IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 4, April 2025

DOI: 10.17148/IARJSET.2025.12439

SECURE ONLINE E-VOTING SYSTEM WITH FACIAL RECOGNITION USING MACHINE LEARNING

P. Vasantha[1], Ch. Ratna[2], E. Divya Sree[3], J. Lakshmi[4], N. Charmi Chowdary[5]

M.Tech, Asst.professor, Computer Science & Engineering, Bapatla Women's Engineering College, Bapatla, India [1]

B.tech , Computer Science & Engineering, Bapatla Women's Engineering College, Bapatla ,India [2-5]

Abstract: Systems for electronic voting (E- Voting) have drawn a lot of interest as a way to improve the effectiveness, openness, and accessibility of the voting process. In order to verify voters and guarantee the fairness of the voting process, this study suggests a unique e- voting system that makes use of face recognition techniques based on machine learning and deep learning algorithms. The proposed system leverages advancements in computer vision and artificial intelligence to address the challenges of traditional voting systems, such as identity fraud, impersonation, and multiple voting instances

Keywords: E-voting, Face Recognition, Image Processing, Machine learning, KNN Algorithm, Open CV

I. INTRODUCTION

Electronic voting (E-voting) systems is offering the electoral process. To ensure the integrity and security of these systems, various technological advancements have been incorporated, including the utilization of face recognition techniques based on machine learning and deep learning algorithms. The objective of this research is to present an innovative E-voting system that leverages state-of-the-art advancements in computer vision and artificial intelligence to authenticate voters and enhance the reliability of the voting process. By incorporating face recognition technology, the proposed system aims to mitigate concerns such as identity fraud, impersonation, and multiple voting instances, thus bolstering the integrity and trustworthiness of the electoral system. In India, voting is done using either the traditional paper ballot system or an electronic voting machine (EVM). Since there is a great possibility of fraudulent or dummy voting, as we have long observed, this voting process is carried out in some way. The current systems are readily manipulated; a dishonest official or candidate might cast a fictitious vote on an EVM because there is no biometric verification, or he could stamp a fictitious ballot on paper. These two systems are designed to be carried while being closely monitored and with security people. The ongoing fraud of fraudulent voting will be stopped since biometrics cannot be taken from anyone or utilized by anyone else. His document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

II. PROBLEM STATEMENT

Despite the progress that our nation has made towards digitalize India, the voting system still has certain issues. In accordance with the current system, voter registration is only feasible if voters visit the polls. The name of the voter appears in the list for his or her particular area at the time of voting. Outside of the area surrounding the address listed on the voting card, they are unable to cast a ballot. Therefore, voters who have moved elsewhere are unable to cast physical ballots. We can see the peril of this system from the current Corona Virus pandemic situation. Due to the requirement that the voter be physically present to cast their ballot, this could result in a failure of social distance throughout the voting process.

III. LITERATURE SURVEY

A The literature survey reveals that E-voting systems employing face recognition technology have garnered significant attention. The studies emphasize the potential of face recognition algorithms, including deep learning approaches, in ensuring secure and efficient voter authentication. Additionally, researchers have explored critical aspects such as system security, privacy preservation, usability, and user acceptance, contributing to the development and improvement of e-voting systems using face recognition. These studies collectively provide valuable insights and pave the way for further advancements in this field.

1) Enhanced Security E-Voting Machine
In this work, voting using paper ballots and an EVM requires a lot of time. In order to save in consideration of the quantity of time. Therefore, the system is being implemented in this case in a manner that prevents the use of paper ballots to ensure voting secrecy. Voting machines now in use cost more money than EVMs and use VVPAT. Results can be accessed with only one click and EVM provides 100% proof of tampering. Because there is no need to hand count votes, labour costs are reduced.

2) Multipurpose, cross-platform online voting system
A multipurpose cross-platform online voting system is a versatile and flexible platform that enables voting processes to be conducted electronically across various devices and operating systems. This type of system serves as a comprehensive solution for different voting scenarios, including governmental elections, organizational decisions, surveys, and opinion polls. The voting ballot is produced by this system. User-end encryption and local administrator-end decryption are used for voting data. As a result, the voting system is more secure and authenticated. The literature review describes the major contributions that various authors have made to the field of face recognition.

