International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 03 | Mar 2023 www.irjet.net p-ISSN: 2395-0072

VIRTUAL VOTING SYSTEM USING FACE RECOGNITION AND OTP

Prof. Prakash Kshirsagar[1], Jitesh Kamble[2], Neha Wagh[3], Satwik Unawane[4]

[1]Prof. Prakash Kshirsagar, Dept. of Computer Eng.., NMIET, Maharashtra, India
[2]Jitesh Kamble, Dept. of Computer Engineering, NMIET, Maharashtra, India
[3]Neha Wagh, Dept. of Computer Engineering, NMIET, Maharashtra, India
[4]Satwik Unawane, Dept. of Computer Engineering, NMIET, Maharashtra, India

---

Abstract - *India now offers two options for casting a ballot. Electronic voting machines and secret ballots both have advantages and problems. Moreover, the current system is unsafe. Simply because they must travel to the polling place and stand in line for several hours, many people lose the chance to vote. In this essay, we suggested a voting procedure. In our system, there are three security phases in the voting process. Face recognition serves as the first stage, election ID (EID) number verification serves as the second stage, and one-time password (OTP) verification using the user's registered mobile number serves as the third stage.*

Key Words **: IDE Spyder, Python, MySQL, Voting System, Face Recognition, OTP**

1. INTRODUCTION

Face recognition technology is a form of biometric identification that uses facial features to identify individuals. It has been used in various applications such as security systems, authentication systems, and even in voting systems. The use of face recognition technology in voting systems can provide benefits such as improved accuracy, reduced fraud, and increased security. It can also eliminate the need for physical identification documents, which can be a significant advantage for individuals who do not have easy access to such documents. However, it is essential to note that the use of face recognition technology in voting systems raises some concerns, such as privacy and security risks. There have been instances where facial recognition systems have been found to be inaccurate or biased, which can result in incorrect identification and potential voter disenfranchisement. Additionally, there is the risk of data breaches, which can compromise the privacy of individuals' personal information. Therefore, it is crucial to ensure that any voting system that uses face recognition technology has robust security measures in place to prevent unauthorized access and protect sensitive information. The system should also undergo regular testing and auditing to ensure its accuracy, fairness, and compliance with relevant laws and regulations. In conclusion, while face recognition technology can offer several advantages for voting systems, it is crucial to consider the potential risks and implement appropriate security measures to protect individuals' privacy and ensure the integrity of the voting process. To speed up ballot counting, reduce the cost of employing personnel to physically count votes, and improve accessibility for voters with disabilities, electronic voting equipment has entered the picture. Expenses ought to decrease with time as well. It is possible to take early remedial action and disclose findings more promptly. A computerized system is used for instruction, addressing, getting, marking, and delivering votes in the smart voting system known as online voting. Vote-related election data is generally recorded, saved, processed, and kept as digital data. To get beyond the client-side flaws in the voter's voting software, voter identification and authentication procedures are therefore crucial for more secure platform processes.

1.1 Problem Statement

In an online voting system, the election data is primarily recorded, stored, and processed as digital information, and ballots are obtained, marked, delivered, and counted via computer. This poses several challenges in terms of security and reliability, particularly when it comes to voter identification and authentication. To ensure the security and integrity of the voting process in an online system, various techniques can be employed to authenticate the voter and prevent fraudulent activities. These techniques may include biometric identification such as facial recognition or fingerprint scanning, two-factor authentication using a combination of passwords and security tokens, and digital signatures. It is crucial for an online voting system to have robust and reliable mechanisms in place for voter identification and authentication to prevent unauthorized access and ensure the integrity of the voting process. The vulnerabilities of the client used by the voter to cast their vote must also be considered and addressed to minimize the risk of security breaches.

1.2 Literature Survey

1.2.1 Smart Voting

The proposed system in the paper appears to have three security phases to ensure the integrity of the voting process. The first phase involves obtaining the information of individuals above the age of eighteen from the Aadhar database. The Aadhar database is a biometric identification system that collects demographic and biometric information, such as fingerprints and iris scans, of Indian residents. In the second phase, voters will receive an ID and password via their registered email address prior to the

voting process. This ID and password will be used to authenticate the voter's identity during the voting process. The third phase involves

validating the voter's identity using fingerprint data. Once the voter's identity is confirmed, they will be allowed to cast their vote. After casting their vote, the voter ID will be deleted, and Aadhar details used by the voter will be locked to prevent any further access. The vote count will be updated simultaneously. Overall, the proposed system aims to ensure the security and integrity of the voting process by using a combination of biometric authentication, unique voter IDs, and parallel vote counting.

1.2.2 Location-free Voting System with IoT Technology

According to the paper, the voting process is conducted through a smartphone using its fingerprint sensor. The voter's fingerprint sensor will be linked to an application in the smartphone, which will validate the voter's identity before allowing them to vote. Additionally, the voter will be allowed to vote only on the scheduled day of the voting process. This is to ensure that the voting process is conducted smoothly and without any discrepancies. Furthermore, the voter can vote from anywhere using their smartphone, but they will only be allowed to vote once. This is to prevent any fraudulent or multiple voting attempts. Overall, the use of smartphone technology and fingerprint sensors for voter authentication aims to make the voting process more accessible, secure, and convenient for voters.

1.2.3 Voting System using Fingerprint Recognition

In these papers, the author mainly focuses on the fingerprint validation process. This is also a less storage consuming process. This system also asks for Aadhar details before going forward for the voting process. Though the Aadhar already contains the fingerprint details of the voters. So, its quick validation process. Once the voter provides the Aadhar details, the system validates the Aadhar number and then after verification, validation of the voters begins, the system requires the hardware for fingerprint validation, once the fingerprint is validated then the system provides the permission for voting or else deny the process.

1.2.4 Smart Voting System using Facial Detection

According to the paper, the current system requires physical presence, which is inconvenient for many people, and the voting process is time-consuming. The author proposes a system that uses facial recognition to unlock the voting system, like unlocking a phone, and does not require physical presence to cast a vote. The proposed web-based system enables people to cast their votes from anywhere in the world, making the process more accessible and convenient. Facial recognition is used to decrease the chance of duplicate voting, and only those registered prior to the election and recognized by the system will be allowed to vote. Just like fingerprints, every face has unique features that remain unchanged with age, such as the distance between the eyes and eyebrows, making the system more secure. By using facial recognition technology, the proposed system aims to streamline the voting process, increase accessibility, and improve security by reducing the likelihood of fraudulent voting g attempts.

1.2.5 Iris Detection in Voting System

Iris is one of the unique Validation of the person. So, in this paper the author mainly focuses on the Iris to validate the correct voter. Whenever the voter starts the digital voting system, the system first asks for Aadhar details, because the Aadhar contains all the details regarding to any person. For ex. Fingerprints, Address, Blood-Group, Iris etc. So, it's become easy to validate the person using Iris through its Aadhar details. This system consumes very less storage of database. Because there is no required to keep any pre-registration process. This complete process mainly required a hardware that can scan the iris of the voters.

1.2.6 Secure Reliable Multimodal Biometric Fingerprint and Face Recognition

According to the paper, the author focuses on using a component-based face detector to extract facial features for recognition purposes. The process involves analyzing the distance between facial marks or features using principal component analysis. The extracted features are then compressed into a single feature vector and fed into the recognizer. Similarly, for fingerprint images, every pixel of the image is analyzed to extract features for recognition purposes. The implementation of this process is done using MATLAB. By using principal component analysis to extract features and compressing them into a single feature vector, the author aims to build a better version of the existing system. Overall, the use of component-based face detector and principal component analysis for feature extraction aims to improve the accuracy and efficiency of the recognition process.

1.3 Proposed System

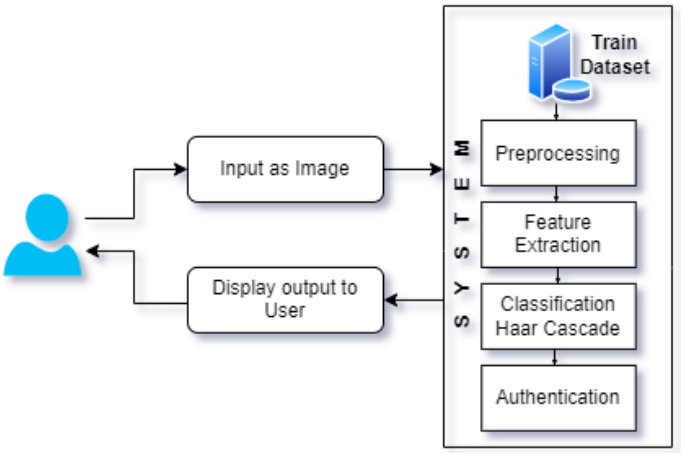


Fig -1.3.1: System Architecture

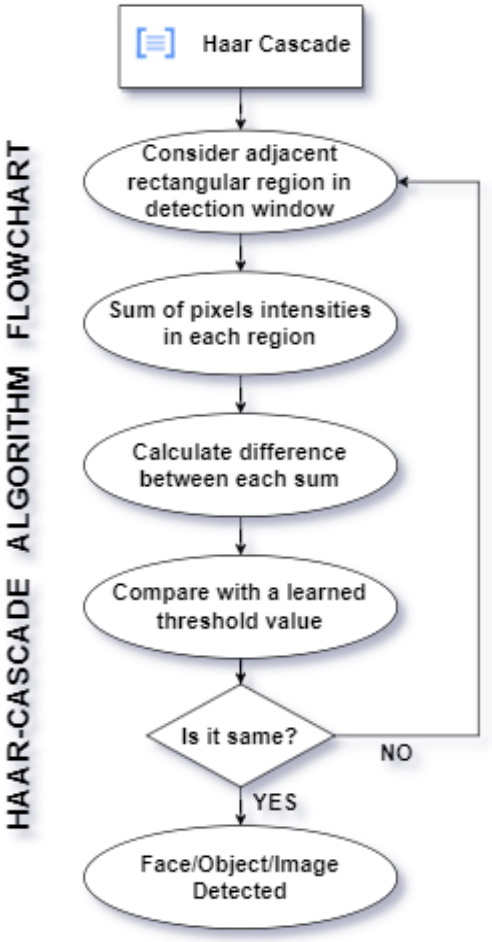
It is great to hear that a smart voting system has been proposed that utilizes face recognition using image processing to enhance security. Face recognition is a popular biometric technique that can help in accurately identifying individuals based on their facial features. The proposed system's approach of using the Haar Cascade Algorithm to extract facial features and recognize facial parts of the image is a widely used method in face detection and recognition. It is based on a machine learning technique that involves training a classifier to detect objects in images. This method has proven to be effective in detecting and recognizing faces in images and videos. It is also good to know that the system checks the captured image against the current database of face images provided by the election commission to ensure that only authorized voters can cast their vote. This approach can help in preventing fraudulent voting and enhancing the overall security of the system. Using Visual Studio, Python, HTML, and Django to create an online platform and implement the algorithm is a wonderful choice since these technologies are widely used and well-supported in the industry. This can help in creating a robust and scalable system that can handle many voters. Overall, the proposed smart voting system using face recognition can be an excellent step towards enhancing the security and transparency of the voting process. It is important to ensure that the system is thoroughly tested and validated before being deployed to ensure its effectiveness and accuracy.

