REVOLUTIONIZING E-VOTING SYSTEMS WITH FACIAL RECOGNITION USING MACHINE LEARNING AND DEEP LEARNING FOR IMPROVED IDENTITY VERIFICATION AND SECURITY

Abhirami .K [1]

[1] PG Scholar dept of MCA
Dayananda Sagar College of Engineering (VTU)
Bangalore, Karnataka, India
abhiramimurthy@gmail.com

Dr. Samitha Khaiyum [2]

[2] Head of department, dept of MCA
Dayananda Sagar College of Engineering (VTU)
Bangalore, Karnataka, India
mcavtu@dayanandasagar.edu

***Abstract*—** Systems for electronic voting (E-Voting) have drawn a lot of interest as a way to improve the effectiveness, openness, and accessibility of the voting process. In order to verify voters and guarantee the fairness of the voting process, this study suggests a unique e-voting system that makes use of face recognition techniques based on machine learning and deep learning algorithms..[9] The proposed system leverages advancements in computer vision and artificial intelligence to address the challenges of traditional voting systems, such as identity fraud, impersonation, and multiple voting instances. By employing face recognition technology[2], the system aims to provide a secure, reliable, and user-friendly voting experience. This research contributes to the advancement of e-voting systems by incorporating cutting-edge machine learning and deep learning techniques to address the security and reliability concerns associated with traditional voting methods. The experimental results demonstrate the system's effectiveness in accurately recognizing and authenticating voters, thereby paving the way for a more efficient and trustworthy democratic process. Each nation must give the verification and validation requirements careful consideration when building electronic voting systems. It is suggested in this study to use deep earning and machine learning to implement an E-voting method using face recognition.

KEYWORDS: E-voting, Face Recognition, Image Processing, OTP Verification ,machine learning, deep learning

I. INTRODUCTION

Electronic voting (E-voting) systems is offering the electoral process. To ensure the integrity and security of these systems,[3] various technological advancements have been incorporated, including the utilization of face recognition techniques[9] based on machine learning and deep learning algorithms.The objective of this research is to present an innovative E-voting system that leverages state-of-the-art advancements in computer vision and artificial intelligence to authenticate voters and enhance thereliability of the voting process. By incorporating face recognition technology[1,2],the proposed system aims to mitigate concerns such as identity fraud, impersonation, and multiple voting instances, thus bolstering the integrity and trustworthiness of the electoral system.In India, voting is done using either the traditional paper ballot system or an electronic voting machine (EVM).Since there is a great possibility of fraudulent or dummy voting, as we have long observed, this voting process is carried out in some way. The current systems are readily manipulated; a dishonest official or candidate might cast a fictitious vote on an EVM[6] because there is no biometric verification, or he could stamp a fictitious ballot on paper. These two systems are designed to be carried while being closely monitored and with security people.

The ongoing fraud of fraudulent voting will be stopped since biometrics[3] cannot be taken from anyone or utilised by anyone else. The elections will go well since anyone may cast a ballot from anywhere; they simply need to sign in to the voting website, identify their biometrics, and do so. The suggested Electronic voting system will close the gaps in the current methods is not allowed to poll the vote.

For voting representatives are appointed by electorates.Currently, in order to cast a ballot at a polling place, a voter must present a voter ID card[10]. As a result, the process takes a while because the official must verify the voter IDcard.

The outcomes of this research contribute to advancing the field of E-voting systems by harnessing the potential of face recognition technology and incorporating machine learning and deep learning techniques. Through extensive experimentation and evaluation,[9] the effectiveness and accuracy of the proposed system will be demonstrated, validating its potential as a secure and efficient alternative to traditional voting methods.

In summary, the utilization of face recognition techniques, coupled with machine learning and deep learning algorithms, offers a robust solution to enhance the authentication and integrity of E-voting systems[5]. This research aims to contribute to the ongoing efforts in developing trustworthy and transparent electoral processes, thus ensuring the democratic rights of citizens are protected in the digital age.

II. PROBLEM STATEMENT

Despite the progress that our nation has made towards digitalize India, the voting system still has certain issues. In accordance with the current system, voter registration is only feasible if voters visit the polls. The name of the voter appears in the list for his or her particular area at the time of voting[4]. Outside of the area surrounding the address listed on the voting card, they are unable to cast a ballot. Therefore, voters who have moved elsewhere are unable to cast physical ballots. We can see the peril of this system from the current Corona Virus pandemic situation.[9] Due to the requirement that the voter be physically present to cast their ballot, this could resultin a failure of social distance throughout the voting process.

