E-Voting For Universities Using Face Recognition

Addepalli Lakshmi Venkata Sai Kumar[1], Mandapaka Kundana[2]
Palisetty Sandhya[3], Edupalli Tarun Rohit[4], K. Udayasri[5]
[1,2,3,4]Student,Department of CSE, NRI INSTITUTE OF TECHNOLOGY, Vijayawada, A.P., India.
[5]AssociateProfessor, Department of CSE, NRI INSTITUTE OF TECHNOLOGY, Vijayawada, A.P., India.

Abstract

This report describes an online voting system designed to meet the needs of colleges and universities. Voting is a widely spread, democratic way of making decisions and can be used for electing student presidents and class representatives at the college level. The main objective of the proposed system is to develop a more secure and user-friendly voting system compared to the existing methods. The process of voting is critical in terms of safety and security. The proposed system allows the voters to scan their faces, which is then matched with the already saved images within the database. There is a high chance that the voter's choice to be revealed in the traditional system, which is not the case in this proposed system. By using face recognition, it provides enough security to eradicate the dummy votes. The system also provides clear visualization of data regarding the percentage of total votes cast, the percentage of votes each party secured, and the final winner in the election.

I. Introduction

Class representatives are the core link between the college staff and the students. These representatives are therefore elected democratically to represent the interests of the students. It is always an expectation of the student that the elections are held fairly and the results are computed accurately. Previously, there have been challenges in the turnout of the voters due to some challenges they faced on the day of voting. This has been bringing some loopholes. The votes of the students who are not present on the day of the voting can be forged. Following these challenges, the solution to curb these problems is by introducing an e-voting system that ensures free and fair elections. This system ensures that one person can vote only once, and also forging the votes is not possible as the system uses face recognition. This system also curbs the chances of manipulating the results by influencing the authorities and thus generates transparency to the highest level.

- **Uploading images into the database:**

The images of the eligible voters are collected and uploaded into the database by the admin. The admin will be the sole person who will have complete access to the data present in the database. The voting process using face recognition begins when the voter stands in front of the camera and when the person's face is compared to the images of the person that have been uploaded into the database by the admin.

- **Detecting faces in Image:**

It is the first step in facial recognition where faces in the image are detected. If there are more than two faces in the image, then the image is discarded, as the main aim here is to uniquely identify the voter using his face. Having two faces in the same picture may lead to inconsistency in the working of the face recognition algorithm, which in turn may reduce the efficiency of the system.

- **Isolating and Projecting faces:**

The next step is to wrap the faces including eyes, lips, etc. perfectly in the frame. Aligning faces accurately during both training and testing gives a boost in performance. For this, the face landmark estimation algorithm is used. This algorithm identifies major landmarks that exist on the faces including the iris of an eye, the inner edge of eyebrows, the top of the chin, lips, etc.

- **Face Identification:**

The last step is to identify the person from our database who has the closest measurement to the test image provided. The classification of the image is

done using KNN (k-nearest neighbor) classifier. KNN is a supervised learning algorithm that classifies the given instance based on the majority of K-nearest neighbors. This algorithm relies on the distance between the feature vectors, and it also has labels associated with each image, so that it can return the name of the person who is being classified. The distance can be calculated with the help of Manhattan distance or Euclidean Distance. The KNN algorithm classifies by finding the most common class among the k-closest examples.

- **Voting process:**

  The actual voting process begins when the voter's face is recognized by the system as an authenticated voter. Once the voter's face is verified, the user will be able to cast his vote in the system. Also, the system ensures the voters' privacy by not displaying to which party the voter has cast his/her vote.

- **Displaying the Results:**

  The winner is displayed at the end of the entire voting process along with the number of votes that are cast under his name. The names of the remaining contestants are also displayed along with the number of votes cast under their names. This representation is also done in a graphical format using data visualization techniques.

II. Existing System

Existing voting systems are electronic voting machines and secret ballot voting, both of which are labor-intensive. Both the systems are time-consuming yet are very easy to manipulate. The EVM machines are validated manually and transported whenever the election is taking place. So, there are a lot of ways to count the votes, which might not be clean. Hence the current system can be made a lot better, more accessible, and more efficient while eliminating human interference from none to barely a minimum.

III. Proposed System

The electronic voting system using face recognition ensures that the system uses the voter's face as the login system, and only once authenticated is the portal for casting votes is opened. The electronic voting system using face recognition ensures that the votes of one person are not forged by the other.

On the other hand, the system also ensures that each person can vote only once. At the same time, the system makes it impossible to manipulate the results as the results are displayed immediately after the elections, along with the number of votes of each contestant. This ensures transparency to the highest level.

