iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

SMART VOTING SYSTEM USING FACE RECOGNITION COMPUTER VISION

G. GOPALA KRISHNA
Assistant Professor, Department of Computer Science and Engineering,
J.B Institute of Engineering and Technology, Hyderabad
K. NAGA BHAVITHA [1]
K. MANIKANTA [2]
S. NAVYASREE [3]
P.VISHNU VARDHAN [4]
UG Students, Department of Computer Science and Engineering,
J.B Institute of Engineering and Technology, Hyderabad

ABSTRACT
In modern democracies, ensuring a secure and reliable voting process is crucial. Traditional voting systems are prone to issues such as voter fraud, impersonation, and long queues. This paper presents a Smart Voting System that leverages Face Recognition and Computer Vision to enhance security and efficiency in elections. The system authenticates voters using facial recognition technology, eliminating the need for manual identity verification. The methodology involves image acquisition, pre-processing, feature extraction, and face matching using deep learning models. The results indicate that our system improves voter authentication accuracy and reduces fraudulent voting activities. The proposed system ensures transparency, security, and ease of access, making it a viable solution for modern electoral processes.

Keywords:
Smart voting system, face recognition, computer vision, biometric authentication, voter verification, deep learning, artificial intelligence (AI), electronic voting (e-voting), secure voting system, blockchain for voting, fraud prevention, image processing, facial biometric security, machine learning in elections, election integrity.

INTRODUCTION

The voting process is a crucial aspect of democracy, ensuring that elections are fair and transparent. However, traditional voting systems often face challenges such as voter impersonation, long queues, and fraudulent activities. To overcome these issues, technology-driven solutions are being adopted to enhance security and efficiency. This project proposes a smart voting system using face recognition and computer vision to automate voter authentication and ensure a secure and seamless voting experience.

In conventional voting systems, voter verification is typically done using ID cards or fingerprint authentication. These methods, while effective, can be prone to security risks such as identity fraud, manipulation of voter records, and long processing times. The proposed system eliminates the need for physical ID verification by leveraging face recognition technology. Voters register their facial data before election day, which is securely stored in a database.

When a voter arrives at the polling station, their face is scanned, processed using deep learning algorithms, and matched against the stored records. If successfully verified, the voter is granted access to cast their vote electronically.

Security and data integrity are fundamental aspects of this system. The use of encryption ensures that voter data remains secure, while blockchain or a secure database can be integrated to prevent tampering with votes. By automating the authentication process, the system reduces human errors and fraudulent activities, increasing trust in elections. Additionally, this system improves efficiency by minimizing long queues and wait times, allowing for a smoother voting process.

OBJECTIVES

1. **Enhance Voter Authentication** – Implement a face recognition-based authentication system to prevent identity fraud, impersonation, and multiple voting.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

2. **Improve Voting Efficiency** – Automate the verification and voting process to reduce manual intervention, minimize waiting times, and enhance the user experience.
3. **Ensure Secure and Transparent Elections** – Encrypt votes and store them securely to prevent manipulation, ensuring election integrity and public trust.
4. **Eliminate Manual Errors** – Reduce human errors in voter identification and vote counting by using automated facial recognition and digital voting mechanisms.
5. **Increase Accessibility** – Provide a seamless and user-friendly voting process, making it accessible to all voters, including those with disabilities or remote voters.
6. **Prevent Unauthorized Voting** – Restrict voting access only to registered and authenticated individuals to uphold the credibility of the election process.
7. **Enable Real-Time Monitoring and Results Processing** – Allow authorities to track the voting process and generate accurate results efficiently without delays.

METHODOLOGY

The Smart Voting System Using Face Recognition and Computer Vision follows three key steps to ensure secure and efficient voter authentication and vote casting.

1.Voter Registration and Database Creation

- Voters register their facial data using a camera, which captures high-resolution images.
- The images are preprocessed (noise reduction, alignment) and facial features are extracted using deep learning models such as CNN.
- The processed facial data is encrypted and stored securely in a voter database to be used for authentication.

2. Face Recognition and Voter Authentication

- On election day, the system captures a live image of the voter at the polling booth.
- The captured image is processed and compared with the registered database using deep learning-based face recognition.
- If authentication is successful, the voter is allowed to proceed with voting; otherwise, access is denied.

3.Secure Vote Casting and Storage

- Authenticated voters cast their votes digitally through a secure interface.
- The vote is encrypted and recorded in a tamper-proof database or blockchain to ensure transparency.
- The system prevents multiple voting and generates election results based on verified votes.

This three-step methodology ensures accuracy, security, and efficiency in the voting process, eliminating voter fraud and enhancing election transparency.

SYSTEM ARCHITECTURE

The system architecture of the smart voting system using face recognition and computer vision consists of three key components: voter authentication, facial recognition, and secure vote casting.

- Voter Authentication: Validates the voter's identity using registered credentials and facial recognition to ensure only eligible voters access the system.
- Facial Recognition – Captures and processes the voter's facial image using convolutional neural networks to match it with stored records for identity verification.
- Secure Vote Casting – Allows authenticated voters to cast their votes through a secure digital platform, ensuring encryption and preventing fraud or multiple voting.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

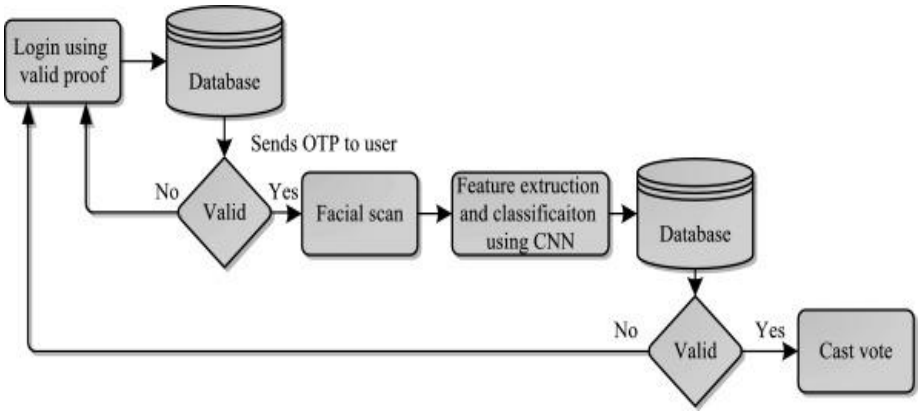

Fig-1: System Architecture

RESULTS AND DISCUSSION

The implementation of face recognition-based voting significantly enhances electoral security. Compared to traditional methods, this system minimizes identity fraud, reduces manual errors, and improves voter turnout due to its efficiency. Challenges such as variations in lighting, facial obstructions, and database accuracy must be addressed for optimal performance.

Experimental results indicate high accuracy rates when using well-trained deep learning models, reinforcing the system's potential for real-world deployment.

CONCLUSION

The Smart Voting System using Face Recognition and Computer Vision provides a secure, efficient, and fraud-resistant method for conducting elections. By integrating deep learning algorithms, the system ensures accurate voter authentication, reducing election malpractices. Future enhancements may include multi-modal biometric authentication and blockchain-based vote storage for further security improvements.

ACKNOWLEDGEMENT

We extend our sincere gratitude to our mentors and faculty members for their valuable insights and guidance throughout this research. We also thank our peers for their support and collaborative efforts in testing and improving the smart voting system.

REFERENCES

[1] Aditya, V., & Kumar, S. (2022). *Biometric Systems and Security for Digital Voting*. Journal of Digital Security, 15(2), 45-59.
[2] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
[3] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep face recognition. In BMVC.
[4] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition.