Grenze International Journal of Engineering and Technology, June Issue

A Smart Approach for Voting using Face Recognition

N. Indumathi[1] and L. Dharshana Deepthi[2]
[1-2]Assistant Professor, Department of CSE, PSNA College of Engineering and Technology, Dindigul, India
Email: indhujegan1996@gmail.com, dharshnadeepthi@gmail.com

***Abstract*—Elections are the cornerstone of democracy and government. The electoral system has essentially undergone a number of changes during the past few decades. The world's largest majority rule nation, India, still uses secret ballot voting (SBV) or electronic voting machines (EVM) for its elections. Voter fraud is more likely because the present procedure only reviewed identifying documents. This project intends to design a computerized voting system to make voting more convenient and secure. Most people choose not to vote because they dislike having to wait in line or travel to polling stations. Voters who are all ineligible may also cast false ballots, which can lead to a great deal of issues. The whole web infrastructure allows people to cast their ballots from anywhere in the world. This tactic could help reduce the amount of money the government spends on elections.**

***Index Terms*— EVM, SBB, Computerized voting system, Democracy, Fake votes.**

I. INTRODUCTION

Elections are important in a country like India, where the people elect their leaders. Because elections provide citizens the freedom to select the form of government they prefer, they maintain the functioning of a true state. Therefore, there should be no bias and transparency in the electoral process. In a democracy, every individual is entitled to cast any kind of ballot. One of the main issues with the old democratic system is its high labor and resource costs. Concerns regarding movement that has been unlawfully disclosed throughout this election season or in the run-up to it may also be present for some persons. There are a number of issues with the conventional election voting method that is used in our country, such as the potential for violence, malfunctions with voting machines, the need for time and resources, scheduling conflicts, and more. Many people were unable to cast their votes because they lived too far away from their original birthplace or because they had to physically visit the voting stations. An online voting method for use throughout the election process via a web-based program. In the beginning, paper ballots were used for voting. Subsequently, electronic voting machines surface; these are straightforward to use and store data on. Compared to paper ballots, they are more secure and require less time. Now, we proposed a biometric authentication technology to minimize the voting process and improve voting security. This enables the voter to use their system to solidify their support for the candidate of their choice. Technology for facial detection and recognition is utilized to confirm whether or not a citizen is the intended customer. We provide several modules where an administrator can explore the numerous features of the product by logging in. People can log in and use their voting rights as well. Upon voter use, the system records the voter's image using a web camera and compares it to an image stored in the database. If the voter's two photographs match, they can cast a ballot. Most universities in Kenya hold elections on a regular basis to choose a student leadership. They recommended utilizing an online system that would enable voter registration, ballot casting, ballot verification, and results announcement. This would offer a good substitute for the structure that Kenyan

Grenze ID: 01.GIJET.10.2.655

educational institutions currently employ.

II. Aims and Scope Objectives

Using the University of Ibadan as a real-world case study, an application is developed with the goal of enhancing political party election processes through the use of several secure authentication levels. The ultimate objective is to offer an online platform that allows any qualified voter to cast a ballot during election season from any place.

The objectives are:

1. To develop a protected online voting system that uses mechanisms like facial recognition and one-time passwords to assure the validity of votes and voters.
2. To strengthen voter identification because biometric functions cannot be shared.
3. To reduce the inconvenience of standing in line throughout the election's voting period.

