IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Face Recognition Based Online System

[1]Jatin Kumar, [2]Neha Veer, [3] Zeel Shah, [4]Saanvi Balki, [5] Prof.Sonali Dhamele

[1,2,3,4]Student, Department of Computer Engineering, Terna Engineering College, Navi Mumbai, India

[5]Professor, Department of Computer Engineering, Terna Engineering College, Navi Mumbai, India

***Abstract***: An online voting system integrating facial recognition enhances voting security and accuracy. It verifies voters' identities, restricting participation to eligible individuals, and eliminates the need for physical polling stations, enhancing accessibility and reducing costs. The system features authentication of voter identities, secure vote storage, and fraud prevention. Object detection employs Haar feature-based cascade classifiers and Local Binary Pattern (LBP). The server cross-references data with the database, granting voting permission upon matching and notifying in case of discrepancies. In Conclusion, this system has the potential to revolutionize elections by increasing efficiency, security, and accessibility.

***Index Terms*** **- Face Recognition, Haar Cascade, LBPH, User Authentication**

## I. INTRODUCTION

Voting serves as a means for groups to collectively reach decisions or voice opinions, manifesting in diverse formats. Among notable innovations in voting technology stands online voting, commonly referred to as E-voting, which has revolutionized conventional voting methodologies. The integration of biometrics within E-voting represents a significant leap forward, offering heightened security measures compared to the inherent vulnerabilities of paper-based voting systems, particularly in democratic societies.

In this research, we introduce an online voting system that employs facial recognition technology for casting votes securely. The facial data is transmitted to the server for verification. The server then cross-references this data with the existing database. If a match is found, the individual is granted permission to vote; otherwise, an error message is displayed, and the individual is denied voting privileges. Traditionally, voting representatives are designated by the electorate, and voters are required to present their voter ID cards at polling booths, a process prone to delays due to verification procedures. To streamline this process and mitigate such issues, our proposed system aims to expedite voting procedures while ensuring security and accuracy.

## II. RELATED WORK

In [1] Smart Online Voting System the proposed system enables remote voting via computer or mobile phone, eliminating the need for physical presence at polling stations. Authentication involves a two-step process: face recognition and OTP verification. Offline voting utilizes RFID tags instead of traditional voter IDs. This enhances efficiency and transparency, allowing citizens to view election results anytime to prevent vote tampering.

In [2] Online Voting System Using Cloud aims to transition from manual voting to online voting systems due to concerns of malpractices in manual methods. Our specific focus is on implementing an online voting system with features tailored to schemes implemented by political parties. This shift allows for time-saving and location-independent voting. The system is developed using C#, Microsoft SQL Server 2012, and Microsoft Azure cloud services.

In [3] Multi-purpose platform independent online voting system various techniques such as Paper Ballot Voting, Electronic Voting, Internet Voting, and SMS/Missed Calls Voting are employed. This paper examines these methods, discussing their pros and cons. The aim is to develop a versatile, cross-platform voting system compatible with any operating system. The voting system is essential for democracy and has evolved significantly over the years.

In [4] Blockchain based E-voting system, E-voting with blockchain technology provides a secure and transparent alternative. Our proposed system uses Ethereum network and Solidity programming to enable voters to select candidates for major and general elections. Votes are securely stored on the Ethereum blockchain, ensuring integrity. Users can vote directly from their Ethereum wallets, enhancing security and affordability of online voting.

[5] A biometric-based Secure Electronic Voting System Using Face recognition. This research proposes using fingerprint sensors for voter registration and authentication to prevent misuse of votes. Voter fingerprints are stored in a database to avoid multiple registrations. During voting, individuals scan their fingerprints for authentication against the database, reducing duplicate registrations. Voters can cast their ballots worldwide using unique identifiers and authentication responses provided during enrollment. Tokens are sent to candidates' email addresses for access. This project has been successfully implemented.

In [6] Web Based Voting System the system enables voters worldwide to cast their votes using a government-assigned IP address. Voters register their name and address on the website, providing fingerprint and face images to the Election Commission for authentication. Images are stored securely and compared on Election Day for secure voting. The system uses facial and fingerprint recognition, like mobile phones, reducing the need for physical presence and saving time. This approach also minimizes fake voting by detecting facial and fingerprint anomalies, ensuring system security.

## III. PROPOSED METHODOLOGY

### 1. Open CV

Open Source Computer Vision Library is a popular open-source computer vision and machine learning software library. It provides a wide range of tools and functionalities for tasks such as image and video analysis, object detection and recognition, facial recognition, feature extraction, and more. OpenCV is widely used in various fields including robotics, augmented reality, medical imaging, and surveillance systems. Its versatility, efficiency, and extensive documentation make it a preferred choice for researchers, developers, and engineers working on computer vision applications.

