

Smart Voting System Support through Facial Recognition

Dr. Ramya C¹, Harish L² and Dr. Bharathi Gururaj³

¹⁻²Department of ISE, CMR Institute of Technology, Bengaluru, Karnataka, India
Email: {¹ramya.c, ²harish.l}@cmrit.ac.in

³Department of ECE, ACS College of Engineering, Bengaluru, Karnataka, India
Email: ³bharathigururaj@gmail.com

Abstract—In India, currently there are two types of voting mechanisms in practice, i.e. Secret Ballot paper and Electronic Voting Machines (EVM). Both of these systems have some of the limitations, hence the existing system is not so secure and safe for voting. The voting system method is time consuming and inefficient. In the existing voting system methods, the voters should go to far places in order to find polling booths and stand for a long time in a very long queue in order to cast their valuable vote, due to which most of the people do not show interest to cast their votes. Due to less security, the people who are ineligible to vote also try to cast their votes which may lead to false voting. To resolve all the above issues, a new system is proposed and in which voting method is very convenient and effective. The technique that has been proposed has three different levels of security to cast vote. The first and foremost level is the verification of unique id number (UID), second is the voter id number verification (EID) and third and the most important level is face recognition. The authentication of the user in the system is improved and enables authenticated users to cast their votes by using face recognition in the application, which will be able to identify whether the user is authenticated user or not.

Index Terms— Voting Systems, Face Recognition, Haarcascade and LBP classifier.

I. INTRODUCTION

The power of vote for the country is an important part of a democratic country like India. There are mainly two techniques that are being used for voting purposes nowadays. The first technique is the secret ballot paper in which voter's identity is secretive and the second one is EVM (Electronic Voting Machine) in which an instrument is used for voting purpose. Here, a methodology has been proposed, which is more secure than the existing voting system and in which facial recognition is the primary concept used to identify the person. This has three different levels of verification for the voters in order to provide secure voting. The first and foremost level is Unique ID number verification, second is election commission ID or voter card number and the third level of security is the main security level where the system recognizes the face of the voter from the database of facial images that are stored in the current database. If the two images match with the image of the voter in the database and the real image, then a voter is eligible to vote. The existing system is not much more secure because any one can carry other person's voter card and cast a vote for other person. But in this proposed system, the false voting can be eliminated which makes it more secure and reliable than the current existing system.

II. LITERATURE SURVEY

This section briefly describes some of the recent related carried out by different researchers and with different methodologies and techniques. Baumberg et. al. has presented robust method for matching automatically the features in images corresponding to some physical point on an object seen from the two arbitrary viewpoints[2]. Unlike conventional stereo matching approach, the author assumes no knowledge about the cameras positions and orientations. The Features are matched using affine texture invariants in two or more images. Problem is explicitly addressed by the method where feature characters are invariant of linear transformation of the image data. Feature matching process is optimized for application where we wish to ignore matching at the expense of reducing number of matching features. P. Belhumeur, J. Hespanha, and D. Kriegman et. al [7], studied that the focus is given on the comparison of the Eigen face vs the fisher face. Since both of them have computational requirements similar to each other but yet the exclusive experimental results have shown that the fisher face has error rates lower than that of the Eigen face method. So this leads to the development of an algorithm that is insensitive to the light variations and the expression of the face. This allows us to observe every pixel of the image in the different light variations and no fixed poses while the image recognition and processing. Here, the images are projected in the opposite way to that of linear projection and this has produced the results better in comparison to the Eigen face. So It has been concluded as the fisher face is comparatively a better idea to face recognition method.

P. Viola et. al. analyzed that face is the important part of a person and it reveals prominent features of a person[11]. Due to its security controlling applications, in the past few years, face detecting has become famous biometric character. Real-time detection of face in frames is the first step in the experimental facial analysis which consists of the faces and complicated elements in the background. Here, a system is proposed for human face detection using Haar features and recognition using Eigen and Gabor filter in videos. Efforts are made to minimize processing time for detection. So in this work, Eigen values are used as they perform very well in the computational complexity as compared to the Gabor Filters. Q. Tao et.al. capturing or recognizing the criminal or suspect which will help the policemen in detecting the right person who is the criminal or suspect by making use of the real time video [9]. The client side face detection is done by making use of any android mobile and at the server side of the application the face is detected against the video based recognition of the face. In this work, the framework is a client-server video based facial recognition which is under surveillance in the real-time. Robust Viola algorithm has been used which is not dependent on the light variations and produces best results in the case of variation of light during the face recognition process.