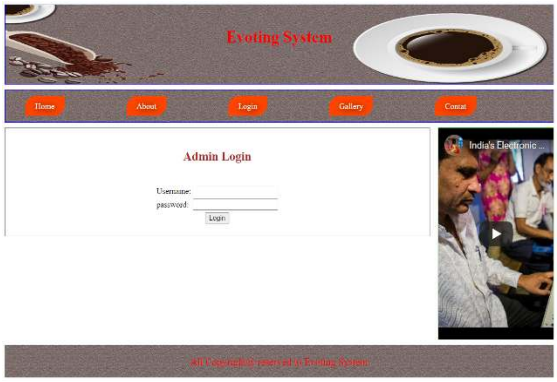
IV. Implementation (Modules)

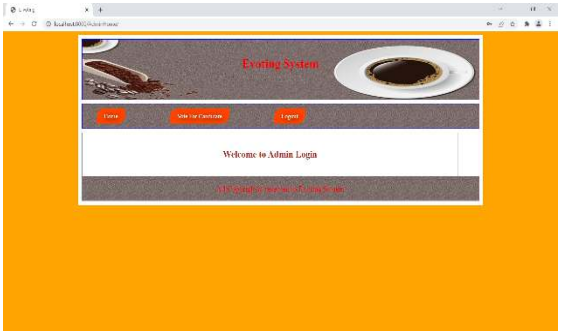
The Electronic Voting System using Face Recognition is implemented using a Machine Learning algorithm called K-Nearest Neighbor (KNN). KNN is used to recognize the user's face which is captured from the system's camera. The images that are captured are then compared to the values in the database, which consists of the images of all the eligible voters.

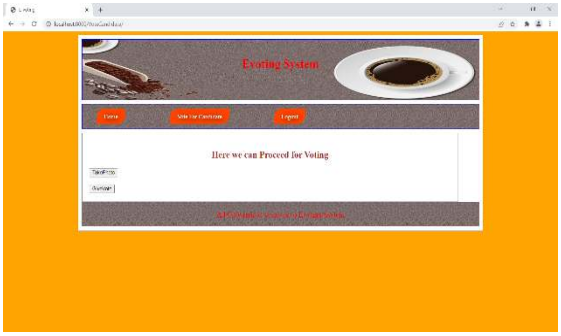
If the image captured matches the images in the database, the user is allowed to cast his/her vote. If the user's face is not recognized by the system, a message stating "YOU ARE UNKNOWN PERSON" is displayed. If the user tries to cast his/her vote multiple times, then the system gives an alert message stating "DEAR XYZ YOU ALREADY SUBMITTED YOUR VOTE."

Once the votes of all the eligible voters are taken, the contestant who gets the highest number of votes will be visible in the database, which can be accessed only by the admin.

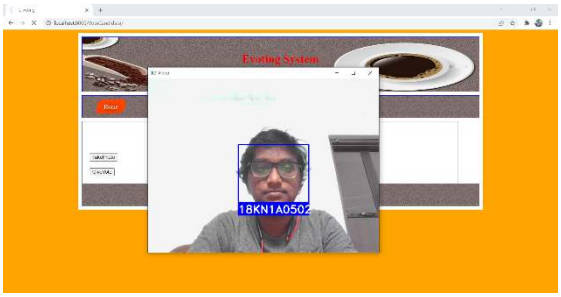
Sample Screens

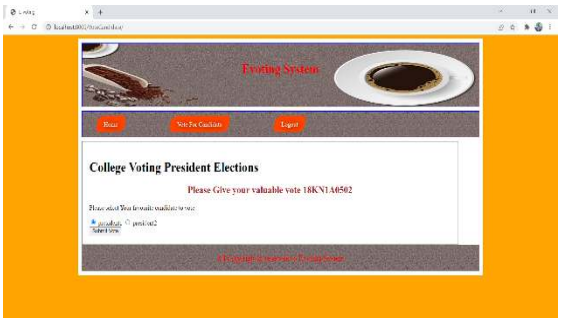




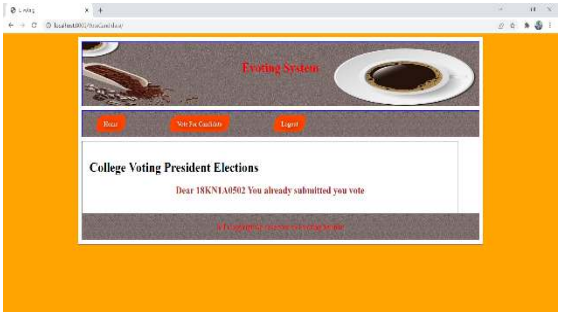


After clicking Take Photo the webcam will take the image of our face then click on Give Vote.