III. LITERATURE SURVEY

The literature survey reveals that E-voting systems employing face recognition technology have garnered significant attention. The studies emphasize the potential of face recognition algorithms, including deep learning approaches, in ensuring secure and efficient voter authentication. Additionally, researchers have explored critical aspects such as system security, privacy preservation, usability, and user acceptance, contributing to the development and improvement of e-voting systems using face recognition. These studies collectively provide valuable insights and pave the way for further advancements in this field.

1) Enhanced Security E-Voting Machine

In this work, the design and building of a voting machine employing an ATMEGA 32 microcontroller,[9] which has three additional security layers, are discussed. Voting using paper ballots and an EVM requires a lot of time. In order to saved in consideration of the quantity of time. Therefore, the system is being implemented in this case in a manner that prevents the use of paper ballots to ensure voting secrecy. Voting machines now in use cost more money than EVMs and use VVPAT.[4] Results can be accessed with only one click and EVM provides 100% proof of tampering. Using this programme accelerates the ballot count. Because there is no need to hand count votes, labour costs are reduced.

2) Multipurpose, cross-platform online voting system

A multipurpose cross-platform online voting system is a versatile and flexible platform that enables voting processes to be conducted electronically across various devices and operating systems. This type of system serves as a comprehensive solution for different voting scenarios, including governmental elections, organizational decisions, surveys, and opinion polls[8]. The voting ballot is produced by this system. User-end encryption and local administrator- end decryption are used for voting data. As a result, the voting system is more secure and authenticated. The literature review describes the major contributions that various authors have made to the field of face recognition.

3) Leveraging Biometric Authentication for Secure and Transparent voting Systems

The concept of leveraging biometric authentication for secure and transparent e-voting systems represents a significant advancement in the field of electoral processes. By integrating biometric technologies, such as fingerprint or iris recognition, into e-voting systems, the aim is to enhance the [7]security and reliability of voter authentication. Biometric authentication offers a highly accurate and unique identification method, as each individual possesses distinct biometric characteristics. This ensures that only eligible voters can participate in the voting process, mitigating the risks of impersonation or fraudulent activities. Moreover, biometric authentication provides a transparent and tamper-proof mechanism, as it relies on physical traits that cannot be easily duplicated or manipulated. This instills confidence in the integrity of the electoral process and assures voters that their voices will be accurately represented.

IV. RELATED WORKS

Several researchers have explored the application of face recognition using machine learning and deep learning techniques in the context of e-voting systems. The following works highlight significant contributions in this area:

i. "Face Recognition-Based Secure E-Voting System Using Deep Learning" (2019): This work presents a secure e-voting system that utilizes deep learning algorithms for face recognition. The authors propose a (CNN) model for facial feature extraction and authentication. The system achieves high accuracy in verifying voter identities, ensuring the integrity of the voting process.

ii. "E-Voting System Based on Face Recognition Using Support Vector Machine" (2020): E-voting system that combines face recognition techniques with the (SVM) algorithm. The system employs feature extraction algorithms to capture and analyze facial characteristics, followed by SVM classification for voter authentication. The experimental results demonstrate the system's effectiveness in achieving accurate and reliable identification.

iii. "Secure E-Voting System Based on Face Recognition Using Deep Learning" (2021): A secure E-voting system that utilizes deep learning for face recognition. The system employs a combination of pre-trained deep learning models and transfer learning techniques to achieve accurate and efficient voter authentication. The authors emphasize the importance of security measures ensure the integrity of the votingprocess.

These related works highlight the potential and effectiveness of face recognition techniques[3] in the development of secure and reliable e-voting systems. By leveraging advancements in computer vision and artificial intelligence, researchers have made significant progress in addressing identity verification, privacy concerns, and ensuring the integrity of the electoral process.

V. PROPOSED SYSTEM

The proposed e-voting system aims to leverage the capabilities of face recognition technology, machine learning, and deep learning to enhance the security, accuracy, and efficiency of the electoral process. The system will offer a robust and reliable method for voter authentication, mitigating potential fraud andensuring the integrity of the voting system.