### 2. Haar Cascade

Object Detection using Haar feature-based cascade classifiers is a robust method for object detection. This approach relies on machine learning and involves training a cascade function with numerous positive and negative images. Subsequently, this trained function is utilized to identify objects in other images. Each feature is computed as the difference between the sum of pixels under a white rectangle and the sum of pixels under a black rectangle.

F(Haar)=∑ F white-∑ F black

∑ F white = Sum of pixels of bright area

∑ F black = Sum of pixels of dark area F(Haar) = the Haar like feature

### 3. LBPH Algorithm

The Local Binary Pattern (LBP) algorithm is a straightforward yet highly effective texture operator used in image processing. It assigns labels to the pixels of an image by comparing the pixel intensities in the neighborhood of each pixel. This comparison results in a binary number, which is then converted to a decimal value and assigned to the central pixel of the matrix. In the original LBP operator, a 3x3 patch is considered, resulting in an 8-digit binary number formed by the surrounding pixels. Once all pixels in the image are labeled, a histogram with 256 bins is generated, representing the LBP feature map. This histogram can serve as a feature vector for classification, with each bin representing a distinct feature. The formula for computing LBP is given by LBP P,R (xc,yc) = Σ from 0 to P−1 (gp−gc)2p, where P is the number of pixels in the neighborhood, R is the radius of the circle, xc and yc are the coordinates of the center pixel, gp is the intensity of the neighboring pixel, and gc is the intensity of the central pixel.

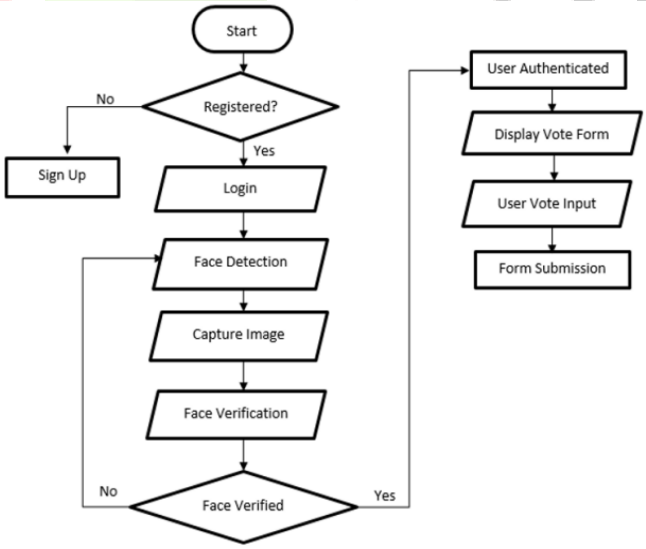



**Fig. 1: User Module Architecture**

Fig.1 uses face recognition to verify user's identity based on their facial features.

Here's a step-by-step explanation of the flowchart:

1.Start: This is the entry point of the process where a user begins the action of voting.

2.Registered?: This decision point checks if the user is already registered in the system.

If No:

Sign Up: The user is prompted to sign up and register in the system.
If Yes:
Login: The user logs in to the system, which is the first step in the authentication process.
3. Face Detection: The system detects the user's face as part of the authentication process.
4. Capture Image: The system captures an image of the user's face to be used for verification.
5. Face Verification: The captured image is compared against the registered facial data to verify the user's identity.
If No (Face not verified):
The process may loop back to the "Face Detection" step or end, depending on the system's design, to allow the user to try again or to take alternative actions.
If Yes (Face verified):
User Authenticated: The user is successfully authenticated and can proceed to the next steps.
6. Display Vote Form: The authenticated user is presented with the voting form to make their selections.
7. User Vote Input: The user inputs their vote on the form.
8. Form Submission: The user submits the completed voting form.
The flowchart ends with the form submission, indicating that the user has successfully cast their vote. This flowchart is useful for understanding the steps involved in a facial recognition-based voting system, ensuring that the process is secure and that each step follows logically from the previous one.

