IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SMART VOTING SYSTEM THROUGH FACIAL RECOGNITION USING OPENCV

S. Bhargavi[1], G. Srinivasa Rao[2], P. Bhagya Sree[3], P. Santoshi[4], P. Lakshmi Sowmya[5]

[1]Assistant Professor, Department of Electronics and Communication Engineering, Bapatla Women's Engineering College, Bapatla 522101

[2] Professor, Department of Electronics and Communication Engineering, Bapatla Women's Engineering College, Bapatla 522101

[3, 4,5] U.G Students, Department of Electronics and Communication Engineering, Bapatla Women's Engineering College, Bapatla 522101

Abstract: The Smart Voting System through Facial Recognition using OpenCV and Support Vector Machine (SVM) with Histogram of Oriented Gradients (HOG) is an advanced, secure, and efficient voting mechanism designed to enhance the accuracy and reliability of electoral systems. Traditional voting systems are prone to issues such as voter impersonation, voter fraud, and inefficiencies in the verification process. This system utilizes facial recognition technology to address these challenges by ensuring that only eligible voters can cast their votes. The proposed system leverages OpenCV for real-time image processing and feature extraction, with HOG being used for identifying facial features. The facial features are then classified using a Support Vector Machine (SVM) model, trained to differentiate between authorized voters and unauthorized individuals. The SVM classifier is trained on facial data, enabling it to achieve high accuracy and robustness in diverse conditions, such as different lighting or angles of faces. The process begins by capturing the voter's face through a webcam or camera at the voting booth. The facial image is then pre-processed, and HOG descriptors are extracted to capture the shape and structure of the face. The descriptors are subsequently input to the SVM classifier, which compares the facial features with a pre-registered database of authorized voters. If the system matches the captured face with the database, the voter is granted permission to vote. This innovative approach improves the efficiency of the voting process, reduces human error, and significantly increases security by preventing fraud or impersonation. Additionally, the system is cost-effective and scalable, making it a viable solution for both small-scale and large-scale elections.

Index Terms: **Support Vector Machine (SVM), Histogram of Oriented Gradients (HOG), OpenCV, Voter Authentication**

I. INTRODUCTION

In recent years, the integrity and security of voting systems have become major concerns worldwide. Traditional voting methods, such as paper ballots and manual verification, are prone to various issues, including voter fraud, impersonation, and inefficiencies in the authentication process. These challenges compromise the credibility of elections and undermine public trust in democratic processes. As technology advances, there is a growing need for more secure, accurate, and efficient voting mechanisms. One promising solution is the integration of facial recognition technology into the voting system. Facial recognition, particularly when combined with machine learning techniques like Support Vector Machine (SVM) and image processing tools like OpenCV, offers a novel approach to voter identification. By using facial features as a biometric trait, this system can ensure that only registered individuals are allowed to vote, significantly reducing the risk of identity fraud and increasing the overall security of the electoral process. The system proposed in this work employs OpenCV for real-time image processing and the extraction of facial features using Histogram of Oriented Gradients (HOG). HOG is a feature descriptor that is particularly effective in detecting objects such as faces by capturing edge and gradient information. These features are then fed into an SVM classifier, which is trained to distinguish between authorized and unauthorized individuals based on their facial characteristics. By automating voter authentication through facial recognition, this smart voting system eliminates the need for manual verification, enhancing both efficiency and accuracy in the election process. It provides a more secure alternative to traditional methods by reducing the possibility of human error or fraudulent activities, such as voter impersonation. Additionally, the system's adaptability to various environmental conditions (e.g., lighting changes, different angles of faces) ensures that it is reliable across diverse voting settings. This paper explores the design, development, and implementation of such a system, focusing on how facial recognition can revolutionize the voting process by making it more secure, efficient, and trustworthy. Through the integration of OpenCV, SVM, and HOG, this solution has the potential to transform the way elections are conducted globally, offering a scalable and cost-effective alternative to traditional voting systems.