Data Collection and Pre-processing: The system will start by gathering a diverse and representative dataset of voters' facial images. This dataset will be pre-processed to ensure consistency and quality, including resizing, normalization, and data augmentation techniques to handle variations in lighting conditions, facial expressions, and mask styles.

Feature Extraction with Deep Learning: The proposed system will employ deep learning techniques, such as convolutional neural networks (CNNs), for facial feature extraction. CNNs have shown remarkable capabilities in learning complex patterns and features from images, making them suitable for face recognition tasks.

Model Training: The pre-processed dataset will be used to train the deep learning model. During the training process, the model will learn to map facial images to unique feature vectors, forming a distinct representation of each voter.

Usability and Accessibility: The user interface of the e-voting system will be designed with user-friendliness and accessibility in mind. Clear instructions and intuitive design elements will make the voting process straightforward and inclusive for all voters, including those with disabilities. Privacy protection measures and user-centric design elements ensure that the system prioritizes voter privacy and accessibility while advancing the state of e-voting technology.

VI. EXISTING SYSTEM

In the current system, there are two types of voting: electronic voting machines and secret ballot papers. It is challenging to finish the poll in a single day since it takes a lot of manpower to maintain order and security. Allocation of surveys carried out by commission. At advance of two weeks, voters' cards are issued and polls are set up at schools and universities. There is a set time and location. On Election Day, all polling places will be open for voting in eight hours. The voter must first enter the polling place, where an officer will check their voter identification card and mark their left forefinger with inedible ink. The voter must then sign the register after the officer has finished.

VII. WORKING OF THE ALGORITHM

1) Haarcascade Algorithm

One of the primary categories for image classification and picture identification is the convolutional neural network (ConvNets or CNNs). CNNs[4] are frequently employed in a variety of applications, including object identification and facial recognition. Using the CNN algorithm,[9] our work project will identify and categorise drones in videos.

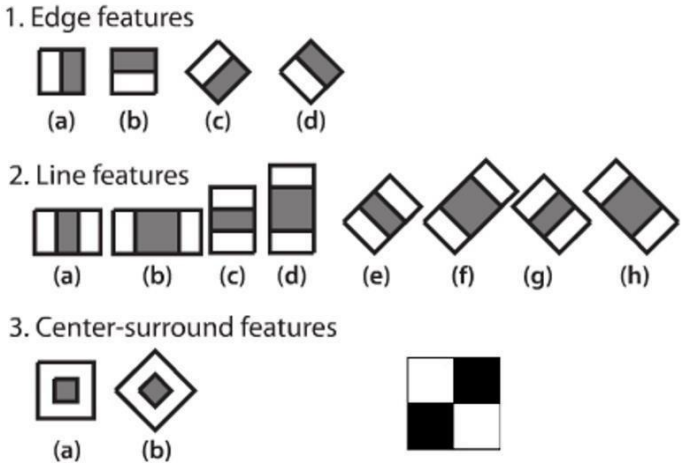

Fig-1: Haarcascade Algorithm Features

Fig-1 tells us about the Haar cascade approach is its speedy image scanning and probable facial region identification with only a little processing burden. It is frequently utilised in many different applications, such as face detection in cameras, video surveillance systems, and even as a component of bigger face recognition systems.

Overall, the Haar cascade algorithm offers a reliable and effective method for face detection, allowing its integration into electronic voting systems to identify voters based on their facial traits.

2) Local Binary Pattern Histogram

Local Binary Patterns Histogram (LBPH) is a popular technique used for face recognition. It extracts robust features from facial images by analyzing the patterns formed by pixel intensity comparisons in a local neighborhood.[9] LBPH utilizes four parameters, which are described as follows:

Radius:

The radius parameter defines the size of the local neighborhood around each pixel. It determines the distance from the central pixel to the neighboring pixels considered for pattern analysis. A larger radius includes more pixels in the local neighborhood, capturing more spatial information but increasing computational complexity.

Neighbors:

The neighbors parameter specifies the number of sample points within the local neighborhood. It determines the number of comparisons made between the central pixel[4] and its neighboring pixels. Each neighbor contributes a binary value (0 or 1) based on the intensity comparison, forming a binary pattern. Increasing the number of neighbors provides more detailed information about the local structure but also increases computational complexity.