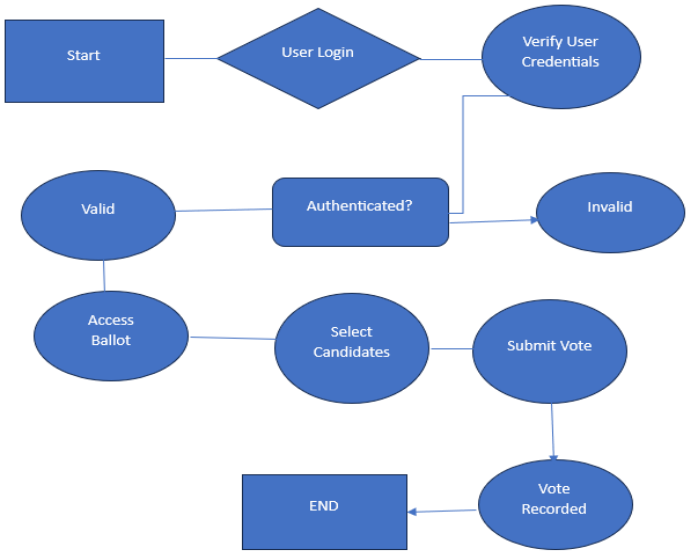



**Fig. 2: Admin Module Architecture**

Fig.2 uses username & password or other forms of authentication to ensure that only authorized administrators can access the admin interface.

Here's a step-by-step explanation of the theory or logic behind the flowchart:

1. Start: This is the entry point of the process where a user begins the action of voting.
2. User Login: The user is prompted to log in to the system, which is the first step in the authentication process.
3. Verify User Credentials: The system checks the credentials provided by the user to ensure they are valid.
4. Authenticated?: This decision point determines the path of the process based on whether the user is authenticated or not.
If the credentials are Valid:
Access Ballot: The user gains access to the ballot to proceed with the voting process.
Select Candidates: The user selects the candidates they wish to vote for.
Submit Vote: After making their selection, the user submits their vote.
Vote Recorded: The system records the vote.
END: The process concludes after the vote is recorded.
If the credentials are Invalid:
The user is presumably taken back to the "User Login" step to try logging in again, or they may be given a certain number of attempts before being locked out or required to go through a recovery process.
The flowchart ends with the vote being recorded, indicating a successful completion of the voting process. This type of flowchart is useful for designing and understanding the steps involved in an electronic voting system, ensuring that the process is clear and that each step follows logically from the previous one.

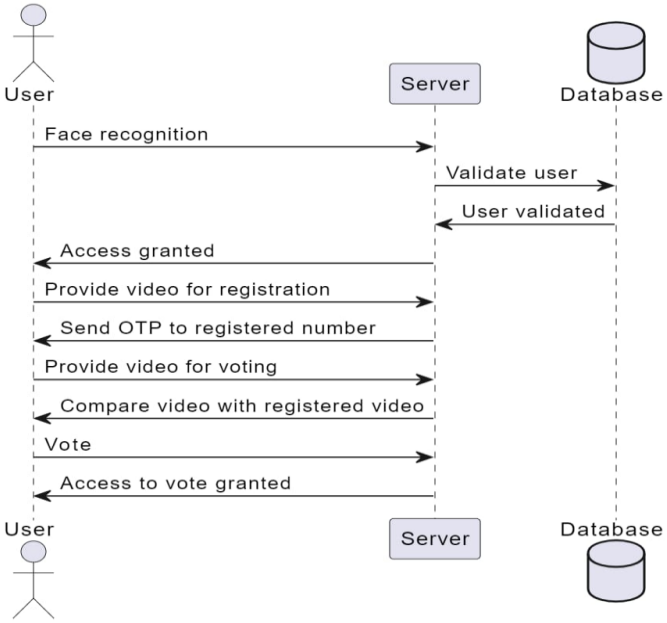



**Fig. 3: Sequence Diagram**

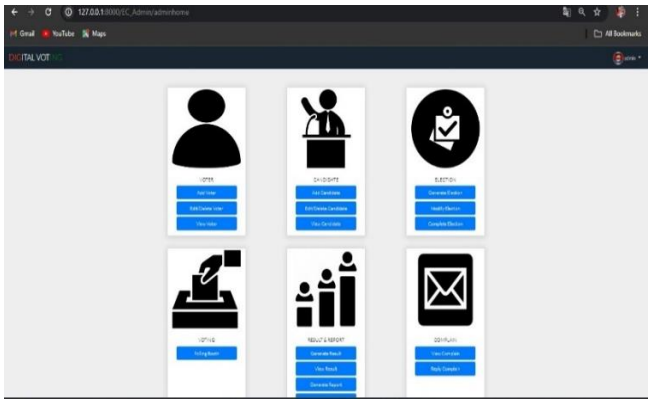
Fig.3 shows the different components of online smart voting system work together to provide user friendly voting experience.

