MALAYSIAN JOURNAL OF COMPUTING AND APPLIED MATHEMATICS (2023) 6 (1) 1-9
©UNIVERSITI SULTAN ZAINAL ABIDIN
DOI: *https://doi.org/10.37231/myjcam.2023.6.1.80*

Article: Received 16.11.2022; Accepted 16.02.2023; Published 31.03.2023

A SECURE ONLINE VOTING SYSTEM USING FACE RECOGNITION TECHNOLOGY

Citra Devi Nair Appunair, Nazirah Abd Hamid, Ahmad Faisal Amri Abidin, Mohamad Afendee Mohamed, Mohd Fadzil Abdul Kadir, Siti Dhalila Mohd Satar

Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Terenganu, Malaysia
060454@putra.unisza.edu.my

Abstract: Each individual has the opportunity to choose the leaders by practicing their democratic right to vote. Therefore, the voting process is fundamental in determining everyone's destiny. The demand for online voting is growing, and most voters prefer online voting because it saves their time and energy. Therefore, an online voting method is highly valued in today's digital age. However, a lack of security and mechanism to verify and validate voters in the voting system may lead to illegitimate voting and unethical behavior. Thus, the voting issue remains a significant concern regarding safety and security. This project proposes a secure online voting system using face recognition, allowing validated users to cast a vote. The proposed online voting system uses a deep learning technique, a convolutional neural network, to verify and validate that the authorized users are voting. In conclusion, the proposed secure online voting system with biometric authentication able to verify and validate the authorized user with the accuracy rate of 90% for voting purposes and the system will be advantageous for users since it is convenient, reliable, energy-efficient, and time-saving.

Keywords: Online Voting, Face Recognition, Deep Learning Technique, Convolutional Neural Network, Biometric Authentication.

1. INTRODUCTION

Voting is a method used by groups to collectively make decisions or express opinions, and it can take various forms. One significant advancement in voting technology is online voting, also known as E-voting, which has transformed traditional voting processes. By incorporating biometrics, E-voting has provided a more secure approach to voting in democratic nations compared to paper-based voting, which is prone to insecurity [1].

Biometrics refers to the unique physical and biological characteristics of individuals. These characteristics are utilized for identification and access control purposes. Authentication is the process of verifying a user's identity. It can be achieved through three types of authentication factors: knowledge-based, property-based, and biologically based. Knowledge-based authentication relies on information known only to the user, such as passwords or PIN codes. Property-based authentication involves possessions unique to the user, such as access cards or keys. Lastly, biologically based authentication employs biometric features, which are physical or behavioral attributes unique to each individual.

Deep learning is a subset of Machine Learning that utilizes multi-layered neural networks to process and analyze vast amounts of data. It mimics the functioning of the human brain. Deep learning algorithms can learn and extract meaningful information from both structured and unstructured data. Supervised and unsupervised learning are the two primary categories of deep learning, each with its own set of algorithms [2]. Supervised learning varies based on training data that has been labelled, whereas unsupervised learning works with raw data. In this study, the focus is on supervised deep learning, specifically the Convolutional Neural Network (CNN). CNNs are specialized network models used for processing pixel input, particularly in image recognition tasks. They excel in computer vision applications and play a vital role in accurate object recognition, such as facial recognition [3].

The main objective of the study is to design an online voting system that can authenticate and validate legitimate users with the integration of a face recognition technology. The next objective is to develop a face recognition online voting system using the CNN algorithm. Lastly, to test the accuracy of the online voting system to authenticate users.

This paper is structured into several sections. In Section 1, a brief introduction is provided, explaining the online voting system and discussing the use of biometric authentication and the CNN deep learning algorithm. Section 2 focuses on related works and includes a literature review to provide background information. In Section 3, the proposed work is outlined, encompassing the system overview and design methodology. Section 4 is dedicated to the discussion of the study's findings and results, offering an analysis and interpretation of the data and the conclusion is presented in Section 5.

2. RELATED WORKS

2.1 Access Control

In the modern era, there is a wide range of access control methods available to ensure enhanced security measures. Many of these methods rely on biometric verification [4]. According to a research paper [5], the implementation of access control measures is crucial for maintaining security in the context of voters and officials. Therefore, it is imperative to establish suitable access control tools. Access control encompasses various stages, including identification, authentication, authorization, and accountability.

