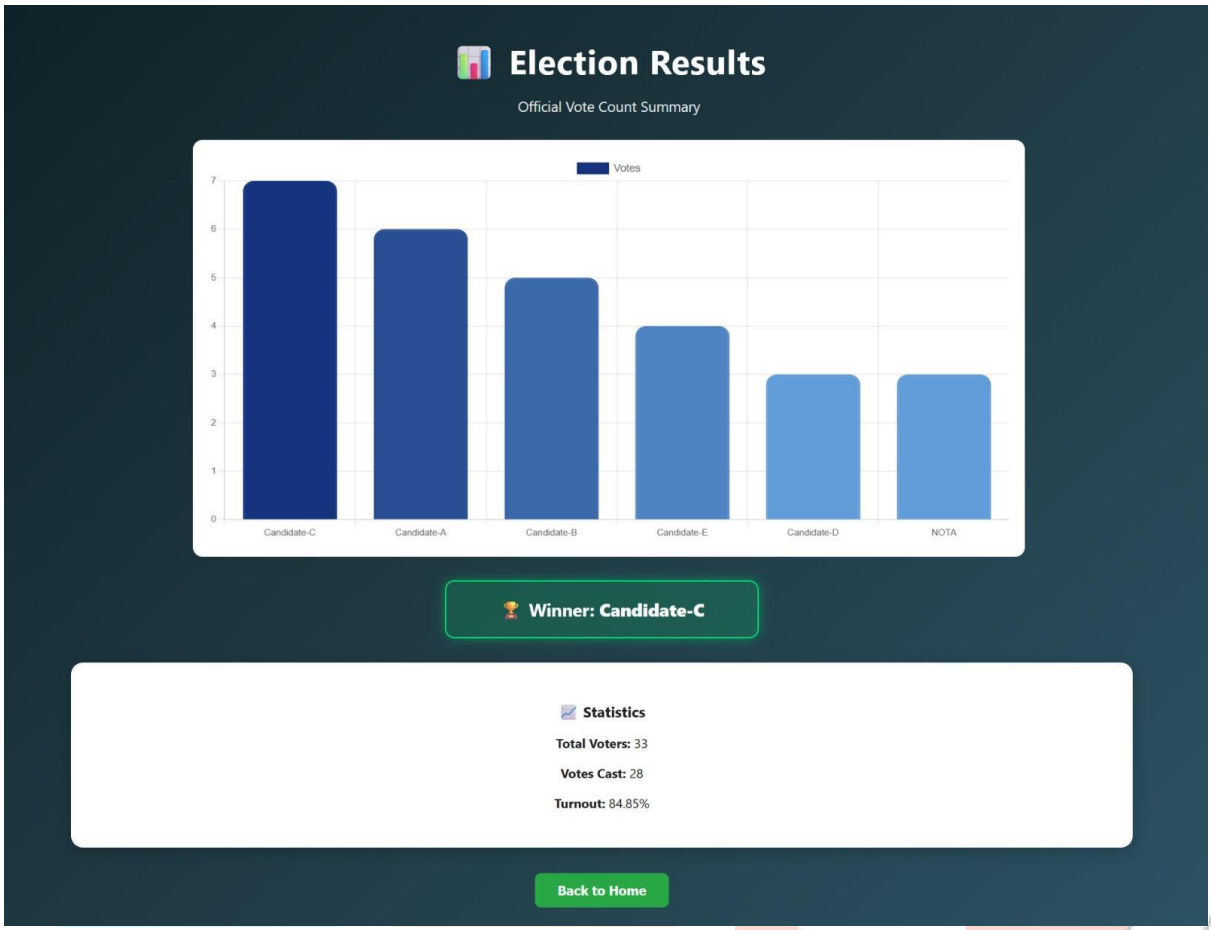

Fig 2: Election Results Dashboard

12. Conclusion

The Smart Voting System Through Face Recognition enhances the security and trustworthiness of the voting process through biometric-based authentication. By integrating facial recognition, liveness detection, and OTP-based verification, the proposed system addresses several limitations of conventional voting methods.

The system is designed to improve operational efficiency, reduce fraudulent activities, and support voting operations in environments with limited or no network connectivity. Furthermore, the modular architecture of the system allows for future enhancements and adaptability to evolving technological and security requirements. Overall, the proposed system represents a promising and effective solution for addressing the challenges associated with modern electronic voting.

13. References

[1]. A. Yadu and O. P. Chandrakar, "A Smart Voting System Combining Fingerprint and Facial Recognition for Enhanced Security", *ShodhKosh: Journal of Visual and Performing Arts*, Vol. 5, No. 1, 2024, pp. 362–366.

[2]. K. Yatheendra, R. S. Kumar, and P. V. Reddy, "E-Voting System with Face Recognition", *International Journal of Information Technology and Computer Engineering*, Vol. 12, No. 3, 2024, pp. 608–619.

[3]. S. Gunthe, R. Patil, and A. Deshpande, "Online Voting System Using Face Recognition and OTP", *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, Vol. 11, No. 6, 2023, pp. 535–540.

[4]. R. Vaikunta Rao, K. S. Reddy, and P. Anil Kumar, "Face Recognition Using Eigenface Algorithm to Support Smart Voting", *Journal of Advanced Zoology*, Vol. 44, Special Issue 2, 2023, pp. 1012–1018.

[5]. N. Abd Hamid, C. D. Nair Appunair, and A. F. A. Abidin, "A Secure Online Voting System Using Face Recognition Technology", *Malaysian Journal of Computing and Applied Mathematics*, Vol. 6, No. 1, 2023, pp. 1–9.

[6]. D. Sreekanth, D. Nishitha, A. Yashwanth Kumar, A. Sudeep Rao, and A. Sindhu, "E-Voting System Using Facial Recognition", *The International Journal of Analytical and Experimental Modal Analysis*, Vol. XIV, June 2023, pp. 1191–1201.

[7]. P. Viola and M. Jones, "Rapid Object Detection Using a Boosted Cascade of Simple Features", *IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, 2001, pp. 511–518.

[8]. I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.

[9]. S. Marcel and S. Bengio, "Improving Biometric Security Using Liveness Detection", *IEEE Signal Processing Magazine*, Vol. 26, No. 5, 2009, pp. 25–36.

[10]. Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of Face Recognition Systems Under Spoofing Attacks", *IEEE Transactions on Information Forensics and Security*, Vol. 9, No. 12, 2014, pp. 2264–2276.

[11]. 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, 2004, pp. 4–20.

[12]. Y. Li, K. Zhao, and X. Wang, "Face Anti-Spoofing Based on Motion and Texture Analysis", *International Journal of Computer Applications*, Vol. 179, No. 18, 2018, pp. 1–6.

[13]. R. Mercuri, "Electronic Vote Tabulation Checks and Balances", *PhD Dissertation*, University of Pennsylvania, 2001.

[14]. M. Bishop, *Computer Security: Art and Science*, Addison-Wesley, 2018.

[15]. A. Juels, D. Catalano, and M. Jakobsson, "Coercion-Resistant Electronic Elections", *ACM Workshop on Privacy in the Electronic Society*, 2005, pp. 61–70.