The process flow is as follows:
• The User initiates the process with a Face recognition request to the Server.
• The Server processes the request and performs a Validate user operation, likely by comparing the user's face with stored data in the Database.
• Once the user is validated, the Server sends an Access granted response back to the User.
• The Server then provides a Provide video for registration message, prompting the user to submit a video for registration purposes.
• The Server sends an OTP (One-Time Password) to the user's registered number to further verify their identity.
• The Server provides a Provide video for voting message, which is another step in the authentication process.
• The User submits a video, and the Server performs a Compare video with registered video operation to ensure the person attempting to vote matches the registered user's video.
• If the comparison is successful, the Server sends a Vote message, indicating that the user is now authorized to cast their vote.
• Finally, the Server sends an Access to vote granted message to the User, completing the authentication process, and allowing the user to proceed with voting.
This sequence diagram illustrates the interactions between the user, server, and database in a secure voting system that uses both face recognition and video verification to authenticate users before they are allowed to vote.

## E. OUTPUT RESULTS

Initially, users are required to register in the system by providing details such as Aadhaar number, mobile number, city, age, and password. This information is stored in the voter dataset. During registration, the system captures the user's image using a webcam, which is then stored in the face dataset for template matching. To cast a vote, users must log in to the system by entering their Aadhaar number and password.

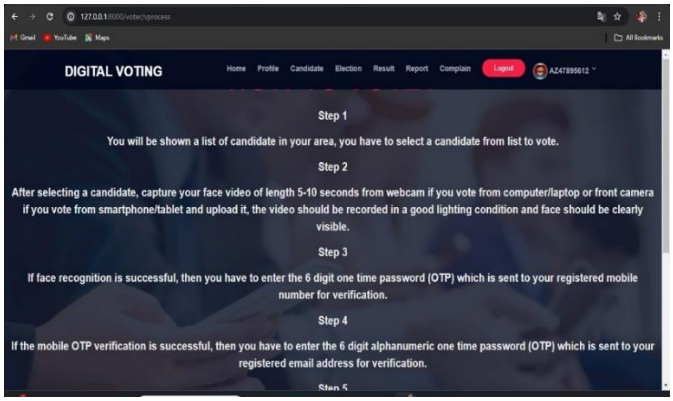
For efficient detection and recognition, a high-quality camera is necessary to capture video. The video is then converted into multiple frames to enhance accuracy in producing results. Facial recognition involves identifying or verifying an individual's identity using their face. Facial recognition systems are utilized for identifying people in photos, videos, or in real-time, making them a category of biometric security.