Nilam Choudhary, Shikhar Agarwal and Girija Lavanya has also provided a study based on comparisons of Fisher faces, Eigen Faces and Speeded Up Robust Features algorithms and they did performance comparison based on how the classification of faces are done in images and the training is done with 2,316 images with 4 samples of image making a total of 9,264 images. The results of the research were as such that the accuracy of Eigen Face is 77%, Fisher Face is 80% and SURF is 88%. They also analyzed that the Speed Up Robust Features algorithm works better only if the images has features which are similar to that of data. Nandan Gowda and Deepak Laman made a analysis that this model has to be built on Adhar and web based system of voting using recognition of face which provides levels of security which are very high. The details of the voter are stored in a computer for which the voter should wipe the RFID card before entering the place and a character will be sent by the RFID reader.

Mahalakshmi MAbala Naik and Preethi suggested that this system must undergo registration of the user first and next levels of verification will be done later. User ID verification and voter ID verification is done simultaneously and this data is stored and it should be same as the database. The recognition of face will be done in the next stage which is the crucial part of the system. And next that person will be able to cast their valid voter. This system uses algorithm of Haarcascade which uses features which are rectangular of haar which is used to find out the white and black slides of image of gray-scale. A Gnana Saravanan stated that including web based technologies such as creation of database and processing of image. These sites will be handled by the government and only verified users will be able to cast their votes. Here the security levels are of finger print and recognition of face. The voter will be able to open the website only on election day and the server stores the finger prints and images of the face received from election commission. When the website gets opened the finger print and face will be captured and that person can vote to any party and this process can be done using any of the devices such as laptop or mobile etc.

Lakshmisha Rai and Amila Rodrigo made an analysis on a real time platform which is robust for mobiles which doesn't have that much computation power and memory when compared to PC platforms and this involves combining two precious implementations and this is said to be robust for different or similar face poses. The

results of the real time system indicate both robustness and capabilities of real time for the hybrid face detection solution.

III. PROPOSED SYSTEM

Many people can show interest towards voting if online voting facility is provided. This saves a lot of voting time and due to the improved security mechanisms, one can always rely on online smart voting system. It uses less man power and resources when compared to the existing system. Considering the problems noticed in existing voting systems and to propose the new solutions for the same, we switch to online smart voting system.

The proposed online smart voting system works with three different security layers which are as follow:

Level 1: *Unique id number (UID)*. This layer will request for the unique ID of a voter which is given at the registration step and is verified from the existing database.

Level 2: *Voter ID card number*. In this verification level, voter ID number has to be entered by the voter which is verified against the server database.

Level 3: *Face recognition*: In this level, The facial image of the voters is recognized by using Haarcascade facial algorithm in order to verify from server databases.

The first two levels are to deal with UID and voter ID. The third level is the facial recognition which uses the algorithm called Haarcascade. Haarcascade is very unique and more secured which was proposed by paul voila and M jones. It is based on the approach of machine learning where a function is trained on more positive and negative images. Based on the training results, its used to detect the other image objects. The image is first loaded and then converted to gray scale to make processing easy. The first stage is detection of the face where various images of a person should be taken and be stored as a dataset format in the form of gray scale images with dimension 152X152. After this conversion process, each image should be labelled accordingly. After the images are trained , numpy arrays are generated. A training classifier file must be saved to test the dataset. It recognizes the image and now at this stage, Haarcascade classifier is used to identify the objects within the images and if the face is recognized, then only the particular individual can vote accordingly.