3) Leveraging Biometric Authentication for Secure and Transparent Voting Systems
The concept of leveraging biometric authentication for secure and transparent e-voting systems represents a significant advancement in the field of electoral processes. By integrating biometric technologies, such as fingerprint or iris recognition, into e-voting systems, the aim is to enhance the security and reliability of voter authentication. Biometric authentication offers a highly accurate and unique identification method, as each individual possesses distinct biometric characteristics. This ensures that only eligible voters can participate in the voting process, mitigating the risks of impersonation or fraudulent activities. Moreover, biometric authentication provides a transparent and tamper- proof mechanism, as it relies on physical traits that cannot be easily duplicated or manipulated. This instills confidence in the integrity of the electoral process and assures voters that their voices will be accurately represented.

IV. EXISTING SYSTEM

In the current system, there are two types of voting: electronic voting machines and secret ballot papers. It is challenging to finish the poll in a single day since it takes a lot of manpower to maintain order and security. Allocation of surveys carried out by commission. At advance of two weeks, voters' cards are issued and polls are set up at schools and universities. There is a set time and location. On Election Day, all polling places will be open for voting in eight hours. The voter must first enter the polling place, where an officer will check their voter identification card and mark their left forefinger with inedible ink. The voter must then sign the register after the officer has finished.

V. PROPOSED SYSTEM

The proposed e-voting system aims to leverage the capabilities of face recognition technology, machine learning, and deep learning to enhance the security, accuracy, and efficiency of the electoral process. The system will offer a robust and reliable method for voter authentication, mitigating potential fraud and ensuring the integrity of the voting system.

Data Collection and Pre-processing: The system will start by gathering a diverse and representative dataset of voters' facial images. This dataset will be pre-processed to ensure consistency and quality, including resizing, normalization, and data augmentation techniques to handle variations in lighting conditions, facial expressions, and mask styles.

Feature Extraction with Deep Learning: The proposed system will employ deep learning techniques, such as K-Nearest Neighbours(KNNs), for facial feature extraction. KNNs have shown remarkable capabilities in learning complex patterns and features from images, making them suitable for face recognition tasks.

Model Training: The pre-processed dataset will be used to train the deep learning model. During the training process, the model will learn to map facial images to unique feature vectors, forming a distinct representation of each voter**.**

Usability and Accessibility: The user interface of the e-voting system will be designed with user- friendliness and accessibility in mind. Clear instructions and intuitive design elements will make the voting process straightforward and inclusive for all voters, including those with disabilities. Privacy protection measures and user-centric design elements ensure that the system prioritizes voter privacy and accessibility while advancing the state of e-voting technology.

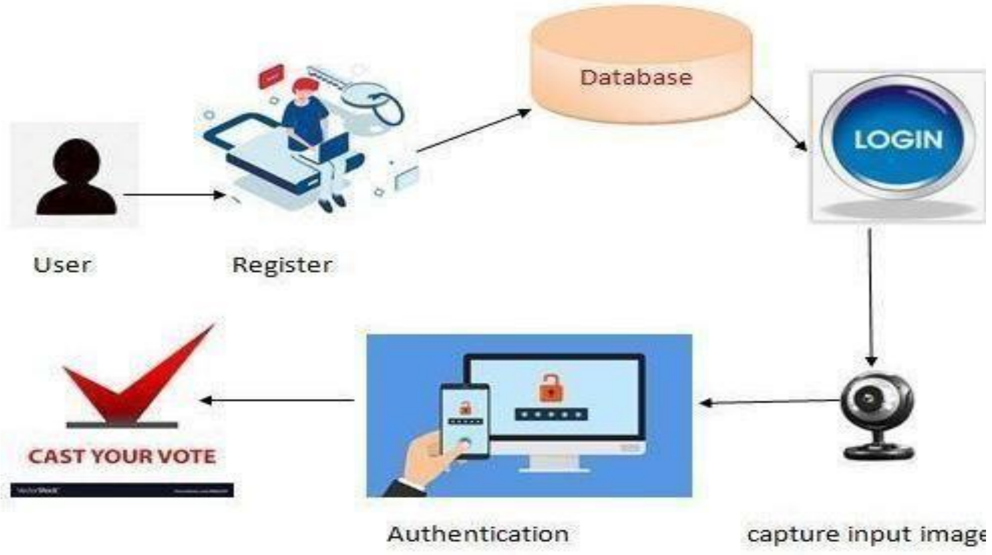
Working of the Algorithm

K- Nearest Neighbour Algorithm

One of the primary categories for image classification and picture identification is the KNN. KNNs are frequently employed in a variety of applications, including object identification and facial recognition. Using the KNN algorithm, our work project will identify and categories drones in videos. In an online e-voting system that incorporates face recognition, the K-Nearest Neighbors (KNN) algorithm can be effectively used to verify the identity of voters based on their facial features. The system first requires a pre-registered dataset of facial images, each labeled with the corresponding voter ID. During the registration phase, facial features are extracted using techniques such as Histogram of Oriented Gradients or deep learning-based embedding, and these features are used to train the KNN model. When a voter attempts to cast their vote online, the system captures a live image using their device's camera, detects the face, extracts the facial features, and compares them with the existing database using the KNN algorithm. The algorithm identifies the closest match based on feature similarity and confirms the voter's identity. This ensures that only authenticated users can vote, helping to prevent fraud and duplicate voting. KNN is particularly useful in this context due to its simplicity, ease of implementation, and effectiveness in handling small to medium-sized datasets commonly found in localized voting systems.

