Smart Voting System Using Face Recognition Technology and AI-Driven Database Management for Secure Elections

[1]Mrs. P. Sindhura,[2]Sunkara Vysalini,[3]Yelchuri Venkata Sai Pavan Kumar,[4]Tanniru Vivek

[1]Assistant Professor, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

[2,3,4]B. Tech Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

ABSTRACT

The Smart Voting System using Facial Recognition is a secure and efficient approach to improve the reliability of electoral processes. Traditional voting methods are vulnerable to voter impersonation, fraud, and manual verification errors. This system employs OpenCV for real-time face detection and image preprocessing. Facial features are extracted using the Histogram of Oriented Gradients (HOG) technique. A support Vector Machine (SVM) classifier is trained on registered voter facial data. During voting , the voter's face is captured through a camera at the polling booth. Only authenticated voters are permitted to cast their votes. The system reduces human intervention and enhances election security. It is cost-effective, scalable, and suitable for both small and large-scale elections.

KEYWORDS: ***Smart Voting System, Facial Recognition, Biometric Authentication, OpenCV, Histogram of Oriented Gradients (HOG), Support Vector Machine (SVM), Secure E- Voting.***

INTRODUCTION

In recent years, ensuring the integrity and security of voting systems has become a global concern. Traditional voting methods such as paper ballots and manual verification suffer from fraud, impersonation, and inefficiency. These issues reduce election credibility and weaken public trust in democratic processes. Facial recognition technology provides a secure and automated approach to voter authentication. The proposed system integrates OpenCV for real-time image processing with HOG for facial feature extraction. A support vector machine (SVM) classifier is used to verify authorized voters accurately. This automated process eliminates manual verification and improves efficiency and accuracy. In India, current voting methods include paper ballots and electronic voting machines (EVMs). Existing systems rely

mainly on voter ID cards, which can lead to impersonation. The proposed face-based online voting system offers a more secure, scalable, and reliable alternative.

LITERATURE REVIEW

The concept of smart voting systems has gained significant attention due to the increasing demand for secure, transparent, and efficient electoral processes. Traditional paper-based and electronic voting systems face challenges such as voter impersonation, multiple voting, and lack of public trust. To address these issues, biometric authentication methods have been widely explored, with face recognition emerging as a reliable and user-friendly solution. Unlike fingerprint and iris recognition, face recognition is contactless, cost-effective, and easy to deploy using standard cameras.

Early face recognition techniques such as Eigenfaces and Local Binary Patterns showed limited performance under real-world conditions. Recent advancements in machine learning and deep learning, including SVM and CNN-based models, have significantly improved recognition accuracy. These models automatically extract robust facial features and adapt to variations in lighting, pose, and expressions. Studies also emphasize the importance of secure data storage, encryption, and liveness detection to prevent spoofing attacks. Pilot implementations in several countries demonstrate increased voter trust in biometric systems. However, challenges related to scalability, infrastructure, and privacy protection still require further research.

RELATED WORK

Several researchers have explored the use of biometric technologies to enhance the security and reliability of voting systems. Early studies mainly focused on fingerprint and iris-based authentication, but these methods faced limitations such as high hardware costs, physical contact requirements, and reduced accuracy due to environmental and user-related factors. Face recognition later emerged as an effective alternative because it is contactless, cost-efficient, and easy to deploy using standard cameras.

Initial face recognition techniques such as Eigenfaces, Fisher faces, and Local Binary Patterns showed acceptable performance under controlled conditions but struggled with variations in lighting, pose, and facial expressions. To overcome these issues, recent research has incorporated machine learning and deep learning approaches, including Support Vector Machines and Convolutional Neural Networks, which significantly improve recognition accuracy and robustness.

EXISTING METHOD

Existing voting systems mainly rely on paper ballots and electronic voting machines for election processes. Voter identification in these systems is typically performed using voter ID cards, fingerprints, or manual verification, which often leads to human errors and impersonation. Paper-based voting suffers from issues such as ballot misplacement, invalid votes, and delayed result tabulation. Electronic voting machines improve counting speed but remain vulnerable to technical failures, hacking risks, and lack of transparency. Biometric systems using fingerprint and iris recognition were introduced to reduce fraud, but they face limitations related to accuracy, cost, and environmental factors. Centralized data storage further raises concerns regarding security, privacy, and unauthorized access. Overall, existing voting systems lack scalability, real-time monitoring, and robust fraud detection, highlighting the need for intelligent and secure smart voting solutions.