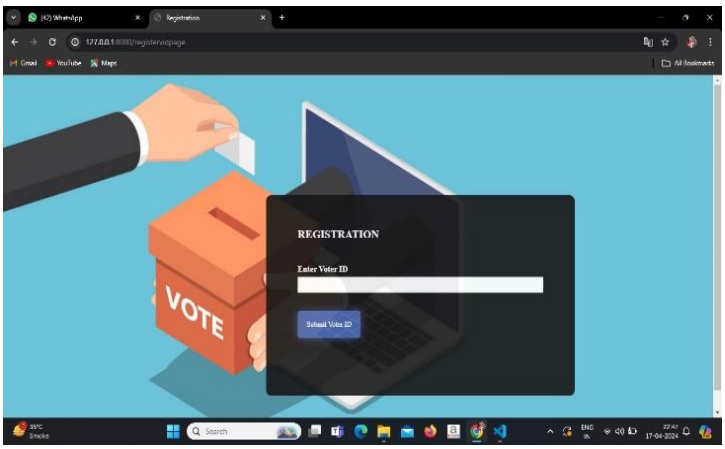
HOME PAGE


REGISTRATION & LOGIN

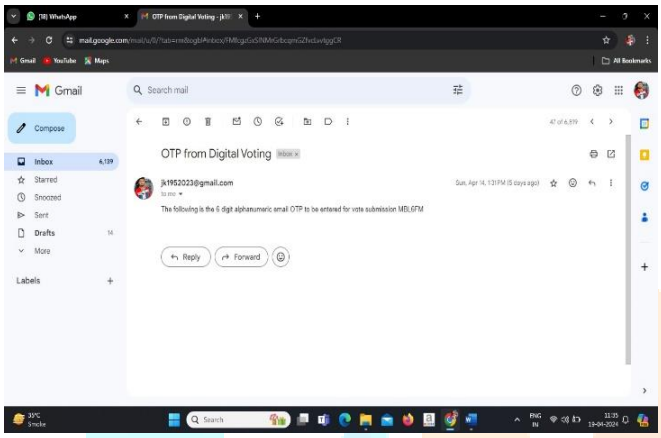
INTERFACE



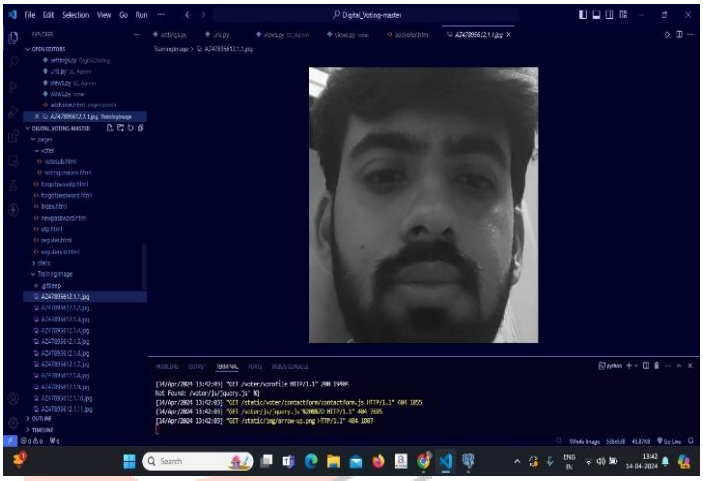

VOTING GUIDELINES




CREDENTIALS FOR VOTING




OTP RECIEVED ON EMAIL



MODEL BUILT USING OPEN CV


## IV. CONCLUSION AND FUTURE SCOPE

Currently, our government allocates over 125 crores for conducting Lok Sabha elections, primarily for security and electoral ballots. However, the voter turnout averages less than 60%, with potential for voting fraud. Moreover, the percentage of literate individuals participating in voting is low. Our proposed system aims to significantly reduce election expenditure to less than 10 crores while eliminating voting fraud and minimizing security costs. With our system, individuals with internet access and a webcam can vote from the comfort of their homes, eliminating the need to visit voting booths. Implementation of an online voting system using facial recognition technology promises increased accessibility, convenience, and security in the electoral process. This technology ensures voter identity verification, fraud prevention, and a seamless voting experience. It's imperative to design the system to safeguard voters' privacy and security while avoiding bias or discrimination. Providing alternative options for individuals uncomfortable with facial recognition technology is essential. Overall, an online voting system utilizing facial recognition holds immense potential for improving the electoral process.

The potential for an online voting system utilizing facial recognition technology is vast and promising. As facial recognition technology evolves, we anticipate higher accuracy rates and enhanced reliability in verifying voter identities, ensuring the integrity of the voting process. Integration of blockchain technology can further enhance security and transparency in voting, creating a tamper-proof system that ensures accurate and transparent results.

User experience plays a crucial role in the success of an online voting system. Future advancements in design and user interface can make the voting process more user-friendly and intuitive. Facial recognition technology also holds potential beyond the electoral process, with applications in sectors such as banking, healthcare, and education, enhancing identity verification and security.

Overall, the future of online voting systems utilizing facial recognition technology is promising, with further development and integration expected in the years ahead.

**REFERENCES**

[1]. K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1-4.
[2]. S. S. Kadam, R. N. Choudhary, S. Dandekar, D.Bardhan and N. B. Vaidya, "Electronic Voting Machine with Enhanced Security," 2018 3rd International Conference on Communication and Electronics Systems (ICCES), 2018, pp. 403-406.
[3]. R. Rezwan, H. Ahmed, M. R. N. Biplob, S. M. Shuvoand M. A. Rahman, "Biometrically secured electronicvoting machine," 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 2017, pp. 510- 512. [
4]. Z. A. Usmani, K. Patanwala, M. Panigrahi and A. Nair, "Multi-purpose platform independent online voting system," 2017 International Conference onInnovations in Information, Embedded andCommunication Systems (ICIIECS), 2017, pp. 1-5.
[5]. K. H. S, B. G. B, H. M. P, A. D. L and A. V, "Secured And Transparent Voting System Using BiometricAnd Face Recognition," 2021 International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C), 2021, pp. 254-259.A. A. Mandavkar and R. V. Agawane, "Mobile based facial recognition using OTP verification for voting system," 2015 IEEE International Advance Computing Conference(IACC), 2015, pp. 644-649.
[6]. S. Wattamwar, R. Mate, P. Rainchwar, S. Mantri and G. Sorate, "Optimal Face Recognition System using Haar Classifier," 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), 2021, pp. 1-7
[7] Das, M. Wasif Ansari and R. Basak, "Covid-19 Face Mask Detection UsingTensorFlow, Keras and OpenCV," 2020 IEEE 17th India Council International Conference (INDICON), 2020, pp. 1-5, doi: 10.1109 /INDICON 49873.2020.9342585.