Grid Size:

The grid size parameter divides the face image into a grid of cells. Each cell corresponds to a specific region of the face. The grid size determines the number of cells in the horizontal and vertical directions. By dividing the face image into smaller regions, LBPH captures local facial details and improves recognition accuracy.[9] However, a larger grid size increases computational requirements.

Histogram Size:

The histogram size parameter determines the number of bins in the histogram created for each cell of the grid. It specifies the range of possible patterns in the local neighborhood. A larger histogram size allows for more distinct patterns to be represented,[9] leading to increased discriminative power. However, a larger histogram size also increases memory requirements and computational complexity.

These four parameters in LBPH enable fine-tuning of the feature extraction process for face recognition tasks. By adjusting the radius, neighbors, grid size, and histogram size, researchers and practitioners can strike a balance between capturing detailed facial information, computational efficiency, and memory requirements, based on the specific requirements of the application.

3) Applying the LBP operation:

The initial computational step is to create an intermediary image that best represents the original image by emphasising the face features.

The method, based on variables like the radius and the neighbours, does this task using the sliding window concept. This stage already includes training the algorithm. Each histogram produced is utilised to represent one image from the training dataset.[11] As a result, given any input image, the procedures are repeated for a brand-new image, and a histogram is produced that will serve as the image's representation.

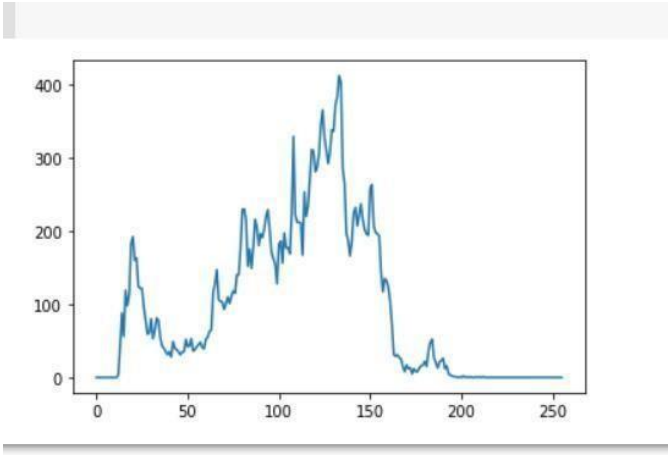

Fig-2 : Histogram of LBP Face Detection

Fig-2 Explains about the Histogram Analysis for Face Detection: The final stage involves analyzing the constructed histograms to determine whether the detected regions contain faces or not. This analysis is achieved through a classification process, where the histograms are compared to a pre-defined set of templates representing face and non-face patterns.

VIII. IMPLEMENTATION

This article is carried out with python, an object- and procedure-oriented programming language, is used to carry out the project[10]. Python is being used to carry out this project. Python offers dynamic typing and garbage collection. Due to its extensive standard library, Python is referred regarded as a "batteries included" language. Machine learning techniques are used in this investigation.Implementation of Security Protocols: Several security protocols are in place to protect the integrity of the electronic voting system. Data encryption techniques guard private voter data and shield it from unlawful access. To strengthen identity verification, multi-factor authentication can be used, which combines facial recognition with other biometric or password-based techniques. Algorithms for anomaly detection and real-time monitoring also aid in identifying and thwarting prospective hacking attempts and cyber threats.

MobileNet SSD for Person Detection

MobileNet SSD (Single Shot Multibox Detector) is a popular deep learning-based object detection framework, designed for real-time applications on resource-constrained devices like mobile phones and embedded systems. It combines MobileNet, a lightweight deep neural network architecture, with the SSD algorithm for efficient and accurate person detection. For person detection using MobileNet SSD, the model is trained on a large dataset containing images with labeled bounding boxes around the persons. During training, the network learns to detect specific patterns and features associated with human bodies.

At inference time, the MobileNet SSD takes an input image and performs the following steps:

i. The input image is passed through the MobileNet backbone to extract low-level and high-level features.
ii. These features [9]are then fed into additional convolutional layers specific to the SSD head, responsible for predicting bounding boxes and class scores.
iii. The SSD head generates bounding box coordinates (x, y, width, height) and confidence scores for each object class at different scales andaspect ratios for each grid cell.
iv. Non-maximum suppression[9] (NMS) is applied to filter out duplicate and low-confidence bounding boxes, keeping only the most confident detections.The remaining bounding boxes are the final predictions for person detection in the input image.