VI. IMPLEMENTATION

This project is carried out with python, an object- and procedure-oriented programming language. Python is being used to carry out this project. Python offers dynamic typing and garbage collection. Due to its extensive standard library, Python is referred regarded as a "batteries included" language. Machine learning techniques are used in this investigation. Implementation of Security Protocols: Several security protocols are in place to protect the integrity of the electronic voting system. Data encryption techniques guard private voter data and shield it from unlawful access. To strengthen identity verification, which combines facial recognition with or password-based techniques. Algorithms for anomaly detection and real-time monitoring also aid in identifying and thwarting prospective hacking attempts and cyber threats.



E-Voting System Architecture

It is a detailed framework that describes the design and parts of the electronic voting system is known as the e-voting system architecture. The architecture's primary goal is to support effective voting procedures that are transparent and secure while still maintaining their integrity. The front end, back end, and database make up the system's three main parts most of the time. Voters can cast their ballots and authenticate their identities using a variety of authentication techniques, such as biometrics or passwords, through the interface that the front-end manages.

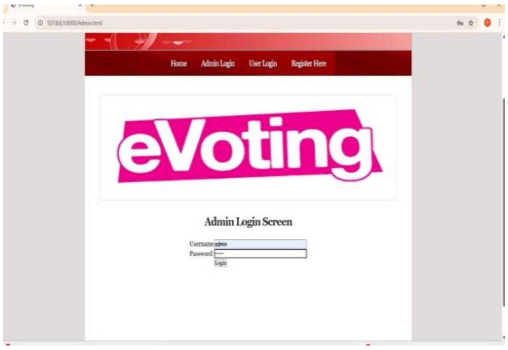
The main operations of the system, such as voter registration, ballot creation, and vote tallying, are included in the back-end. For the purpose of protecting voter privacy and preventing tampering, this component makes use of cutting-edge cryptographic methods. Finally, the database contains important data such voter registration information, ballot information, and voting outcomes. To protect the data, security measures like encryption and access limits are put in place. The e-voting system architecture takes advantage of technology's potential to speed up voting, lessen administrative burden, and give citizens a cutting- edge, reliable platform for taking part in democratic elections.

FACE MASK DETECTION WITH TENSOR FLOW AND KERAS SECTION

The implementation and methods utilised to determine whether or not people are wearing face masks using deep learning techniques are the main topics of the section on face mask detection using TensorFlow and Keras. This section seeks to give a general overview of the procedures required in creating a face mask detection system utilizing the TensorFlow and Keras frameworks. It provides an explanation of the dataset's structure, including the quantity of photos and the distribution of instances with and without a mask. It also emphasizes how crucial it is to gather a wide variety of representative photos in order to guarantee the model's usefulness in real-world situations. The section next goes over the pre-processing techniques used on the dataset. The purpose of these pre- processing procedures is to improve the model's generalization and handling of changes in facial appearances, lighting situations.