2. FACE DETECTION USING HAAR CASCADE

It is great to see that the Haar Cascade method is being used for face detection in the proposed smart voting system. This method is a popular and effective object detection algorithm that can detect faces in an image or video with high accuracy. The process of detecting faces using the Haar Cascade method involves several stages. Firstly, the input image is converted into grayscale to simplify the image and reduce computational complexity. Then, the algorithm detects a sequence of square-shaped features called Haar features. These features are calculated by computing the difference between the sum of pixel intensities in adjacent rectangular regions of the image. In the next stage, the algorithm uses integral images to speed up the computation of Haar features. An integral image is a two-dimensional array that stores the sum of pixel intensities of all the pixels in the rectangle defined by its upper left and lower right corners. The third stage involves training a classifier using the Adaboost algorithm. This algorithm selects the best features that can accurately distinguish between faces and non-faces. Finally, the algorithm uses a cascade of classifiers to classify the input image as a face or non-face. The cascade of classifiers is a series of stages where each stage consists of several weak classifiers. If an input image fails to pass any stage, it is immediately rejected, which helps in reducing false positives and increasing the accuracy of the algorithm. Overall, the Haar Cascade method is an effective approach for face detection and can help in accurately identifying voters in the proposed smart voting system. It is important to ensure that the system is trained and validated using a diverse set of positive and negative images to ensure its effectiveness in real-world scenarios.

2.1 Detecting Haar features

It is interesting to learn that prior to the Haar Cascade method, image pixel intensities were used for face detection, which required a lot of effort and work. Paul Viola and Michael Jones' contribution to the field of face detection using Haar wavelets was a significant breakthrough. Their approach involves taking smaller subsections of a face at once into consideration and computing the sum of their pixel intensities. Then, the difference between these sums is calculated to detect features like the edge of the nose or the contour of the eyes. The use of Haar wavelets has proven to be effective in detecting faces in images and videos, and the Haar Cascade method builds on this approach by training a classifier to detect faces based on a set of Haar-like features. It's important to note that in real-world scenarios, images are not ideal black and white pixel values of 0 or 1. Instead, images are usually normalized grayscale images with pixel values between 0 and 1. This normalization is essential for accurate face detection since it helps in reducing the effects of variations in lighting and other factors that can affect image quality. Overall, the use of Haar wavelets and Haar Cascade methods has revolutionized face detection and has enabled the development of advanced applications like the proposed smart voting system that uses face recognition for enhanced security.



2.2 Using Integral Images

Integral images are used to speed up the computation of Haar features. Integral images are created by summing up the pixel intensities of an image in a way that makes it easy to compute the sum of pixel values in any rectangular area of the image. This is done by creating a new image where each pixel value represents the cumulative sum of pixel values above and to the left of that pixel. The value of each pixel in the integral image is calculated using the following formula:

integral (x, y) = integral (x-1, y) + integral (x, y-1) – integral (x-1, y-1) + image (x, y)

where integral (x, y) represents the sum of pixel intensities in the rectangle defined by the upper left corner (0,0) and the lower right corner (x, y) in the original image, and image (x, y) represents the pixel value at location (x, y) in the original image.

2.3 Adaboost Algorithm

The Adaboost algorithm is used to train a classifier that can accurately distinguish between faces and non-faces. The algorithm works by combining multiple weak classifiers into a strong classifier. Each weak classifier is trained on a subset of the training data and assigned a weight based on its performance. The weights of misclassified samples are increased, while the weights of correctly classified samples are decreased. The final classifier is obtained by combining the weak classifiers with the highest weights.

2.4 Haar Cascade

The cascade classifier is a sequence of stages where each stage consists of multiple weak classifiers. The output of first stage is given to as input to the further-next stage. The classifier rejects the input if it fails to pass any stage, which helps in reducing false positives and increasing the accuracy of the algorithm. The cascade classifier is trained using the Adaboost algorithm and a set of positive and negative training samples. The final classifier can detect faces with high accuracy and low false positive rates.

3. FUTURE SCOPE

Improvements to the system's security and level of efficiency are among its potential future uses. In addition to that, it would be intriguing to meet the other secret primitives to boost system effectiveness. Future upgrades could also address power outages and system crashes to give voters greater confidence while casting their ballots.

