Online Voting System Using Face Recognition and OTP

Prof. S.B. Chaudhari
Professor, Department of Computer science
JSPM’s Jaywantrao Sawant College of Engineering, Pune, India.

Praapti Jagtap¹, Rafay Khan², Shraddha Shahane³, Tanishka Mane⁴
Department of Computer science
JSPM’s Jaywantrao Sawant College of Engineering, Pune, India.

Abstract—
Elections, in which voters may express their preferences and views by voting ballots, are the defining feature of all democracies. Over the years, the voting procedure has advanced significantly, moving from simple handwritten ballots to online voting systems. 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.” All of the voter data is stored on a server in a database. Before voting can start, a person must be positioned in front of a computer with a camera reading their picture. The desktop application programme is in charge of managing the person database. After casting a ballot, the "smart voting system" indicates that it has been counted. If the voter tries to cast a ballot again using a face sample, the desktop page will indicate that this is not possible. The election commission may then review the outcomes, reset the votes, and revise the candidate results yearly.

Keywords: Voting System, facial recognition, desktop page, machine learning

1. INTRODUCTION
In India, there are two types of voting systems: direct voting and indirect voting. The first technique, secret ballot paper, which required the use of a sizable amount of paper, has been in use since 2003. We must design a more secure means of conducting online voting since the current system is not adequately safe. In this suggested project, the idea of face detection and recognition is applied to identify the individual. In our suggested technique, the voters are examined at three different stages. When you get to the third level of security, the machine searches a database of pictures provided by the election commission for your face and recognises it. The verification of a unique identity number and the verification of an electoral commission identification number or voter card number make up the first two levels of security. You will be moved to level three, the greatest level of protection, if you confirm that the number on your voter card is accurate. Voters are only permitted to participate in an election if the photo they took corresponds to the image in the voter's record in the database. Otherwise, they won't be allowed to cast a ballot. Because the present system limits security to a voter card, anyone can use a voter card to cast a vote on someone else's behalf. On the other side, our team has developed a voting method that is far more secure than the current method.

1.1 Motivation: The voting machine gets a minor improvement every few decades. Conventional Electronic Voting Machines have a lot of faults, thus India’s Election Commission has taken a number of initiatives to enhance the system throughout the years. Skewed results, illegal activities at voting stations, and low attendance were still problems they had to cope with. Given how far technology has come, it makes sense to include it into the voting process. We must be able to meet the challenge that our society is currently experiencing as Future Engineers. As a result, we decided to use the Smart Voting System in an effort to help society as a whole. We are able to stop all of these instances of fake voting by using our sophisticated voting technology. This project proposes and implements a simple and secure voting process using a biometric sensor and cloud technology. By utilising the improvisations, model adaptability, security, reliability, and scalability are all enhanced. The citizen's fingerprints were already in the government's database. Therefore, this effort provides the best means of preventing fraud and high voter turnout through the use of electronic voting. The project's design is lightweight, adaptable, and power-efficient.

1.2 Problem Statement:
An online voting system is one that records, stores, and processes election data largely as digital information. As a result, voter identification and authentication methods are crucial for more secure platform mechanisms to get beyond the client vulnerabilities of the voter's voting device. Voter face recognition is employed as a new authentication method in the online voting system.

1.3 Objective and Scope of Project:
Finding a mechanism to boost voting in municipal, state, and federal elections is the project's main objective. As a result, we are striving to develop a voting system that enables individuals to cast their votes remotely while using their previously captured image face as identification. The objective of this study is to speed up facial recognition. In order to handle these challenges, as well as the computational complexity and time constraints, several approaches and strategies for feature extraction, normalisation, selection, and classification are required. It is possible to use
II. LITERATURE SURVEY

Ganesh Prabhu S. et.al. IEEE 2021 The suggested approach aims to eliminate every flaw in the conventional or present voting system by creating a safe online voting system based on facial recognition. Several strong characteristics of the suggested system include accuracy, verifiability, ease, and others. With this approach, voting may be done securely from anywhere without the need for an election official, a paper ballot, or any electronic voting equipment. All that is needed is an internet connection.

M. Kandan et.al. The complete internet infrastructure gives people the ability to safeguard their votes from anywhere in the world. By using ID based on looks, the likelihood of vote-copying is reduced, and only those who have registered to vote and are recognised by the system will be able to do so. In light of the methodology, selecting a framework is the best course of action.