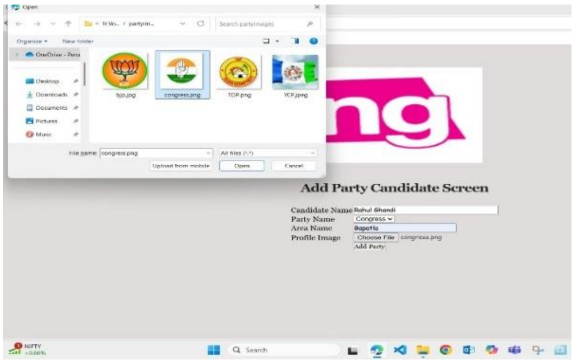
VI. RESULT ANALYSIS

The result analysis of the **Online voting system using face recognition with the K-Nearest Neighbors (KNN) algorithm** shows promising outcomes in terms of security, accuracy, and user experience. The system is divided into two main modules: The User Module and the Admin Module. In the User Module, voters undergo a facial verification process during login, where the KNN algorithm identifies the most similar face encodings from the stored dataset based on distance metrics. This approach ensures fast and accurate recognition, even under varying lighting conditions or minor facial variations. Upon successful authentication, the user can cast their vote, which is then securely stored and recorded. The Admin Module is responsible for managing the voter database, monitoring vote status, and generating election results. Administrators can view logs of user activities, detect any anomalies, and ensure that only verified individuals have participated. The use of KNN for face recognition significantly reduces false acceptance and rejection rates, ensuring that each voter is uniquely identified. Furthermore, the integration of secure hashing (e.g., SHA-256) can be used alongside KNN to encrypt votes and sensitive data, enhancing system integrity. From performance evaluations, the system exhibits high recognition accuracy, low computational cost, and ease of implementation, making it suitable for small to mid-scale elections. The interface is user-friendly, allowing even non-technical users to participate confidently. Overall, the combination of facial recognition using KNN and robust administrative control provides a secure, efficient, and transparent solution for modern e-voting applications.



Admin Login Screen

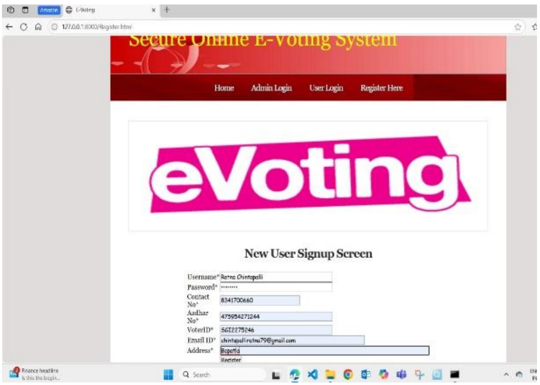
Username admin
Password ••••••



File name: congress.png

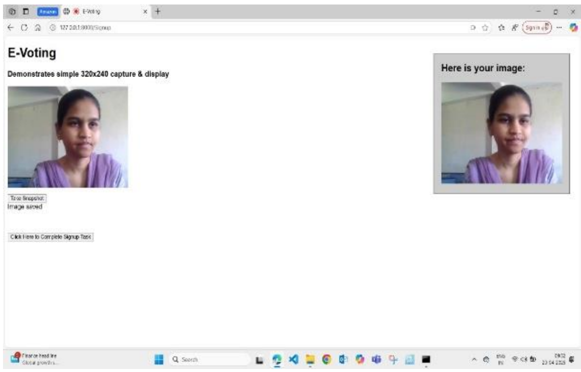
Add Party Candidate Screen

Candidate Name Rahul Ghandi
Party Name Congress
Area Name Bapatla
Profile Image congress.png



New User Signup Screen

Username* Ratna Chintapalli
Password* ••••••••
Contact No* 8341700660
Aadhar No* 475954271244
VoterID* SGT2275246
Email ID* chintapalliratna79@gmail.com
Address* Bapatla

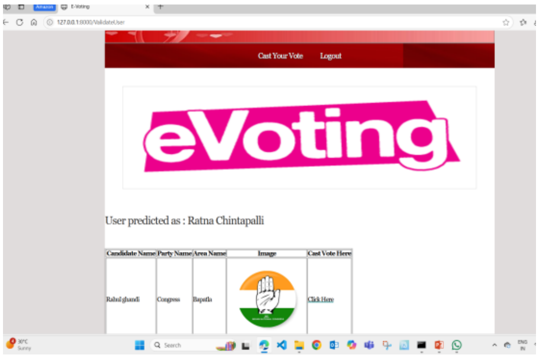


E-Voting

Demonstrates simple 320x240 capture & display

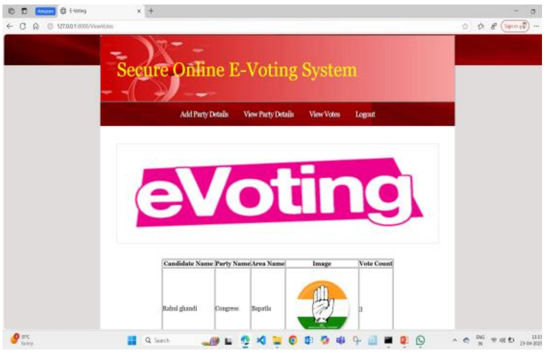
Image saved

Here is your image:



User predicted as : Ratna Chintapalli

Candidate Name	Party Name	Area Name	Image	Cast Vote Here
Rahul ghandi	Congress	Bapatla		Click Here



Candidate Name	Party Name	Area Name	Image	Vote Count
Rahul ghandi	Congress	Bapatla		3