2.2 Biometric

Biometrics refers to the distinct physical and biological characteristics unique to each individual. These traits include various types, such as facial recognition, fingerprint recognition, palm print recognition and iris recognition [1]. According to [6], every person possesses exclusive biometric properties like fingerprints, iris patterns, gaits, voice, and facial features that cannot be replicated by anyone else.

According to Rasheed [7], biometric systems are pattern recognition systems that confirm the veracity of particular physiological or behavioral characteristics displayed by a user. An effective biometric system ensures that the biometric information originates from a live individual at the time of verification and matches the stored master biometric data.

In contrast, token-based systems and knowledge-based systems pose significant risks, such as the potential for passwords to be stolen or forgotten. Consequently, biometric systems are widely utilized in various applications, including access control, automated banking, criminal identification and autonomous vending. This is primarily due to the unique and non-transferable nature of biometric features [8].

Utilizing the fact that biometric and facial features are difficult to share or duplicate, [9] research proposes a system to enhance voter identification through biometric facial recognition. According to [1] research, environmental factors during the image acquisition phase and the quality algorithms used to evaluate image quality can influence the performance of a biometric system.

2.3 Authentication

Authentication, often referred to as identification, involves a one-to-one comparison between the user's biometric sample and the pre-stored information [1]. As mentioned in a research paper [8], a highly accurate human identity authentication system has become crucial in today's context due to the rise in identity fraud-related crimes and losses. A study by [9] emphasize the significance of their project, which incorporates a two-factor authentication approach to facilitate seamless and precise voter verification.

Multiple studies have demonstrated that inherence-based authentication, such as biometric authentication, addresses the challenges and issues associated with knowledge-based authentication methods like passwords and tokens. By implementing inherence-based authentication, system security can be enhanced. Moreover, user preference leans towards biometric authentication over PIN or passwords, as it is deemed more secure, despite 93.51% of respondents still utilizing the PIN/password approach, as revealed in a study conducted by [10]. Therefore, incorporating biometric authentication instils greater trust among users, as it offers enhanced security and augments the system's overall usability.

2.4 Face recognition

Face recognition has become a widely adopted access control method in various domains, including public security, daily life, military areas, and banks. It leverages computer vision technology to identify individuals based on their facial features. The facial recognition system matches a person's face captured in a digital image or video frame against a database of stored faces, typically used for user authentication and ID verification services. Nowadays, face recognition is considered a reliable and accurate access control technique, often used in conjunction with other biometric methods.Facial recognition involves the process of identifying a person's face from a collection of stored face samples within the system. This is achieved by converting images into digital binary representations and extracting relevant features using various techniques. With the advancements in deep learning, face recognition based on Convolutional Neural Networks (CNN) has emerged as a prominent approach in the field of face recognition [11].

As discussed in [8] research, face recognition entails the automated detection and recognition of objects such as human faces, animals, or other entities using computer-based processes. Facial recognition has been the focus of research in fields such as pattern recognition, image processing, and machine vision for decades. As a unique biometric feature, the face possesses inherent stability and distinctive characteristics, making it an ideal basis for identity verification.

The study by [9] proposes a system that employs a face recognition algorithm for voter verification of identification in an effort to increase the electoral process's security. Their system offers an online platform that allows eligible electors to exercise their right to vote from any location. They've implemented face recognition authentication using TensorFlow.js and DeepFace because these technologies provide enhanced security, simplicity of integration, and automated identification.

2.5 Online voting

Making use of an online system would make an application more accessible, efficient, and practical. On a global scale online voting systems have been implemented. Online voting systems are a subset of electronic voting (E-voting), which is comprised of four distinct subsets, including Direct recording electronic (DRE) voting machines, Optical Mark Reader (OMR) systems, Electronic ballot printers (EBPs), and Internet voting systems (I-Voting). I-Voting refers to an online voting system in which ballots are cast via the Internet [10]. As highlighted by [1], E-voting, particularly when coupled with biometrics, has revolutionized traditional voting methods. It offers a more secure approach to voting in democratic countries compared to the traditional paper-based and insecure voting systems.

The focus of the paper [12] centres on a system that allows users to vote remotely using their computers or mobile phones, eliminating the need for voters to physically visit polling stations. This system employs a two-step authentication process involving face recognition and a One-Time Password (OTP). By using an online voting system, the entire voting procedure for an election is conducted over the internet and is only enabled during the election's scheduled time. The paper by [12] also stated that an online voting system significantly reduces the chaos associated with traditional elections while saving labour, money, and time.