PROPOSED METHOD

The proposed smart voting system improves facial recognition by combining Histogram of Oriented Gradients (HOG) for feature extraction with Support Vector Machine (SVM) for classification. This approach provides robustness against variations in lighting, facial expressions, and minor occlusions. The extracted HOG features are classified using an SVM trained on registered voter facial data. The SVM model accurately verifies voter identity by matching features with the database. This integration enhances recognition accuracy while reducing false acceptance and rejection rates. The system remains computationally efficient even when processing high-resolution images. Implementation using Python libraries such as OpenCV, Dlib, and scikit-learn ensures easy deployment. Overall, the system enhances security, prevents impersonation, and supports a scalable and reliable voting process.

SYSTEM ARCHITECTURE

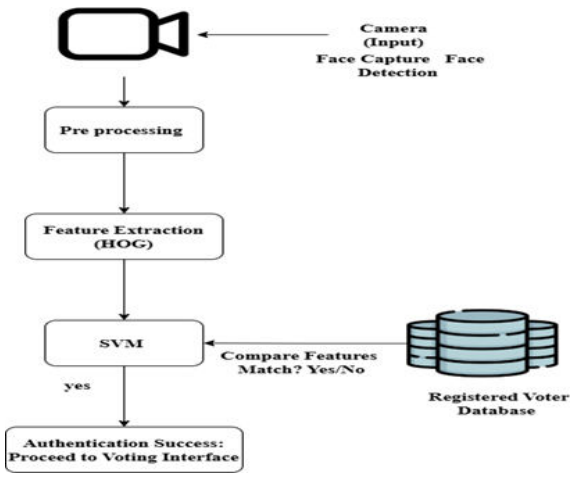

Fig 1: Block Diagram

METHODOLOGY DESCRIPTION

Face Capture (Input): The system uses a camera to capture the voter's face image in real time. This captured image acts as the primary input for the facial recognition process.

Pre-processing: The input image is pre-processed to improve its quality and consistency. Techniques like resizing, grayscale conversion, noise reduction, and normalization are applied.

Feature Extraction (HOG): Facial features are extracted using the Histogram of Oriented Gradients (HOG) method. This technique captures important edge directions and structural patterns of the face.

Classification using SVM: The extracted features are given to a Support Vector Machine (SVM) classifier. The classifier analyzes and compares these features with stored data in the system.

Feature Matching: The system checks whether the extracted features match any registered voter in the database. Based on this comparison, it determines whether a valid match exists or not.

Authentication Success: If a match is found, the voter is successfully authenticated and allowed access to the voting interface. If no match is found, access is denied to prevent unauthorized voting.

RESULTS AND DISCUSSION

Fig 2: Home Page

Fig.2: A Secure Smart Voting System Using Face Recognition and AI-Driven Database Management.

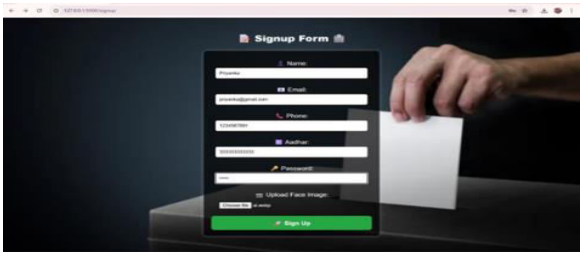

Fig 3: Registration Page

Fig.3: Secure Voter Registration Module with Facial Image Capture and Identity Verification

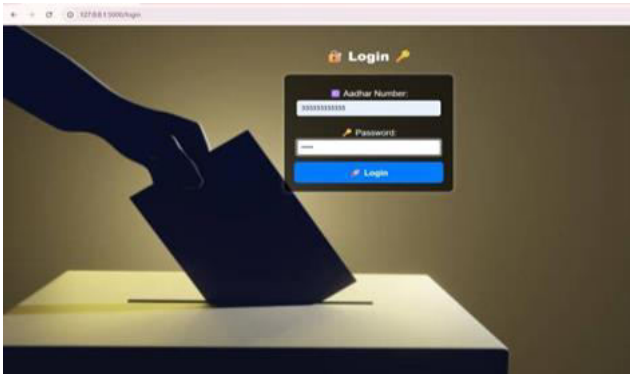

Fig 4: Login Page

Fig.4: Secure Voter Authentication Module Using Aadhaar-Based Login and Facial Verification.