4. CONCLUSION

Our proposed system is a machine learning-based solution that utilizes face detection and One Time Password (OTP) verification to allow voters to register and vote from any location, regardless of their physical location. This system offers enhanced security measures and prevents individuals from casting multiple votes. It is a dependable and trustworthy system that offers the convenience of remote voting, reducing the need for human resources and time-intensive processes.

5. ACKNOWLEGEMENT

We are pleased to present the preliminary project report for our project on "Online voting system using face recognition and opt". We would like to express our sincere gratitude to our internal guide, Prof. Prakash Kshirsagar, for providing us with all the necessary help and guidance throughout the project. We are grateful for their kind support, and their valuable suggestions have been immensely helpful in shaping our project. We would also like to thank Dr. Hod Name, the Head of Computer Engineering Department at “Nutan Maharashtra Institute of Engineering and Technology,” for their indispensable support and suggestions. Finally, we extend our special thanks to Dr. Vilas Deotare, the Principal of our college, for providing us with various resources such as a laboratory equipped with all the necessary software platforms and continuous internet connections for our project.

6. REFERENCES

1. Professors Kriti Patidar and Swapnil Jain have published a research paper on a proposed decentralized e-voting portal that would use blockchain technology to enhance security and transparency. The blockchain would provide an immutable record of all transactions, making the system more secure and resistant to hacking.

2. Another research paper authored by Prof. Shashank S Kadam, Ria N Choudhary, Sujay Dandekar, Debjeet Bardhan, and Namdeo B Vaidya focuses on developing an electronic voting machine with improved security features. The aim is to create a more reliable and trustworthy voting system that is less susceptible to tampering or manipulation.

3. Rahil Rezwan, Huzaifa Ahmed, M. R. N. Biplob, S. M. Shuvo, and Md. Abdur Rahman have proposed a "Biometrically Secured Electronic Voting Machine" in their research paper.

4. Z.A. Usmani, Kaif Patanwala, Mukesh Panigrahi, and Ajay Nair have developed a "Multipurpose Platform-Independent Online Voting System" that can be used for various purposes.

5. Ravikumar CV has published a research paper in the Indian Journal of Science and Technology titled "Performance Analysis of HSRP in Provisioning Layer-3 Gateway Redundancy for Corporate Networks."

6. Ashwini Mandavkar and Prof. Rohini Agwane have proposed a "Mobile-based Facial Recognition Using OTP Verification for Voting System" in their 2015 IEEE paper.

7. Himika Parmar, Nancy Nainan, and Sumaiya Thaseen have proposed a method for generating secure one-time passwords based on image authentication in their paper presented at CS IT-CSCP 2012.

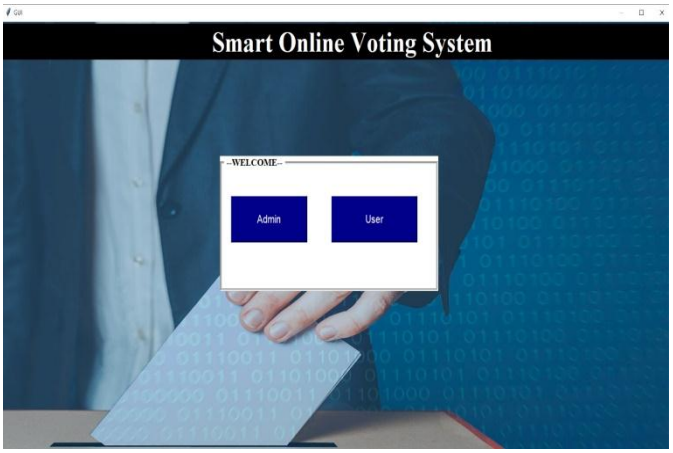
8. Hongyu Zhang, Qianzi You, and Junxing Zhang have proposed a "Lightweight Electronic Voting Scheme Based on Blind Signature and Kerberos Mechanisms" in their paper presented at the International Conference on Advanced Networks and Telecommunications Systems in 2015.