The study by [13] emphasizes that this system eliminates the requirement for election officials, paper ballots, or electronic voting machines. A webcam is the primary hardware needed for online voting. The introduction of online voting systems addresses the drawbacks of conventional voting methods, providing benefits such as accuracy, security, flexibility, and mobility. The research by [14] presents an online voting system as a web-based application designed for integration into the election process, offering a more efficient and modern approach.

2.6 Convolutional Neural Network (CNN)

Convolutional Neural Networks (CNNs) are a specialized type of deep learning neural network primarily used for image classification [11]. Their effectiveness and improved performance in competitions have made them a prominent area of research. CNNs are known for their reliability, accuracy, and ability to minimize data pre-processing [11]. The main objective of CNNs is to identify patterns within extracted image pixels, enabling accurate classification of images into their respective classes.

CNNs are inspired by human neural networks and can be divided into two types of layers, which are the image feature extraction layer and the classification layer [8]. The image feature extraction layer, situated at the initial stage of the architecture, is composed of numerous layers of neurons connected to local regions of the previous layer. The classification layer, comprising several fully connected layers, receives input from the output layer of the feature extraction process and transforms it using additional hidden layers, similar to Multilayer Perceptron networks. Overall, CNNs gradually transform the original image from pixel values to class scoring values for classification. The use of CNNs in automatic voting systems simplifies the voting process by minimizing human intervention [13].

3. PROPOSED WORK

3.1 System Overview

The proposed system was built using the Django framework, Python, and Visual Studio code. The system takes images of electors as input and uses them to train and predict output using OpenCV and PyTorch. Moreover, the MySQL database is used to store the voter's registered image and details, the voter's captured face image for verification, and also voting responses. This system's primary purpose is to ensure that online voting takes place ethically and to authenticate electors using facial recognition technology.

Figure 1 depicts the implementation approach for the online voting system using face recognition technology.

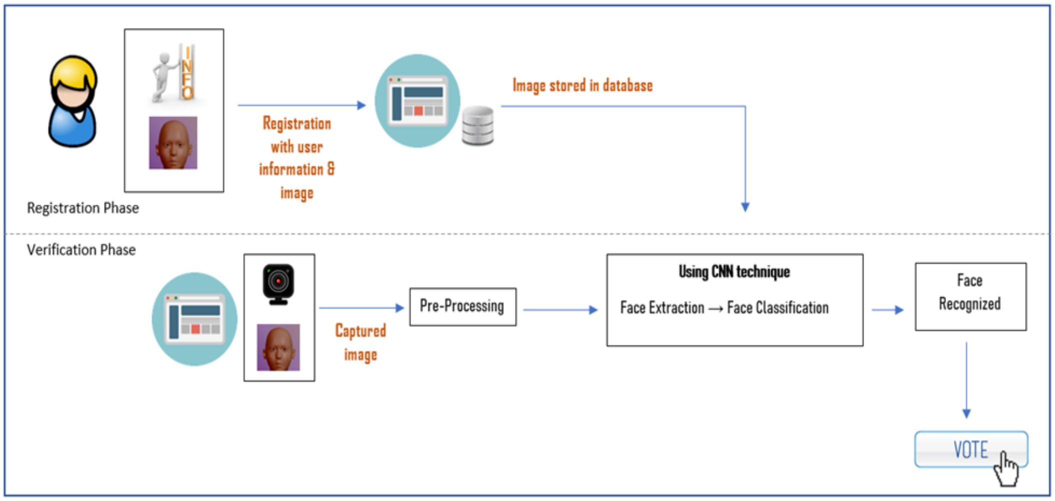


Figure 1. System framework of the online voting system using face recognition technology

As demonstrated in Figure 1, the proposed system encompasses two phases, registration phase and the verification phase. At the registration phase, users are required to enter their information and an image of their face in order to be registered in the system. Once the user inputs their image at the registration page, it performs face detection by using the Haar Cascade classifier, which is imported from OpenCV. If the user's image is detected, the information and facial image collected during the registration process will then be saved to a database. The facial image entered during this step will thereafter be used for authentication. The subsequent phase is the verification phase, which occurs when a person logs into the system to vote. When a user accesses the system to cast a vote, his or her face image is captured for verification purposes. After an image has been captured, it will undergo pre-processing, which includes face detection, resizing, and normalization. Following pre-processing, the CNN technique will be utilized for face extraction and classification. At this stage, both the database-stored face image and the face image obtained at user login will be used for classification. Next, classification is performed by comparing the acquired image to the user's image in the database. If the features match, the face image is recognised, and the voter is authorized to cast a vote.