II. PROBLEM STATEMENT

Conventional voting systems often face critical challenges including voter impersonation, lengthy verification processes, human error, and vulnerability to fraud. Biometric approaches such as fingerprint or iris recognition, while effective, require physical contact or specialized hardware, which may limit scalability and hygiene particularly in high-density populations. Facial recognition offers a non-intrusive alternative, yet traditional facial recognition systems often struggle with varying lighting conditions, facial orientations, and real-time performance demands. Therefore, there is a pressing need for an accurate, contactless, and efficient voter verification method. This paper addresses this gap by proposing a smart voting system that integrates Histogram of Oriented Gradients (HOG) for robust facial feature extraction and Support Vector Machine (SVM) for precise classification. The goal is to enhance the security, speed, and reliability of the voter authentication process in electronic voting systems.

III. OBJECTIVES

To design and develop an intelligent system capable of executing the following core functionalities with precision and reliability

- Secure Voter Authentication: Utilize facial recognition through HOG and SVM to accurately verify voter identities. This prevents impersonation and ensures only eligible individuals cast votes.
- Enhance Voting Efficiency: Automate the identification process to reduce manual checks and long queues. The system speeds up voter processing, especially in high-traffic areas.
- Prevent Electoral Fraud: Ensure each voter is uniquely recognized, eliminating chances of duplicate or false voting. This strengthens the integrity and fairness of elections.
- Promote Contactless Verification: Enable a hygienic, touch-free authentication process, suitable for health-conscious environments. This modernizes the voting experience while ensuring safety.

IV. EXPECTED OUTCOME

This Smart Voting System using facial recognition with HOG and SVM aims to provide a secure, contactless, and accurate voter authentication method. It minimizes impersonation and fraud by extracting key facial features and classifying them efficiently. The system is designed for real-time performance with low false acceptance and rejection rates. It also ensures scalability, easy integration with existing EVMs, and promotes inclusivity for all voters. A prototype will be developed and evaluated on accuracy, speed, and user satisfaction to validate its effectiveness.

V. LITERATURE REVIEW

In recent years, substantial progress has been achieved in the development of intelligent systems designed to enhance security, accessibility, and automation across multiple sectors, including electronic voting, biometric verification, and assistive technologies.

Numerous studies have played a pivotal role in shaping this dynamic field, driving innovation and addressing key challenges in these domains.

In [1], Authors Proposed a pioneering smart lock system that integrates embedded intelligence and automation, establishing a foundational model for modern secure access control technologies. Their approach integrates electronics and informatics for real-world security solutions, emphasizing automation and access control.

The authors in [2] surveyed web-based voting techniques, highlighting the shift from traditional to digital voting methods. Engineered an advanced security lock leveraging embedded systems and automation, setting a precedent for next-generation intelligent access control frameworks.

In a broader societal context, the Authors of [3] examined postcolonial urban transformations in India, offering valuable insights into how evolving information infrastructures influence urban planning and governance. Though not directly related to voting systems, this work frames technological transitions in sociocultural settings.

The Authors in [4] presented a voting system tailored for India, proposing enhancements through intelligent embedded systems. Their approach emphasizes voter authentication and system integrity, aligning closely with democratic reliability.

The Researchers in [5] developed a method for efficient image set classification based on linear regression, contributing to pattern recognition and biometric verification key elements in face-based authentication systems.

The Authors in [6] explored face identification techniques using advanced image processing. Their work reinforces the relevance of facial biometrics for secure authentication, which is instrumental in applications such as e-voting and surveillance.

The Author in [7] proposed a location-independent voting model leveraging IoT technologies, enabling greater voter accessibility while minimizing dependence on physical polling infrastructure. This method improves voting participation and system robustness.

In [8], Author presented a biometric-based smart voting system, reviewing biometric integration techniques and emphasizing the benefits of fingerprint and facial recognition for electoral authentication.

The Authors in [9] addressed multi-modal biometric recognition, combining fingerprint and facial data to enhance the accuracy and reliability of user authentication systems, particularly in sensitive environments such as electronic voting.

The Authors in [10] introduced an anti-cheating presence system using dual vision face recognition and PCA. Their system enhances monitoring capabilities in real-time environments, making it useful for exam halls, offices, and secured access zones.