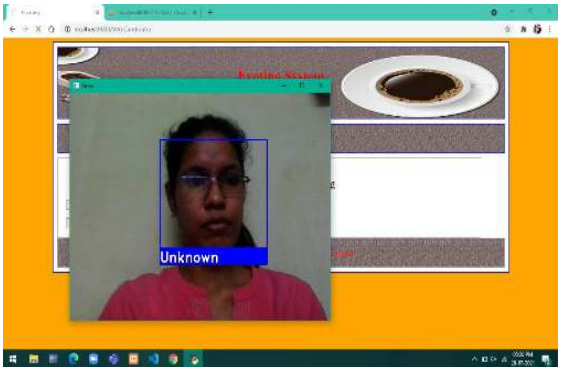




If any user is trying to cast the vote for second time it shows that your vote is already submitted.



If any unknown person is trying to cast the vote it shows that you are unknown person.



V. Conclusions

Today, we are at the age of modernization, and we should prepare for the changes that will occur in the next few years. A change in how elections are conducted may seem shocking and grueling, but it can be possible with the right approach.

Having the right approach to online voting is very important, especially since a single vote can dictate a considerable part of the contesting parties. Therefore, making sure that a

voting system is secure, relevant, accessible, and fair is of the almost importance. This new form of voting may seem intimidating, but change is always confusing and sometimes scary. It's all in how we carry ourselves despite the confusion.

VI. Future Scope

As time passes, new machines can continue to transition into different sectors and industries. Among these is the online voting system that has begun to increase in popularity.

The global pandemic has forced many universities to transition the existing system online. Anything from enrolling, school lectures, and graduation ceremonies, many institutes have to use online systems.

Online voting may not be ideal and is the topic of many heated debates. However, one thing is for sure, the option is there, and it might be the only option available.

If universities were to go strictly virtual, then many things need to be fixed. As of now, one of the biggest concerns when it comes to online voting is to develop better face recognition algorithms.

VII. References

[1] Pandit, Varad, Prathamesh Majga onkar, Pratik Meher, Shashank Sapaliga, and Sachin Bojewar, "Intelligent security lock." In Trends in Electronics and Informatics (ICEI), 2017 International Conference on pp. 713-716. IEEE, 2017.

[2] Bhimanwar, Chinmay, Rupesh Biradar, Nikhil Bhole, and Milind Rane. "Face Identification." International Journal of Engineering Science11923 (2017).

[3] Ishani Mondal, Sombuddha Chatterjee. "Secure and Hassle-Free EVM Through Deep Learning Based Face Recognition." International Conference on Machine Learning, Big Data, Cloud Computing and Parallel Computing (COMITCon). IEEE, 2019

[4] S. Kumar and E. Walia, "Analysis of electronic voting system in various countries," International Journal on Computer Science and Engineering, vol. 3, no. 5, pp. 1825-1830, 2011.

[5] D. Nikram, D. Shetiye, and D. Bhorite, "A critical study of electronic voting machine EVM utilization in electronic procedure," International Journal of Trend in Scientific Research and Development, vol. Special Issue, pp. 1-3, 03 2019.

[6] S. Ravi and D.P. Mankame, "Multimodal biometric approach using fingerprint, face and enhanced iris features recognition," in 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT), IEEE, 2013, pp. 1143-1150.

[7] D. Menotti, G. Chiachia, A. Pinto, W. R. Schwartz, H. Pedrini, A. X.Falcao, and A. Rocha, "Deep representations for iris, face, and fingerprint spoofing detection," IEEE Transactions on Information Forensics and Security, vol. 10, no. 4,pp. 864–879, 2015.

[8] J. Soldera, G. Schu, L. R. Schardosim, and E. T. Beltrao, "Facial biometrics and applications," IEEE Instrumentation & Measurement Magazine, vol. 20, no. 2,pp. 4–30, 2017.

[9] S. Kumar, S. Nandury, and S. Raj, "An extended client server architecture inmobile environment," International Journal of Computer Engineering and Applications, vol. 5, pp. 97–107, 02 2014.

[10] T. Ko, "Multimodal biometric identification for large user population using fingerprint, face and iris recognition," in 34th Applied Imagery and Pattern Recognition Workshop (AIPR'05), 2005, pp. 6 pp.–223.