3.2 Design Methodology

3.2.1 Dataset collection

To train the face recognition model, a dataset was collected from 50 voters. Using the OpenCV module of the Python programming language, 30 photos were captured of each voter to collect their images. The dataset is created by saving the captured image in a file directory by creating a separate folder for each user, and it is saved with their respective names.

3.2.2 Image preprocessing

There are several preprocessing steps that are applied to the input images, which are the dataset images, before training the face recognition CNN model. First, the images are resized to a fixed size of 224 x 224 pixels. Then, the images are transformed into PyTorch tensors using the ToTensor transformation, which converts the pixel values to a normalized range of 0, 1 and rearranges the dimensions to channels, height, and width. Finally, the pixel values of the images are further normalized using the normalize transformation, which subtracts the mean, 0.5, and divides by the standard deviation, 0.5, for each color channel. These preprocessing steps ensure that the input images are in a consistent format and have a standardized range of values, which can help improve the training process and model performance.

3.2.3 Architecture of Convolutional Neural Network (CNN)

CNN's architecture is comprised of a variety of multi-building block layers. CNN consists of several convolution layers, followed by subsampling pooling layers and Fully Connected (FC) layers. For the proposed system, the ResNet-18 model is used as the architecture of the CNN to train the model. ResNet-18 is a deep neural network architecture commonly used for image classification tasks. It comprises two main parts, which are feature extraction and classification.

The first layer is composed of the convolutional layers in the ResNet-18 backbone, which involve feature extraction. These convolutional layers are accountable for extracting essential features from the input face images. The feature extraction backbone is initialized with a ResNet-18 model obtained from the torch vision models module. They employ learnable filters, known as kernels. The kernels slide over the input images, perform convolution operations by scanning the images to detect patterns and features at various scales and orientations. It is composed of multiple convolutional layers. To train the model, the weights are initialized randomly while creating the model.

By using ResNet's architecture, downsampling is performed by utilizing convolutional layers with a stride of 2 and bottleneck blocks that include downsampling operations. This downsampling minimizes the spatial size of the feature maps, helping the model focus on the most important features while also reducing computational complexity.

Following the feature extraction step, the Rectified Linear Unit (ReLU) activation function is utilized. The output from the feature extraction backbone is passed through a ReLU activation function to introduce non-linearity to the model. It takes the output of the convolutional layers and applies a non-linear transformation by replacing any negative values with zeros, while leaving positive values unchanged. This non-linearity improves the model's ability to discover intricate relationships between extracted features and classes.

The last layer is the classifier layer, which comes after the application of the ReLU activation function. This fully connected linear layer is responsible for classification and maps the output from the ReLU activation layer to the number of classes in the face recognition task. By learning the weights of this layer during training, the model is able to find the optimal mapping between the extracted features and the target classes. The output of the linear classifier layer represents the model's predicted probabilities or scores for each class, providing the ability to identify the most probable class for a given input face image.

3.2.4 Integration of Convolutional Neural Network (CNN) Model for Face Recognition

The online voting system uses face recognition technology, using CNN to perform the face recognition task. After the face recognition model has been trained using the input dataset, it is integrated into the voting system to detect and verify the faces of authenticated voters, assuring that they only vote once.

During the voting process, the system employs the pre-trained face recognition model to perform face recognition on the preprocessed face image of the voter. The face image is first preprocessed using a series of transformations, including resizing, converting to a tensor, and normalizing the pixel values. These transformations ensure that the input image is compatible with the model's requirements.

Next, the preprocessed face image is passed through the trained face recognition model. The model analyses the facial features and extracts relevant information to generate a numerical representation of the face, often referred to as face embeddings or feature vectors. These embeddings capture unique characteristics of the face that can be used for identification purposes.