IV. WORKING OF THE MODEL

The first step for the new user for voting is to get registered in the portal. In the Registration step, the person who wants to vote has to undergo the process of face recognition which is done by using Web Camera and then the captured image samples are stored for security and detection purposes in the server database. After the successful registration, the three level security includes verification of unique ID, verification of voter ID followed by facial recognition. If both the IDs are unique then vote entered by the voter will be crosschecked for its correctness. If both the IDs match successfully then the voter will be allowed to take his images. This will be matched with the respective server images which are already present in the database set.

Face Recognition will be done using the HaarCascade Algorithm. The user will be allowed to vote only if his image matches successfully with the server images stored in databases. Later, voting desk page will arrive which contains the list of all the parties participating for Election. Voter can cast his /her vote by voting the party of their interest in the election. Next, the voter will give his vote to the deserving party and he will be logout automatically so that he can cast only one vote.

V. PROPOSED SYSTEM

The application can be used for various circumstances and purposes such as viewing the number of candidates and their respective profiles, view the results of election from past years and so on prior the election day. On the election day, use of one more application is made to perform various voting operations which will be only made available to the government sites that are authorised only for eligible users. Then the application can be moved into users mobile phone by installing it from the site. By opening and authenticating the user with the application, he/she will be able to move forward to cast a vote. Next, the face recognition security technique verifies the user that whether he is eligible or not to vote.

VI. METHODOLOGY

A. Face detection

The recognition of each face present in an image is the major task of the face detection and is implemented using OpenCV. The steps are as follows:

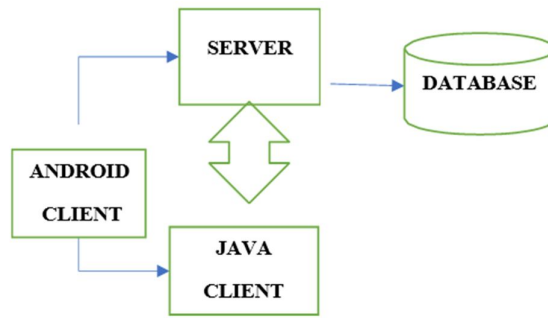


Figure 1. Block Diagram of Voting System

- Load the images.
- Convert the input images into grey scale images.
- Apply the Haarcascade and LBP classifier.
- Compare both classifiers based on the accuracy and time.
- Import the required libraries.
- Take the images which we captured by the camera.
- Convert into grey scale image to process the image through the classifiers.
- Load the image using OpenCV.
- Image will be loaded into BGR color-space by default

B. Haar Cascade Classifier

- Load the input image using built in function `cv2.imread(img_path)`, by passing the image path as an input parameter .
- Convert it to grey scale mode and then displaying it.
- Load the Haar cascade classifier.

First an image of the person is taken from the camera. Then the images taken are converted to gray scale images. Faces are then detected using cascade classifier which is a function of OpenCV. The eyes of the face gets detected under various lighting circumstances and if the face gets recognized then a face sample is collected and sent for training the images. If the face is not detected then the face won't be recognized and hence that person is unable to vote. Suppose one person sits for capturing image and other person sits for facial recognition that person will be labeled as unknown and further he/she won't be able to cast the votes and hence this facial recognition is enough secured than the existing system.

VII. RESULTS

The admin should enter the details and is used for valid authentication of voter, valid user id, voter id, face recognition. If it is valid, then the candidate is allowed to vote. Fig. 4 shows the registration module for admin and users.