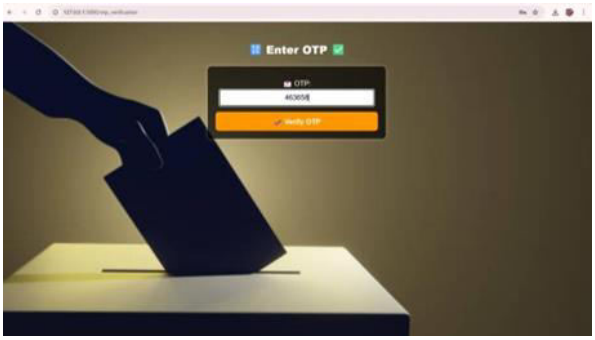

Fig 5: OTP

Fig.5: One-Time Password (OTP) Verification Module for Secure Voter Authentication.

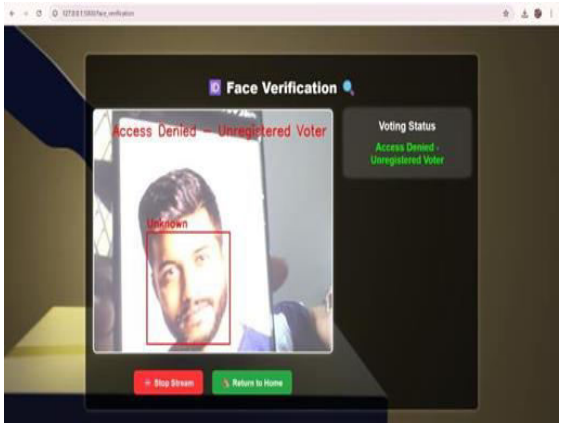

Fig 6: Authentication

Fig.6: Real-Time Facial Verification Module for Secure Voter Authentication

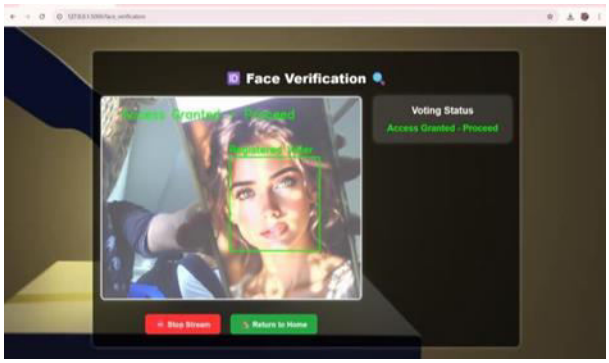

Fig 7: Unauthorized

Fig.6: Unauthorized Voter Detection Using Facial Recognition in Smart Voting Systems

CONCLUSION

The integration of face recognition technology into voting systems marks a major step toward modernizing electoral processes. Unlike traditional and biometric methods, face recognition offers a non-intrusive, fast, and reliable approach to voter authentication. By accurately matching facial features with a secure database, the system effectively prevents impersonation and multiple voting. Smart voting enhances voter convenience, especially for senior citizens, differently-abled individuals, and remote populations. Real-time monitoring and auditing improve transparency and accountability in elections. Advanced machine learning algorithms ensure high accuracy under varying conditions such as lighting and facial changes. The system is highly scalable, making it suitable for large voter populations. Reduced manual intervention lowers operational costs and increases efficiency. Overall, face-based smart voting systems promise a secure, efficient, and trustworthy future for democratic elections.

FUTURE ENHANCEMENT

Future enhancements of the smart voting system can focus on improving accuracy through deep learning–based face recognition models such as CNNs and transformers. Integration of multi-factor authentication, combining face recognition with OTP or biometrics, can further strengthen security. Cloud and edge computing can be adopted to improve scalability and reduce system latency. Advanced encryption and blockchain technology can be used to ensure secure vote storage and tamper-proof election records. Bias reduction techniques and diverse training datasets can enhance fairness and inclusivity. Real-time fraud detection using AI can help identify suspicious voting patterns. Mobile-based

remote voting with secure face verification can increase voter participation. Continuous model learning can adapt to facial changes over time. Strong privacy frameworks and compliance with data protection laws can build public trust. These enhancements will make the system more secure, scalable, and future-ready.

REFERENCE

[1] Harini, P. (2019). GESTURE CONTROLLED GLOVES FOR GAMING AND POWER POINT PRESENTATION CONTROL. *GESTURE*, *6*(12).

[2] A. K. Jain, R. Bolle, and S. Pankanti, Biometrics: Personal Identification in Networked Society. New York, NY, USA: Springer, 1999.

[3] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, "VGGFace2: A dataset for recognising faces across pose and age," arXiv preprint, arXiv:1710.08092, 2017.