9. Herb Deutsch has discussed the influence of public opinion on voting system technology in his 2005 paper titled "Public Opinion's Influence on Voting System Technology."

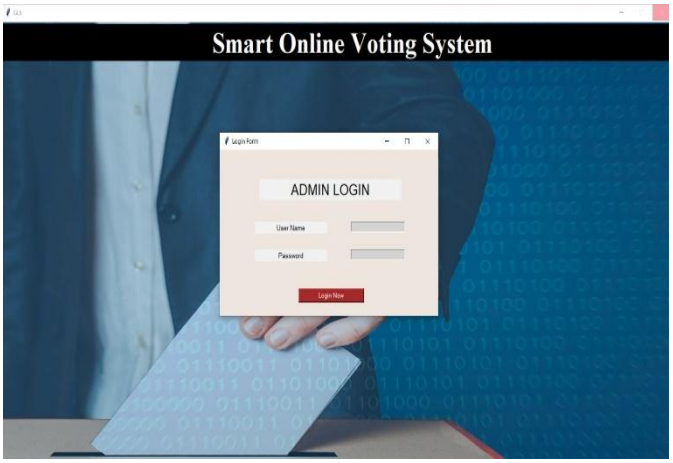
10. Anandaraj S., Anish R., and Deva Kumar P.V. have proposed a "Secured Electronic Voting Machine Using Biometric" in their paper presented at the IEEE International Conference on Innovations in Information, Embedded, and Communication Systems in 2015.