III. Literature Survey

Smart voting by facial recognition was presented in 2021 by Mahalakshmi Mabla Naik and Dr. Preethi N. Patil for the International Journal of Creative Research Ideas (IJCRT). For face identification, they have used the Haar Cascade method, which coordinates the face using Haar-Like characteristics. A method for detecting objects is called Haar Cascade. Three degrees of confirmation exist in the suggested scheme. The first one confirms the user id, and the second one asks for the voter card number. The voter moves on to the next level of checks in the case that they successfully completed the first two levels of confirmation. This approach can only be used to verify whether a voter is legitimate at the most basic level of security. Smart Voting Machine Based on Fingerprints and Face Recognition was presented in 2020 by Nadar Rajkani Paulraj, G. Rajagopalan, M. Rajesh, S. V. Kirutika, and I. Jasmine A/P, an International Journal of Engineering Research & Technology. They have created a smart voting machine that eliminates the requirement for the user to carry an ID that has the necessary information. Smart voting method utilizing face recognition was presented in 2021 by Swapnil Singh, Krunal Patil, Shaik Aftab, Kapil Chuadhary, and Prof. Sushma A Shirke for the International Journal of Advanced Research in Science. The objective of this project is to create a facial recognition voting system that would allow any Indian voter to cast their ballot at the nearest polling place from "ANYWHERE IN INDIA." The implementation of this project maintains high-level biometric security. All of the voter data is stored on a server in a database. In order to enhance the current voting process, a brand-new, secure voting system is being created in this paper. The proposed method establishes an automated voting system that does not require human involvement. In this technique, voters are photographed and the images are recorded in a database for analysis. Smart Voting System Using Face Detection and Recognition Algorithms was presented in 2021 by M. Kandan, Koppula Durga Devi, Kasani Durga navya Sri, and Nunna Ram at the IEEE International Conference on Intelligent Systems, Smart and Green Technologies (ICISSGT). They created a cutting-edge face detection and recognition method in addition to a web-based smart voting system. The complete online infrastructure gives people the ability to safeguard their votes from anywhere in the world. By using ID based on appearances, the likelihood of vote-copying is reduced, and only those who have registered to vote and are recognized by the system will be able to do so.

IV. Existing System

The efficiency of the current system is low. These days, there are two types of voting processes:

1. Voting at ballot booths
2. Voting using EVM

A. Ballot Booth Voting

In elections, a ballot is a voting tool. It can also be a piece of paper used for secret voting. In this election, each voter receives a sheet of paper bearing the names and logos of all the political parties as well as their representatives. Here, voters visit the polls, complete their ballots, and mark their vote with the corresponding party symbol. After folding, the ballot is inserted into the voting machine. Ultimately, the votes are totaled by the members of the electoral commission.

B. EVM (Electronic Voting Machine) Voting

An Electronic Voting Machine (EVM) is a device. This device displays the representative's name, party emblems, and buttons at the end of each party name. Voters approach the electronic voting machine (EVM) after completing their early level voting verification. After verification, the voter approaches the EVM and hits the button to cast their vote. The voting procedures indicated above could be vulnerable to fraud, which would reduce their accuracy. Votes may be miscounted, giving the wrong people power, or ballots may be misplaced during the counting process, which could affect the result in that particular location. Voting is stopped and a lot of time is lost when EVMs break down. On the other hand, votes meant for many candidates or parties may be cast exclusively for one party if an electronic voting machine is tampered with. Power could end up in the wrong hands as a result of this.

V. METHODOLOGY

There are three steps in the process:

A. Phase 1- Individual Recognition

The total number of people in the picture is now being ascertained. One excellent pre-trained convolutional neural network (CNN) for facial recognition is included in this. The new model performs better in face detection when compared to earlier models like Haar. The new model is trained in the context of Caffe.

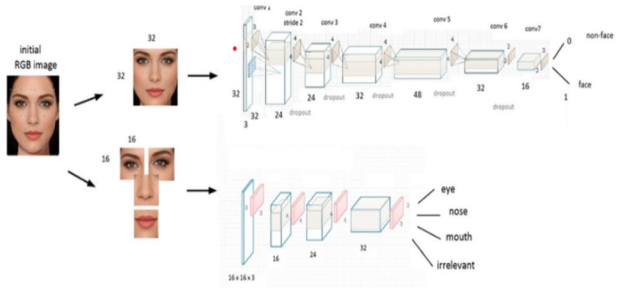


Fig 1: CNN Model for Facial Recognition

B. Phase 2- Face Mask Detection

You can detect and operate with faces from Python or the command line using Face Mask Detection, the most basic face recognition package available. The model achieves 99.38% accuracy on the Labeled Faces in the Wild benchmark. Additionally, a simple command line tool for face recognition is included, which lets you do face recognition on a folder of photos right from the command line! Find and modify facial traits in pictures. Determine the locations and outlines of each person's mouth, nose, eyes, and chin.