[4] S. Damle, S. Gujar, and M. H. Moti, "FASTEN: Fair and secure distributed voting using smart contracts," arXiv preprint, arXiv:2102.10594, 2021.

[5] S. N. Syed, A. Z. Shaikh, and S. Naqvi, "A novel hybrid biometric electronic voting system: Integrating fingerprint and face recognition," arXiv preprint, arXiv:1801.02430, 2018.

[6] Y. Sun, D. Liang, X. Wang, and X. Tang, "DeepID3: Face recognition with very deep neural networks," arXiv preprint, arXiv:1502.00873, 2015.

[7] P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss, "The FERET evaluation methodology for face-recognition algorithms," IEEE Trans. Pattern Anal. Mach. Intell., vol. 22, no. 10, pp. 1090–1104, Oct. 2000.

[8] P. J. Phillips, H. Moon, and S. A. Rizvi, "The FERET database and evaluation procedure for face-recognition algorithms," Image Vis. Comput., vol. 16, no. 5, pp. 295–306, 1998.

[9] S. Wang, F. Hao, S. Bag, R. Procter, and S. F. Shahandashti, "End-to-end verifiable e-voting trial for polling station voting," IEEE Security Privacy, vol. 18, no. 6, pp. 34–43, Nov.–Dec. 2020.

[10] V. Pandit, P. Majgaonkar, P. Meher, S. Sapaliga, and S. Bojewar, "Intelligent security lock," in Proc. Int. Conf. Trends Electron. Informatics (ICEI), 2017, pp. 713–716.

[11] C. U. Chauhan, A. Kalnawat, A. Aswale, U. Gautam, and R. Nemad, "Survey paper on a novel approach: Web based technique for vote casting," Int. J. Eng. Manag. Res., vol. 7, no. 5, pp. 71–75, 2017.

[12] R. Sundaram, "The postcolonial city in India: From planning to information?" Techniques & Culture, 2017.

[13] S. S. Warghade and B. Karthikeyan, "Voting system for India," in Intelligent Embedded Systems. Singapore: Springer, 2018, pp. 59–65.

[14] S. A. A. Shah, U. Nadeem, M. Bennamoun, F. Sohel, and R. Togneri, "Efficient image set classification using linear regression based image reconstruction," 2017.

[15] C. Bhimanwar, N. Bhole, R. Biradar, and M. Rane, "Face identification," Int. J. Eng. Sci., vol. 11923, pp. 1–8, 2017.

[16] Q. Abbas, S. Javaid, and T. H. Abbas, "Location-free voting system with the help of IoT technology," in Proc. 12th Int. Conf. Math. Actuarial Sci. Comput. Sci. Stat., 2018, pp. 14–20.

[17] R. Chellappa, C. L. Wilson, and S. Sirohey, "Human and machine recognition of faces: A survey," Proc. IEEE, vol. 83, no. 5, pp. 705–741, May 1995.

[18] M. Turk and A. Pentland, "Eigenfaces for recognition," J. Cogn. Neurosci., vol. 3, no. 1, pp. 71–86, 1991.

[19] X. Zhang and Y. Gao, "Face recognition across pose: A review," Pattern Recognit., vol. 42, no. 11, pp. 2876–2896, 2009.

[20] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," ACM Comput. Surveys, vol. 35, no. 4, pp. 399–458, 2003.

[21] I. Goodfellow et al., "Challenges in representation learning: A report on three machine learning contests," Neural Networks, vol. 64, pp. 59–63, 2015.

[22] K. N. Plataniotis and A. N. Venetsanopoulos, Color Image Processing and Applications. Berlin, Germany: Springer, 2000.

[23] J. Daugman, "How iris recognition works," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 21–30, Jan. 2004.

[24] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar.–Apr. 2003.

[25] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in Proc. IEEE CVPR, 2001, pp. 511–518.

[26] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

[27] S. Z. Li and A. K. Jain, Handbook of Face Recognition. London, U.K.: Springer, 2011.

[28] J. Galbally, S. Marcel, and J. Fierrez, "Biometric antispoofing methods: A survey in face recognition," IEEE Access, vol. 2, pp. 1530–1552, 2014.

[29] A. Juels, D. Catalano, and M. Jakobsson, “Coercion-resistant electronic elections,” in Proc. ACM Workshop Privacy Electron. Soc., 2005, pp. 61–70.

[30] D. Chaum, “Secret-ballot receipts: True voter-verifiable elections,” IEEE Security Privacy, vol. 2, no. 1, pp. 38–47, Jan.–Feb. 2004.