7. RESULTS

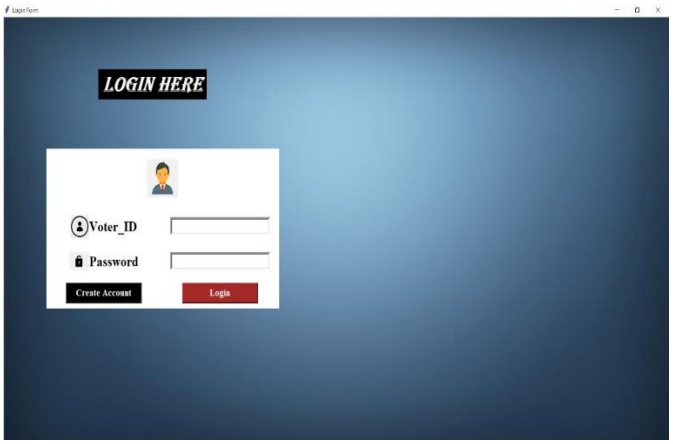
HOME PAGE



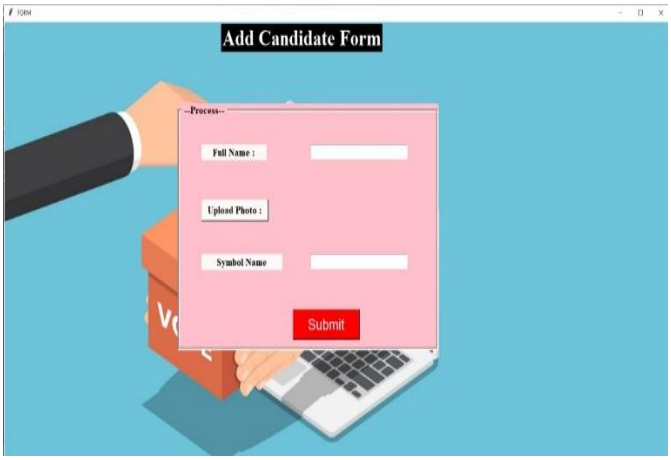
ADMIN LOGIN PAGE



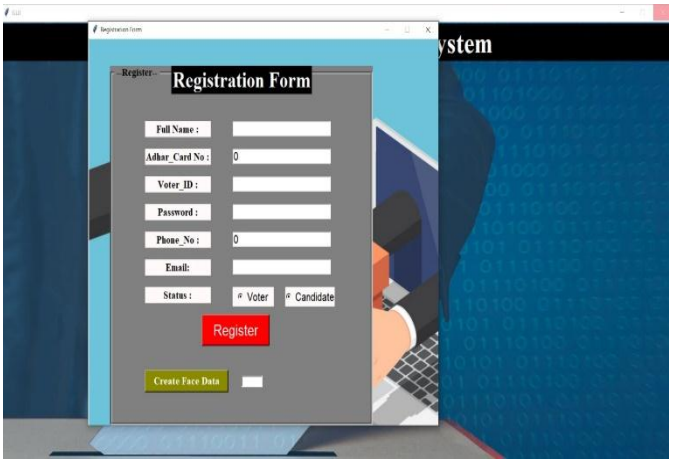
USER LOGIN PAGE



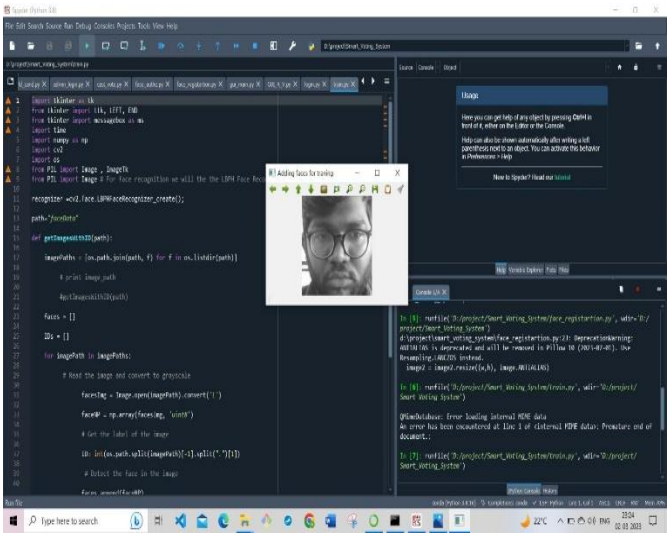
CANDIDATE FORM



VOTER REGISTRATION PAGE

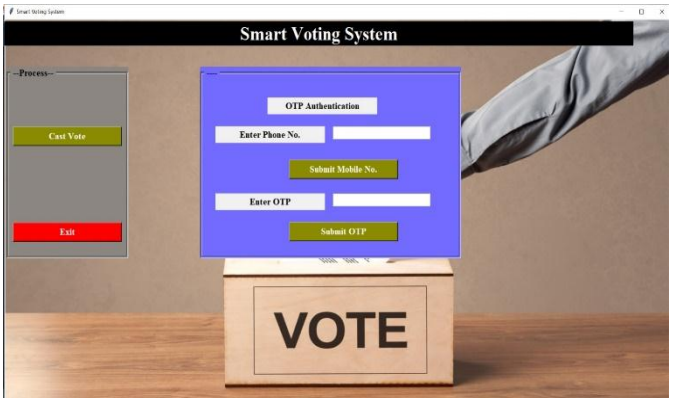


FACE REGISTRATION



CAST HOME PAGE

OTP & FACE AUTHENTICATION



VOTE CASTING

8. BIOGRAPHY

Prof. Prakash Kshirsagar,

CEO & Professor at Department of ComputerEng., Nutan Maharashtra Institute of Engineering and Technology,Talegaon.

Jitesh Janardan Kamble,

Student, Department of Computer Eng., Nutan Maharashtra Institute of Engineering and Technology, Talegaon.

Neha Dnyaneshwar Wagh,

Student, Department of Computer Eng., Nutan Maharashtra Institute of Engineering and Technology, Talegaon.

Satwik Vasant Unawane,

Student, Department of Computer Eng., Nutan Maharashtra Institute of Engineering and Technology, Talegaon.