The Researchers and collaborators in [11] proposed an e-smart voting system with cryptographic data security, ensuring data integrity during vote transmission and verification. This solution addresses critical concerns about privacy, vote tampering, and secure identification.

VI. SYSTEM DESIGN

System design involves outlining the architecture, components, interfaces, and data structures required to meet specific system requirements. It applies principles of systems theory to the development of products and solutions. The primary goal of system design is to deliver detailed and comprehensive information about the system and its elements, ensuring smooth implementation in alignment with the models and views established during the architectural phase.

Architecture: This Smart Voting System is designed to enhance the security and efficiency of the voting process using facial recognition. The system begins with the Face Capture Module, which captures a live image of the voter. This image is processed by the HOG (Histogram of Oriented Gradients) Feature Extractor, converting it into a set of significant features. These features are then passed to the SVM (Support Vector Machine) Classifier for identity verification. The SVM Classifier matches the extracted features with the data stored in the Database. Upon successful authentication, the voter accesses the User Interface to proceed further. The User Interface guides the authenticated voter to the Voting Process module, allowing them to cast their vote securely. The Database maintains the records of registered voters, extracted features, and voting activity logs. This modular approach ensures high system accuracy, fast processing, and enhanced security.

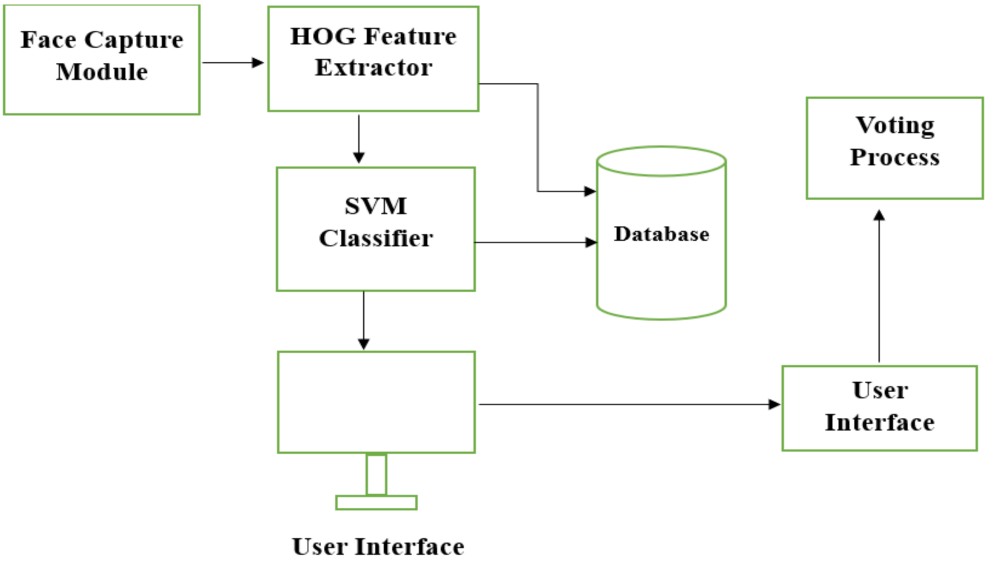

Fig 1: Architecture of Smart Voting System through facial recognition

Flowchart: The proposed smart voting system initiates its operational flow when a voter accesses the designated secure online voting portal. This platform serves as the central interface for communication between the user and the server, leveraging secure web technologies to maintain the integrity and confidentiality of the data exchange. Upon accessing the portal, the voter is prompted to undergo an identity verification procedure, which begins with the real-time acquisition of a facial image via a live camera integrated into the user's device. This live feed ensures that only present and active users are considered, minimizing the possibility of spoofing or use of static images. Once the facial image is captured, it undergoes a crucial Pre-Processing and Feature Extraction phase. During this stage, the system performs operations such as image normalization, background