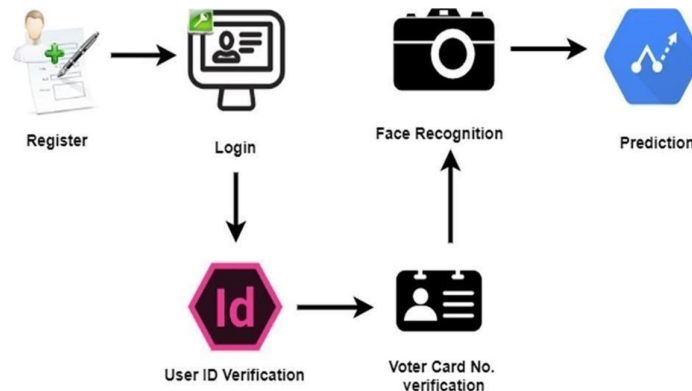


Figure 2. Basic Architecture of Smart Voting System

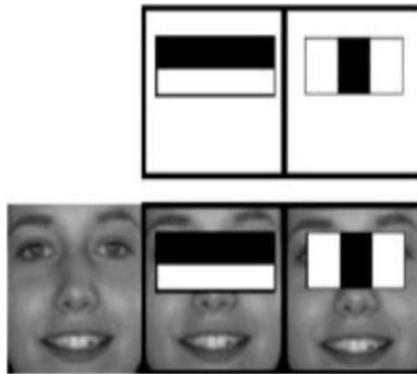


Figure 3. Haar Like Features



Figure 4. Registration Module (Admin and Users)

This module is for the users who undergo a registration process for voting. The users can be viewed who have already registered from the Users module. The registration process includes filling all the necessary details. An OTP will be generated for security purpose. Fig. 5 shows the register here and view voter list. Fig. 6 shows the voting module for face authentication and Vote here. For voting purpose users have to undergo a face authentication process. This allows users to vote for a particular party. After successful voting, a window will pop up as “Thank you for your vote” and the voter will be logged out of the system in order to avoid more than one vote. This is shown in Fig. 7.

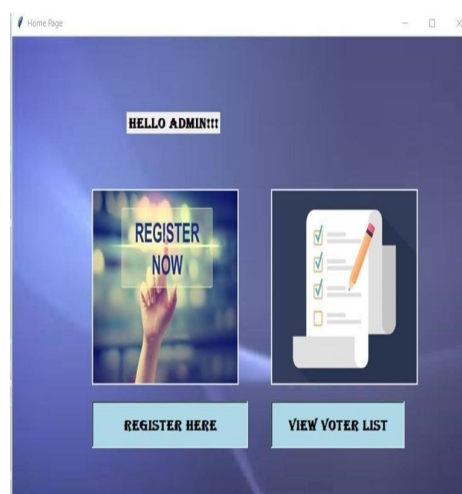


Figure 5. Register Here and View Voter List

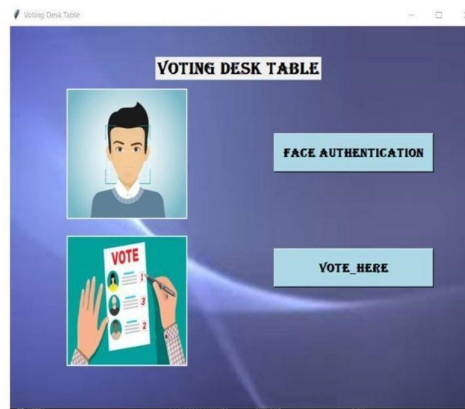


Figure 6. Voting Module (Face authentication and Vote here)

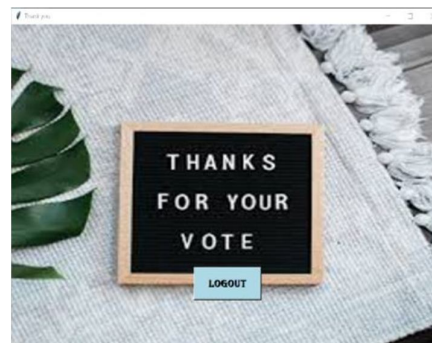


Figure 7. Logging out Window

VIII. DISCUSSIONS

Since the current methods of voting have a lot of demerits such as voting is lengthy, counting of voting is time consuming process, no security layers to eliminate false voters and so on. This makes the presented approach the best over the existing system. In this approach three layers of security is deployed at each level. The face recognition is the most important layer which identifies all the fraud voters and filters out the authenticated users only who are eligible to vote. The greatest advantage of this system is that the users can remotely cast their vote without having to go to the voting booth by using a simple application. This is quiet useful as it increases the percentage of people voting for a party as most of the aged people couldn't cast vote because of having to go to a far place just to cast vote.