C. Phase 3: Face Recognition

Everything we learned previously about turning faces into feature vectors and figuring out how to tell one face from another is included in an incredibly simple Python module. A Python library called face recognition that has a number of machine learning methods to help with the development of intricate C++-based applications.

VI. PROPOSED SYSTEM

Our suggested solution enables consumers to cast their votes online rather than offline. Before being able to cast an online vote, users must input their details and upload a photo. Multiple recordings of each user's unique data, including their facial image, are made and stored in the database that is made available. After entering all of their details and registering their face in the system, the voter is ready to cast their ballot. The user need a mobile phone for OTP authentication, a webcam for facial recognition, and a robust internet connection for a smooth operation. It goes through two-factor authentication when elections are taking place. The first method is to use OTP authentication. The registered mobile number of the user receives an OTP. The user is prompted to enter the OTP in the system and is then advanced to the next authentication step if the OTP matches. For the second, face recognition is employed. When the user authenticates with his face through the camera, the system compares the face presented with the images kept in the database. If the user's face is recognized, the process advances to the following stage. In the next step, the user can select a party and cast a vote. As a result, the

voting process was effective. After the voting process is finished, or even before the user has cast their vote, everyone can examine the results of the ongoing election by visiting the provided website.
The following diagram shows the flow of the proposed system, which collects data from multiple platforms, stores it in a database, and uses it for validation. The proposed structure includes three degrees of confirmation, which can effectively lower the number of bogus votes.

Step I

Included is the user ID that was created during registration. All of the fields on the registration page require the user to enter accurate information. The user ID and password that were created during the registration step will be used for the initial verification stage. If a user's password and user ID are both correct, the system will allow them to move on to the next verification step.

Step II

In the second level of security, voter identity issued by the Election Commission is used and cross-checked by an official. The additional verification process the voter must go through will greatly boost security. If the voter's ID matches the data already in the database, only the voter will be allowed to move on to the next confirmation stage.

Step III

Here, the likelihood of fraud will be decreased and the security and accuracy of the framework will be improved by comparing the voter's current facial features to those in the database. The proposed framework will be used to apply the algorithm to facial recognition, and the method's precision will be estimated by practical application and testing on a test set.

Step IV

The last stage of the voting process, during which only voters who have been verified may cast ballots. The voter entered after passing through every security stage.

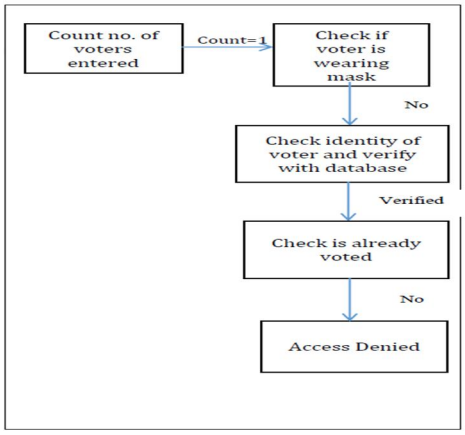
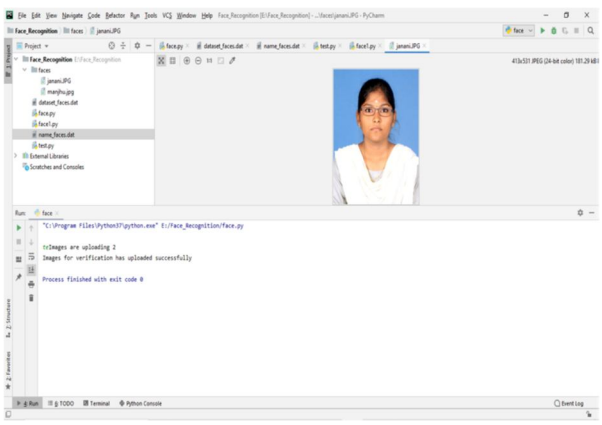
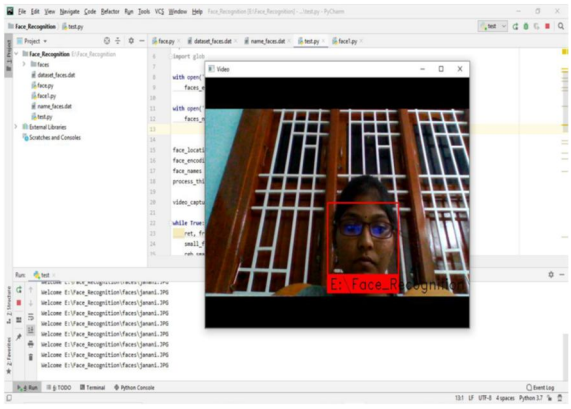