removal, grayscale conversion, and facial landmark detection. These steps help in enhancing the image quality and isolating the most significant facial regions. The Histogram of Oriented Gradients (HOG) technique is then applied to extract distinctive features from the face capturing the shape, structure, and orientation of facial contours. These extracted features are formatted into a high-dimensional feature vector that uniquely represents the individual's face. This refined feature vector is then passed to a Support Vector Machine (SVM) classifier, a powerful and widely used supervised learning algorithm. The SVM model, pre-trained on a comprehensive dataset of authorized voters, evaluates the incoming data by mapping it into a high-dimensional space where it can accurately distinguish between authorized and unauthorized faces based on the boundaries it has learned. This classification step is critical to ensuring that only valid users proceed through the system. Simultaneously, the system accesses a secure and encrypted reference database, which houses facial data of pre-registered and verified voters. A matching algorithm compares the feature vector from the live capture with the vectors stored in the database. This comparison involves a similarity assessment, often based on Euclidean distance or cosine similarity, to determine whether the current face corresponds to any of the stored identities. If the computed similarity exceeds a pre-defined threshold, the system identifies the individual as an Authorized Voter. This successful authentication grants the user access to the next phase of the voting process, which may include ballot selection, vote submission, and secure vote confirmation. Conversely, if no matching identity is found or if the similarity falls below the acceptance margin, the system flags the attempt and classifies the user as an Unauthorized Voter. In such cases, the system immediately terminates the session and optionally logs the attempt for auditing purposes. This secure and intelligent pipeline not only enhances the accuracy of voter authentication but also ensures that each vote cast is legitimate, traceable and protected from manipulation. By integrating AI-based classification, and encrypted data handling, the system offers a scalable, tamper-resistant, and user-friendly solution to modern electoral challenges. Moreover, it significantly reduces the risk of impersonation, duplicate voting, and unauthorized access issues that often compromise traditional voting methods.

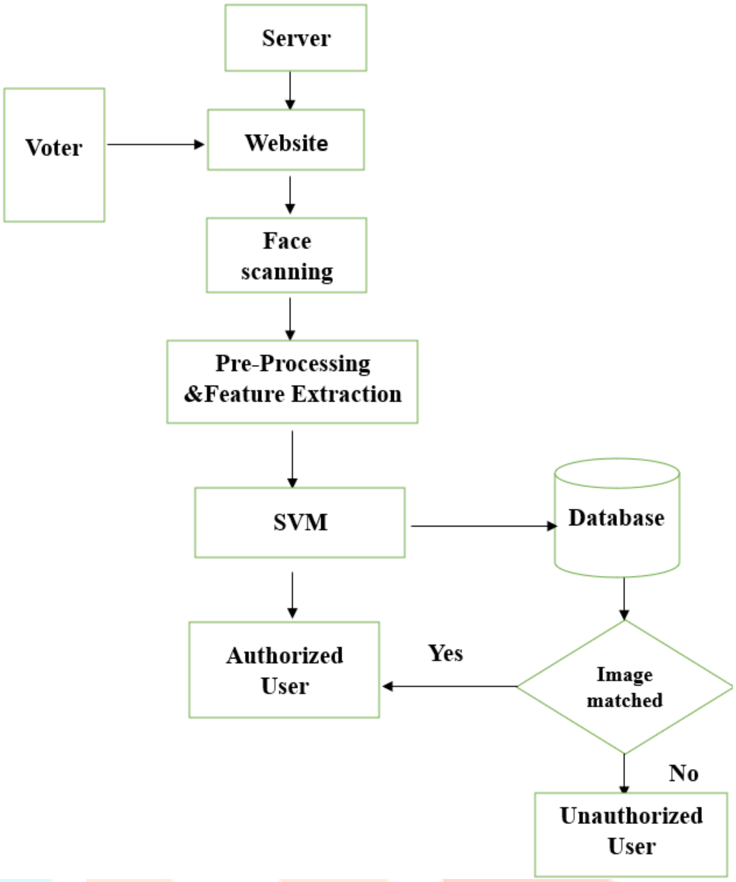

Fig 2: Flowchart for Smart Voting System through facial recognition

VII. SYSTEM IMPLEMENTATION

HOG (Histogram of Oriented Gradients)