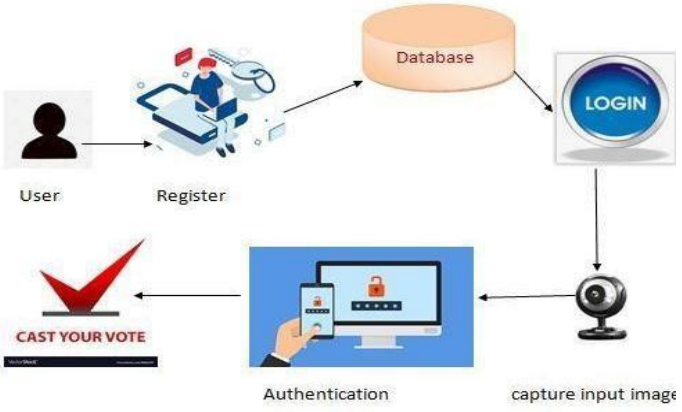

Fig-3 E-Voting System Architecture

Fig-3 is a detailed framework that describes the design and parts of the electronic voting system is known as the e-voting system architecture[14]. The architecture's primary goal is to support effective voting procedures that are transparent

and secure while still maintaining their integrity. The front end, back end, and database make up the system's three main parts most of the time. Voters can cast their ballots and authenticate their identities using a variety of authentication techniques, such as biometrics or passwords, through the interface that the front-end manages. The main operations of the system, such as voter registration, ballot creation, and vote tallying, are included in the back-end. For the purpose of protecting voter privacy and preventing tampering, this component makes use of cutting-edge cryptographic[14] methods. Finally, the database contains important data such voter registration information, ballot information, and voting outcomes. To protect the data, security measures like encryption and access limits are put in place. The e-voting system architecture takes advantage of technology's potential to speed up voting, lessen administrative burden, and give citizens a cutting-edge, reliable platform for taking part in democratic elections.

FACE MASK DETECTION WITH TENSOR FLOW AND KERAS SECTION

The implementation and methods utilised to determine whether or not people are wearing face masks using deep learning techniques are the main topics of the section on face mask detection using TensorFlow and Keras[12]. This section seeks to give a general overview of the procedures required in creating a face mask detection system utilising the TensorFlow and Keras frameworks.It provides an explanation of the dataset's structure, including the quantity of photos and the distribution of instances with and without a mask. It also emphasises how crucial it is to gather a wide variety of representative photos in order to guarantee the model's usefulness in real-world situations. The section next goes over the pre-processing techniques used on the dataset.The purpose of these pre- processing procedures is to improve the model's generalization and handling of changes in facial appearances, lighting situations.

CONCLUSION

The study of facial recognition in E-voting systems utilising machine learning and deep learning techniques shows the enormous potential of this strategy in enhancing the safety, effectiveness, and integrity of the electoral process. The E-votingsystems can successfully authenticate voters, reduce fraud, and improve privacy by integrating cutting- edge technology like machine learning and deep learning.

Since we can see that the current democratic framework has several shortcomings, including lengthy procedures that take a lot of time, are insecure, we may argue that our method is more beneficial and safe than it.

We can steer clear of them during political contest commissions by using the facial validation technique to detect voters who cast fraudulent ballots. voting system on the web. For the most part, India's cities are the result of smart voting. It ought to be seen as the biggest problem facing the majority of us. The current voting processes need a lot of physical labour and human resources, and if voting is moved online, asecure voting system is required. The approach to machine[9] learning. Are used to identify faces and determine if a voter is authorised or not.

FUTURE SCOPE

The E-voting system using face recognition based on machine learning and deep learning systems presents several exciting future possibilities that can further enhance the security, accessibility, and efficiency of the electoral process. While significant progress has been made, there are still ample opportunities for research and development in this area. Some key future scope areas include:

1) Robustness and Generalization: Future research should focus on improving the robustness and generalization of face recognition models used in E-Voting systems. Efforts can be made to address challenges related to variations in lighting, facial expressions, and occlusions.

2)Multi-Modal Biometrics: Integrating multiple biometric modalities, such as fingerprint, iris, or voice recognition, with face recognition can enhance the accuracy and security of e-voting systems.

3)Real-Time Processing: Research can focus onoptimizing face recognition algorithms for real-time processing to enable instantaneous voter authentication during the voting process.