VII. CONCLUSION

The study of facial recognition in E-voting systems utilising machine learning shows the enormous potential of this strategy in enhancing the safety, effectiveness, and integrity of the electoral process. The E- voting systems can successfully authenticate voters, reduce fraud, and improve privacy by integrating cutting- edge technology like machine learning. Since we can see that the current democratic framework has several short comings, including lengthy procedures that take a lot of time, are insecure, we may argue that our method is more beneficial and safe than it. We can steer clear of them during political contest commissions by using the facial validation technique to detect voters who cast fraudulent ballots. voting system on the web. For the most part, India's cities are the result of smart voting. It ought to be seen as the biggest problem facing the majority of us. The current voting processes need a lot of physical labour and human resources, and if voting is moved online, a secure voting system is required. The approach to machine learning. Are used to identify faces and determine if a voter is authorized or not.

VIII. FUTURE SCOPE

The E-voting system using face recognition based on machine learning and deep learning systems presents several exciting future possibilities that can further enhance the security, accessibility, and efficiency of the electoral process. While significant progress has been made, there are still ample opportunities for research and development in this area. Some key future scope areas include:

1) ***Multi-Modal Biometrics***: Integrating multiple biometric modalities, such as fingerprint, iris, or voice recognition, with face recognition can enhance the accuracy and security of e-voting systems.

2) ***Continuous Model Improvement:*** To keep pace with evolving technology and potential threats, e-voting systems should adopt a continuous improvement approach. Implementing mechanisms for model updates and retraining will ensure that the face recognition algorithms remain up-to-date, accurate, and secure.

3) ***Hardware Integration:*** Future e-voting systems could explore hardware integration, particularly on mobile devices and other edge devices. This would enable on- device face recognition, minimizing data transmission and increasing privacy.

4) ***Privacy-Preserving Techniques***: To address concerns about voter privacy, research can delve into advanced privacy-preserving techniques for face recognition.

5) ***Usability and Accessibility:*** Future research should focus on making e-voting systems more user-friendly and accessible to a wider range of voters, including those with disabilities.

In conclusion, the future scope for E-voting systems using face recognition based on machine learning is vast and promising. By addressing challenges related to robustness, privacy, and usability while exploring innovative technologies and integration approaches, these systems have the potential to revolutionize the electoral landscape, ensuring secure, transparent, and accessible voting processes for citizens around the world.

REFERENCES

[1]. A.S.Narote, S.P.Narote, S.V.Tathe "Face Detection and Recognition in vids" Sinhgad College of Engineering 2015.

[2]. Adam Baumberg, Surrey(2020)" reliable Features Matching Across the Extensively Seperate Views". Ordinance Research Center Europe Limited Occam Court, Surrey Research Parks Guildford, Surrey GU2 5YJ United Kingdom 2000 IEEE

DOI: 10.17148/IARJSET.2025.12439

[3]. A.K. Syafeeza,M.Khalil-Hani,S.S. Liew,R. Bakhteri Electrical Engineering, Universiti Teknologi Malaysia(2014)" Convolutional Neural Network(KNN) for the Face Recognition with Pose and Illumination Variation" International Journal of Engineering and Tech Vol 6 No 1 Feb-Mar 2014 ISSN 0575- 4024
[4]. Nasser Kehtarnavaz, Mohammad Rahman and Jianfeng Ren Department of Electricals Engineering, University of Texas at Dalla(2009)" A cross strain faces position approach for nonstop association on cell phone" 2009.
[5]. Prof. Shashank S Kadam, Ria N Choudhary, SujayDandekar, DebjeetBardhan, Namdeo B Vaidya "Electronic Voting Machine with Enhanced Security"
[6]. RahilRezwan, Huzaifa Ahmed, M. R. N. Biplob,S.M. Shuvo, Md. AbdurRahman "Biometrically Secured Electronic Voting Machine"
[7]. Z.A. Usmani, Patanwala, MukeshPanigrahi, Ajay Nair "Multipurpose platform independent online voting system."

BIOGRAPHY

P.Vasantha,M.Tech, Asst.professor,
Dept of Computer Science & Engineering,
BWEC, Andhra Pradesh,India

Ch.Ratna ,B.Tech, Student,
Dept of Computer Science & Engineering,
BWEC, Andhra Pradesh,India

E.Divya Sree,B.Tech, Student,
Dept of Computer Science & Engineering,
BWEC, Andhra Pradesh,India

J.Lakshmi,B.Tech, Student,
Dept of Computer Science & Engineering,
BWEC, Andhra Pradesh,India

N.Charmi Chowdary,B.Tech,Student,
Dept of Computer Science & Engineering,
BWEC, Andhra Pradesh,India