The Histogram of Oriented Gradients (HOG) is a robust and highly effective feature descriptor, frequently employed in image processing and computer vision, particularly excelling in tasks such as object detection and facial recognition. It captures essential structural and textural information from an image by examining the distribution of gradient orientations across localized regions. The process begins with converting the image to grayscale, which simplifies the image by eliminating color information and reducing computational complexity. Following this, gradient magnitudes and orientations are computed for each pixel in both the horizontal and vertical directions. These gradients represent changes in intensity across neighboring pixels, enabling the identification of edges and contours crucial for object recognition. The image is then subdivided into small cells typically 8×8 pixels in size where a histogram of gradient orientations is constructed for each cell. These histograms quantify the frequency of specific gradient directions within the cell, providing insight into local structures and patterns. To enhance the descriptor's invariance to lighting changes, shadows, or contrast variations, neighboring cells are grouped together into larger blocks, often sized 2×2 cells.

Within each block, the histograms are normalized to compensate for variations in illumination, ensuring that the extracted features remain robust and consistent under varying environmental conditions. The final HOG feature vector is constructed by concatenating the normalized histograms from all blocks, resulting in a high-dimensional vector that encapsulates the shape and texture characteristics of the entire image. This feature vector serves as a compact yet highly informative representation of the image, capable of effectively distinguishing between objects or faces even under varying conditions. The power of HOG lies in its ability to preserve spatial coherence, making it ideal for use in real-time applications where both speed and accuracy are critical. The simplicity of HOG, combined with its ability to capture detailed edge information, makes it an excellent choice for real-time recognition systems, particularly when integrated with machine learning classifiers like Support Vector Machines (SVM). This pairing allows HOG to leverage its rich feature set in a computationally efficient manner, enabling the effective recognition of objects and faces. HOG's widespread application in facial recognition is a testament to its capacity for encoding subtle structural patterns that are essential for distinguishing between similar faces in complex environments. Furthermore, HOG has demonstrated its versatility across various domains, from human detection in surveillance systems to medical imaging and autonomous driving, showcasing its utility in diverse fields where detailed and reliable feature extraction is crucial.

SVM (Support Vector Machine)

Support Vector Machines (SVM) are a sophisticated method used in the field of machine learning, primarily designed for the tasks of categorization and prediction. They excel in situations where the data is complex and high-dimensional, and they consistently yield accurate results. The essence of SVM revolves around finding an optimal divider that can separate distinct groups within a set of data points. This divider is referred to as a "hyperplane," and it is selected based on the principle of maximizing the distance between it and the nearest data points from each group. These nearest points are called "support vectors." By maximizing this distance, the algorithm ensures that the model performs well on new, unseen data, reducing the risk of overfitting to the training data. Although SVM is often applied to distinguish between two groups, it can be extended to situations where multiple groups need to be identified, using strategies that break down the problem into multiple binary classification tasks. A key challenge in many real-world problems is that the data is not always separable by a straight line or hyperplane, especially in complex scenarios.

To address this, SVM uses a clever technique known as the "kernel trick." This trick enables the transformation of the data into a higher-dimensional space, making it easier to find a straight line or hyperplane that can separate the groups. This process is computationally efficient because it avoids the need to explicitly calculate the transformation. The flexibility of SVM comes from its use of a tuning parameter that controls how the algorithm balances two important factors: maximizing the distance between the groups (margin) and minimizing the number of errors made in classification. By adjusting this parameter, the model can be adapted to fit different types of problems, optimizing for either generalization or accuracy. One of the distinguishing features of SVM is its focus on the "support vectors," which are the critical data points that define the boundary between groups. This ensures that the model remains efficient, relying only on the most important points for its decision-making process, rather than all data points, which can be especially valuable when data is limited or noisy.