IX. CONCLUSIONS

The loopholes of the current existing voting system such as time consuming, cost inefficient, insecure and false voting mechanism, provoked to find a new approach of voting system which is very much secure and eliminates all the elements of false voting. In this approach, three layers of security is deployed at each level. The face recognition is the most important layer which identifies all the fraud voters and filters out the authenticated users only who are eligible to vote. The greatest advantage of this system is that the users can remotely cast their vote without having to go to the voting booth. This also requires less manpower and resources to carry out the voting process. Voting data is stored and retrieved from a database which is managed centrally. It needs to be updated every minute and should be consistent. The new and eligible voters need to be added into the database and the ones who are dead must be removed to maintain data coherency.

REFERENCES

- [1] J.Deepika,S.Kalaiselvi,S.Mahalakshmi and S.AgnesShifani "Smart Electronic Voting System Based On Biometric IdentificationSurvey:2017", Third International Conference on Science Technology Engineering & Management

- (ICONSTEM), pp. 939-942, 2017.
- [2] Sanjay Thakre, Ambikesh Kumar Gupta and Shilpi Sharma, "Secure Reliable Multimodel Biometric Fingerprint and Face Recognition", International Conference on Computer Communication and Informatics (ICCCI -2017), Coimbatore, INDIA, Issue: January 2017, pp. 95-99, January 2017.
 - [3] Edy Winarno, Wiwien Hadikurniawati, Imam Husni Al Amin and Muji Sukur, "Anti-Cheating Presence System Based on 3WPCA Dual Vision Face Recognition", EECISI 2017, Yogyakarta, Indonesia, pp. 121-124, September 2017.
 - [4] Amish Basal, Utkarsh Raina, Vaibhavi Pujari and Roushan Kuma, "E-Smart Voting System with Secure Data Identification using Cryptography", 3rd International Conference for Convergence in Technology (I2CT), India, pp.1-4, April 2018.
 - [5] Vikas Kumar, MS Swetha, MS Muneshwara and S Prakash, "Cloud computing: towards case study of data security mechanism", vol-2 issue-4 pp. 1-8, 2011.
 - [6] MS Muneshwara, MS Swetha, M Thungamani, and GN Anil, "Digital genomics to build a smart franchise in real time applications", IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT), pp. 1-4, 2017.
 - [7] A. Baumberg, "Reliable feature matching across widely separated views", CVPR, 2000.
 - [8] P. Belhumeur, J. Hespanha and D. Kriegman, "Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection", IEEE Transactions on Pattern Analysis and Machine Intelligence, pp.711-720, 1997.
 - [9] F. Song, D. Zhang, J. Wang, H. Liu, and Q. Tao, "A parameterized direct LDA and its application to face recognition," Neuro computing, Vol.71, 2007.
 - [10] Kashif Hussain Memon, Dileep Kumar and Syed Muhammad Usman, "Next Generation A Secure EVoting System Based On Biometric Fingerprint Method", 2011.
 - [11] P. Viola and M. J. Jones, "Robust real-time face detection," International Journal of Computer Vision, Vol. 57, pp. 137-154, 2004.
 - [12] Nilam Choudhary, Girija Lavanya and Shikhar Agarwal, "Smart Voting System through facial recognition", Isroset-Journal, Vol.7, Issue.2, pp.7-10, Apr-2019.
 - [13] Nandan Gowda S H, Jayam Hareesh Tharun, Ashik B M, and Deepak Lamani, "Smart Voting System using face recognition", IRJET, August 2020.
 - [14] Mahalakshmi MAbalaik, DR. Preethi N Patil. "Smart Voting system through face recognition", IJCRT, May 2020.
 - [15] S. Jehovah Jireh Arputhamana M.E and Dr. A. Gnana Saravanan, "Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection on Image Processing", CNN-IEEE, 2021.
 - [16] Lakshmisha Rai, Amila Rodrigo and Zhiyuan Wang, "A hybrid faces detection approach for real-time deployment on mobile devices", International Journal of Interactive Mobile Technologies, March 2020.