S. Jehovah Jireh Arputhamoni et.al. Which is more effective and secure than the current method is covered in this journal. Voting takes less time and is less fraudulent than the previous system. No matter how old you get, distinctive traits like the space between your eyebrows and eyes never alter. While fingerprint characteristics cannot be altered, they can be shared by two people. Yet by utilising Tenprint photos of minutiae records, we can figure out whose voter fingerprint is in the database. Smart voting is a better method to vote since the planned system makes holding elections cheaper, easier, and less time-consuming.

Rajendra P Prasad et.al. High level biometric security is maintained with this project. The dataset directory contains the voter information. The user should stand in front of the computer before beginning the voting procedure so that the camera can interpret their image. After reviewing the information, the PC permits the authorised individual to cast their vote. A signal is then sent to the microcontroller, allowing the user to cast their vote without touching the EVM at all by simply hovering over the voting party. The person data is maintained by the application programme. Once a voter casts their ballot in the “smart voting system,” the controller notifies them that their vote was correctly registered.

S Ganesh Prabhu et.al. This study focuses on a system that allows users to cast ballots remotely from any location using a computer or a mobile device and eliminates the need for voters to physically travel to the polling place through two-step verification utilising facial recognition and an OTP system. The user may also choose to vote offline through this project if they feel more comfortable doing so. The face scanning system is used to capture images of voters' faces before the election and is helpful while casting a ballot. Instead of voter identification, the offline voting method is improved with the use of RFID tags. Moreover, this technology allows users and citizens to view the results at any moment, preventing circumstances that may lead to vote rigging.
D. Admin: Administrators must sign into the system. Election party information and logos are managed and manipulated by the admin. Admin can also show the outcome.

3.3 Algorithms

1. HARR CASCADE ALGORITHM:

The main building block for Haar classifier object recognition is a set of Haar-like characteristics. It modifies the contrast values between consecutive rectangular pixels in instead of utilising the pixel's intensity values pixels in groupings. Using contrast variances between pixel groups, it is possible to detect how bright and dark a region is relative to another. Two or three neighbouring groups with relative contrast variance combine to generate a Haar-like feature. By simply raising or lowering the size of the pixel group, it is simple to scale the Haar characteristics, allowing them to be applied to objects of different sizes. With subimage analysis, which enables the cascade of classifiers, the maximum likelihood of analysing the Haar-features that differentiate an item is achieved. It permits only one change in a classifier's accuracy. It is possible to increase false alarm and positive alert rates while lowering the number of phases. This method, developed by Viola and Jones, used 200 straightforward characteristics to recognise human faces with 95% accuracy. First, the Haar classifier cascades need to be trained to recognise human face characteristics such the lips, eyes, and nose. As for the training of the classifier, a moderate AdaBoost algorithm must also be used. However, Intel has created the Open Computer Vision Toolkit, an open source library that facilitates the construction of computer vision-related applications (OpenCV).

![Fig. Types of Harr features(www.willberger.org)](image)

2. LBPH:

A discernible descriptor style used for computer vision classification is called local binary patterns (LBP). LBP was made into a special case from the 1990 Texture Spectrum model. The first time LBP was represented was in the year 1994. As a result, it has been utilised as a texture for identifying solid components. Combining LBP with the descriptor histogram of directed gradients improves the execution of identification on specific datasets (HOG).

To encode features, the input picture is partitioned into cells (4 × 4) of pixels. By carrying the surrounding pixel values either clockwise or anticlockwise, the contrast is achieved. Every neighbor's intensity value is compared to the value of the focal pixel. The location has been given a 1 or a 0 depending on whether the difference is higher or lower than 0. The results are an 8-bit value in a single cell.

![Fig. LBPH face recognizer](image)

IV. RESULT AND DISCUSSION

Our suggested approach combines facial identification with machine learning to enable voters to register and cast ballots from any location, regardless of where they are. This technique offers security and prevents one individual from casting numerous votes. This approach, in which we may cast our votes from many locations, is more dependable. It also reduces human and labour work needs and available time.

#### add you project screenshot here####

V. CONCLUSION

The suggested method attempts to address every flaw in the present or conventional voting system by developing a secure internet voting system based on otp authentication and facial recognition. It also offers a lot of powerful characteristics, like verifiability, practicality, accuracy, etc. The sole requirements for this system are an internet connection, a cell phone for otp authentication, and a desktop or laptop with a camera for face authentication. This allows voters to cast their ballots safely from any location.

REFERENCES

4. Z.A. Usmani, KaifPanwanla, MukeshPanigraphi, Ajay Nair “Multipurpose platform independent online voting system.