Fig 2: Architecture Diagram of Proposed system

VII. Implementation Results





REFERENCES

[1] Abbas Behrainwala, Amar Saxena, Ishika Nalani, Sakshi Sahay, Noshir Tarapore , “International Journal for Research”. Applied science & Engineering technology(IJRASET) Vol 10(2022).

[2] Mahalakshmi Mabla Naik, Dr. Preethi N. Patil.” Smart Voting Through Face Recognition”.International Journal of Creative Research Thoughts (IJCRT),2021.

[3] Nadar Rajkani Paulraj, G.Rajagopalan, M.Rajesh, S.V.Kiruthika, I.Jasmine. “Smart Voting Machine Based on Finger Prints and Face Recognition”. International Journal of Engineering Research & Technology (IJERT),2020.

[4] Swapnil Singh , Krunal Patil ,ShaikAftab,Kapil Chuadhary , Prof. Sushma A Shirke.” Smart voting system using Face Recoginition”. International Journal of Advanced Research in Science, Communication and Technology (IJARSCT),2019.

[5] A.Aravindhan, M.Kalaiyarasi, S.Bharanikumar, P.Dhanapal, R.Dharmaraj.”Smart Online Voting System using Facial Recognition Based On IOT and Image Processing”.IEEE 2019.

[6] Shrivastava, Vishesh, and Girish Tere. "An analysis of electronic voting machines for their effectiveness."International Journal of Computing Experiments (IJCE) Vol 1 (2019): 8-12

[7] Shanthi, D., Prabha, S.S., Indumathi, N. et al. A satin optimized dynamic learning model (SODLM) for sentiment analysis using opinion mining. Soc. Netw. Anal. Min. 13, 110 (2023).

[8] Dr.P. Golda Jeyasheeli and N. Indumathi, “Sentence Generation for Indian Sign Language Using NLP”, Webology Journal Special Issue on Artificial Intelligence in Cloud Computing, Volume 18, 196-210, **2021**

[9] Amarbayasgalan, T.; Pham, V.-H.; Theera-Umpon, N.; Piao, Y.; Ryu, K.H. An Efficient Prediction Method for Coronary Heart Disease Risk Based on Two Deep Neural Networks Trained on Well-Ordered Training Datasets. *IEEE Access* **2021**, *9*, 135210–135223.

[10] Dr.P. Golda Jeyasheeli, Dr.J. Raja Sekar, N. Indumathi , “AI Based Sign Language Recognition of Words Using Sensors”, International Journal of Advanced Science and Technology, 29(7s), 1713 – 1720, **2020.**

[11] Deepthi, L.Dharshana and Shanthi, D. and Buvana, M., An Intelligent Alzheimer’s Disease Prediction Using Convolutional Neural Network (CNN) (2020). International Journal of Advanced Research in Engineering and Technology (IJARET), 11(4), pp 12-22, 2020.

[12] S. V. Tathe, A. S. Narote and S. P. Narote, “Face detection and recognition in videos”, Proceeding in Annual India Conference (INDICON), pp. 1-6, 2018.

[13] Bhimanwar, Chinmay, Rupesh Biradar, Nikhil Bhole, and Milind Rane. "Face Identification." International Journal of Engineering Science 11923 (2018).

[14] Amna Qureshi, David Megias and Helena Rifa-Pous, "SeVEP: verifiable secure and privacy-preserving remote polling with untrusted computing devices", IEEE Access, vol. 7, pp. 19266-19290, 2018.

[15] Ms.Ashwini Ashok Mandavkar “Mobile Based Facial Recognition Using OTP Verification for Voting System” IEEE Access, vol. 7, pp. 19266-19290, 2018.