4) Continuous Model Improvement: To keep pace with evolving technology and potential threats, e-voting systems should adopt a continuous improvement approach. Implementing mechanisms for model updates and retraining will ensure that the face recognition algorithms remain up-to-date, accurate, andsecure.

5) Hardware Integration: Future e-voting systems could explore hardware integration, particularly on mobile devices and other edge devices. This would enable on-device face recognition, minimizing data transmission and increasing privacy.

6)Privacy-Preserving Techniques: To address concerns about voter privacy, research can delve into advanced privacy-preserving techniques for face recognition.

7) Usability and Accessibility: Future research should focus on making e-voting systems more user-friendly and accessible to a wider range of voters, including those with disabilities.

8)Deployment and Real-World Trials: Large-scale deployment and real-world trials of the e-voting systems in diverse electoral settings would provide valuable insights into their practicality, effectiveness, and acceptance among voters.

In conclusion, the future scope for E-voting systems using face recognition based on machine learning and deep learning systems is vast and promising. By addressing challenges related to robustness, privacy, and usability while exploring innovative technologies and integration approaches, these systems have the potential to revolutionize the electoral landscape, ensuring secure, transparent, and accessible voting processes for citizens around the world.

REFERENCES

[1] Shikhar Agarwal, Geerija Lavania, Nilam Choudhary.(2019)E-ISSN 2320- 7639." Smart Voting Systems through the Facial Recognition"J. Sci. Res. In Computer Science and Engineering Vol- 7, April 2019.

[2] A.S.Narote, S.P.Narote, S.V.Tathe "Face Detection and Recognition in vids" Sinhgad Collegeof Engineering 2015. IEEE

[3] Adam Baumberg, Surrey(2020)" reliable Features Matching Across the Extensively Seperate Views". Ordinance Research Center Europe Limited Occam Court, Surrey Research Parks Guildford, Surrey GU2 5YJ United Kingdom 2000 IEEE

[4] A.K. Syafeeza,M. Khalil- Hani,S.S. Liew,R. Bakhteri Electrical Engineering, Universiti Teknologi Malaysia(2014)" Convolutional Neural Network(CNN) for the Face Recognition with Pose and Illumination Variation" International Journal of Engineering and Tech Vol 6 No 1 Feb-Mar 2014 ISSN 0575- 4024

[5] Nasser Kehtarnavaz, Mohammad Rahman and Jianfeng Ren Department of Electricals Engineering, University of Texas at Dalla(2009)" A cross strain faces position approach for nonstop association on cell phone" 2009.

[6] Prof. Shashank S Kadam, Ria N Choudhary, SujayDandekar, DebjeetBardhan, Namdeo B Vaidya "Electronic Voting Machine with Enhanced Security"

[7] RahilRezwan, Huzaifa Ahmed, M. R. N. Biplob, S.M. Shuvo, Md. AbdurRahman "Biometrically Secured Electronic Voting Machine"

[8] Z.A. Usmani, KaifPatanwala, MukeshPanigrahi, Ajay Nair "Multipurpose platform independent online voting system."

[9] Dr. Sanjay Sange, NMIET, Maharashtra, India "Online voting system using face recognition and OTP" Harshith K "AI EVM - An Electronic voting machine using machine learning ", Volume:04/Issue:07/July-2022 . "Smart Voting System using Deep Learning

[10] Techniques" M. Nisha P. Pooja,ETEDM – 2022 .Prof. KritiPatidar, Prof. Swapnil Jain "Decentralized E-Voting Portal Using Blockchain".

[11] Nisha P. Pooja, T. Anuja, 2022, Smart Voting System using Deep Learning Techniques, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) ETEDM – 2022 (Volume 10 – Issue 08).

[12] Roberto Olmos, Siham Tabik, and Francisco Herrera Automatic Handgun Detection Alarm in Videos Using Deep Learning Soft Computing and Intelligent Information Systems research group, Department of Computer Science and Artificial Intelligence, University of Granada, 2017. 1, 2

[13] K. Simonyan, A. Zisserman Very Deep Convolutional Networks for Large-Scale Image Recognition Visual Geometry Group, Department of Engineering Science, University of Oxford, 2015. 1, 2

[14] International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 volume: 08 Issue: 06 figure-3 citationhttps://www.citlprojects.com/blog/online-voting-system-facial-recognition-project/Evoting system for face recognition