VIII. RESULTS AND ANALYSIS

This smart voting system demonstrated outstanding performance in real-time facial recognition, achieving high accuracy even under varying lighting conditions and different facial angles. The system's ability to authenticate registered voters reliably in such challenging conditions underscores its robustness and adaptability. The integration of Histogram of Oriented Gradients (HOG) for feature extraction played a pivotal role in capturing important facial features, such as edges and textures, which are essential for distinguishing between individuals. HOG's ability to extract discriminative features from facial images, even with changing environmental factors, contributed significantly to the system's resilience in real-time applications. Support Vector Machine (SVM) classification further enhanced the system's effectiveness by providing a powerful decision-making framework that efficiently handled the high-dimensional feature space generated by HOG. SVM's capacity to classify facial data with minimal false acceptances (when an unauthorized person is wrongly recognized as a registered voter) and false rejections (when a registered voter is wrongly denied access) ensured high accuracy and trustworthiness of the system. During testing, the smart voting system exhibited consistent reliability across various scenarios, confirming its effectiveness in preventing voter impersonation and fraud. The combination of advanced feature extraction techniques (HOG) and a robust classification model (SVM) provided a secure and efficient solution for voter authentication. This result highlights the potential of such smart systems in improving the security and integrity of electoral processes, ensuring that only legitimate voters can cast their votes. In conclusion, the system not only demonstrated high accuracy but also proven reliability, confirming its suitability for real-world deployment in preventing electoral fraud and ensuring the fairness of voting processes.

IX. CONCLUSION

The smart voting system using facial recognition with OpenCV, HOG, and SVM enhances the security, accuracy, and efficiency of the electoral process. It addresses key issues like voter impersonation and human error by enabling automatic and reliable voter authentication. The system's robustness across various lighting conditions and facial angles makes it adaptable to real-world scenarios. Its reliance on open-source tools and minimal hardware requirements ensures cost-effectiveness and scalability for large-scale deployment.

REFERENCES

[1] Varad Pandit, Prathamesh Majgaonkar, Pratik Meher, Shashank Sapaliga and Sachin Bojewar, "Intelligent security lock", Trends in Electronics and Informatics (ICEI) 2017 International Conference on, pp. 713-716, 2017.
[2] C. U. Chauhan, Abhishek Kalnawat, Akshay Aswale, Ujwal Gautam and Roshan Nemad, "Survey Paper on a Novel Approach: Web Based Technique for Vote Casting", International Journal of Engineering and Management Research (IJEMR), vol. 7, no. 5, pp. 71, 2017.
[3] Ravi. Sundaram, "The Postcolonial City in India. From Planning to Information?", Techniques & Culture. Revue semestrielle d'anthropologie des techniques, 2017.
[4] Shrikant Subhash Warghade and B. Karthikeyan, "Voting System for India" in Intelligent Embedded Systems, Singapore:Springer, pp. 59-65, 2018.
[5] Syed Afaq Ali Shah, Uzair Nadeem, Mohammed Bennamoun, Ferdous Sohel and Roberto Togneri, "Efficient image set classification using linear regression based image reconstruction", 2017.
[6] Chinmay Bhimanwar, Nikhil Bhole Rupesh Biradar and Milind Rane, "Face Identification", International Journal of Engineering Science, vol. 11923, no. 2017, pp. 8.
Qasim Abbas, Sarah Javaid and Tanzeel HussnainAbass, "Location-free Voting System with the help of IOT Technology", 2018 12th International Conference on Mathematics Actuarial Science Computer Science and Statistics, pp. 14-20, 2018.
[8] J. Deepika, S. Kalaiselvi, S. Mahalakshmi and S. AgnesShifani, "Smart Electronic Voting System Based On Biometric Identification-Survey:2017", Third International Conference on Science Technology Engineering & Management (ICONSTEM), no. 2017, pp. 939-942.
[9] Ambikesh Kumar Gupta Sanjay Thakre and Shilpi Sharma, "Secure Reliable Multimodel Biometric Fingerprint and Face Recognition:2017", International Conference on Computer Communication and Informatics (ICCCI -2017), pp. 95-99, Jan. 05 – 07, 2017, January 2017.
[10] Husni Al Amin and Muji Sukur, "Anti-Cheating Presence System Based on 3WPCADual Vision Face Recognition: Proc. EECSI 2017", Yogyakarta Indonesia, pp. 121-124, 19 - 21 September 2017.
[11] Amish Basal, Utkarsh Raina, Vaibhavi Pujari and Roushan Kumar, "E-Smart Voting System with Secure Data Identification using Cryptography:2018", 3rdInternational Conference for Convergence in Technology (I2CT), pp. 1-4, Apr 06-08, 2018.