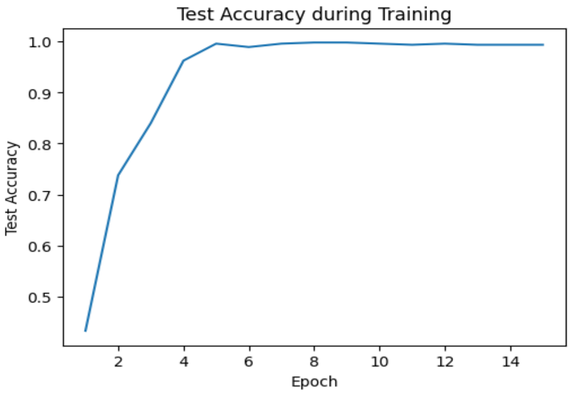
The system then compares the extracted face embeddings with the embeddings of previously registered voters stored in the system's database. This comparison is performed using metrics, such as Euclidean distance and cosine similarity. By measuring the similarity between the face embeddings, the system can determine whether the detected face corresponds to an authenticated voter.

If the similarity exceeds a certain threshold, indicating a high degree of resemblance, the system verifies the voter's identity and allows them to proceed with casting their vote. This ensures that only eligible and verified electors can take part in the voting process. On the other hand, if the similarity falls below the threshold, the system rejects the face as unrecognized, preventing unauthorized individuals from voting.

4 RESULTS AND DISCUSSION

4.1 Discussion

The performance of the face recognition system, designed to authenticate valid users, has been tested for the proposed system. After training and testing the model using the dataset, graph 1 was generated to evaluate the performance of the trained face recognition model on the test data.



Graph 1. Test accuracy during CNN model training

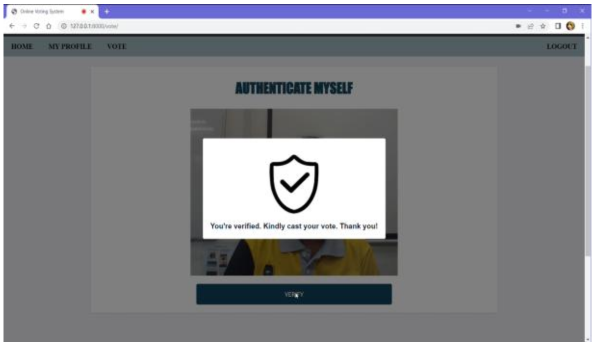
Graph 1 depicts the accuracy of the test dataset during training. After each epoch, the testing dataset is used to measure the accuracy, and it achieves an accuracy rate of approximately 99% at the end of the epochs.

Next, the trained model is integrated into the voting system in real-time to perform the task of face recognition, thereby authenticating legitimate voters to access their voting sessions and cast their votes. To evaluate the accuracy of the system in authenticating valid voters, 20 voters have been enrolled in the system.

The performance of the system is measured using various evaluation metrics, including accuracy, precision, recall, and F1 score. To calculate these metrics, the values such as True Positive (TP), True

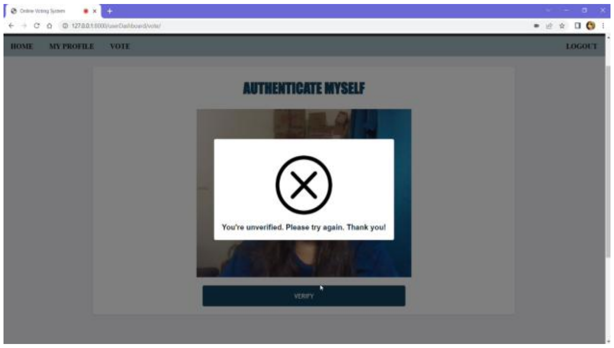
Negative (TN), False Positive (FP), and False Negative (FN) are counted from the sample of testing users. For testing purposes, each user account was used for two trials, where trial 1 was enrolled by the correct user while trial 2 was enrolled by a different user.

To perform the testing on the verification module, the user is required to enrol in the system. The verification of the voter is performed on the vote page. After the user clicks the "Verify" button, a pop-up box displays the result. If the user is verified, the result is displayed as shown in figure 2. If the user is not verified, the result is displayed as unverified.



You're verified. Kindly cast your vote. Thank you!

Figure 2. Result of verified



You're unverified. Please try again. Thank you!

Figure 3. Result of unverified

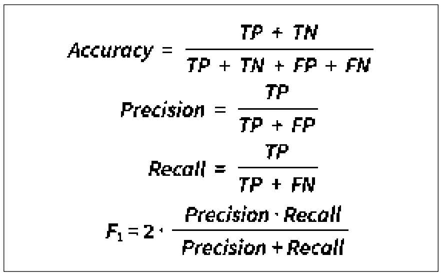
If the user's face is not detected or multiple user faces are detected, an error message will be displayed.

Table 2 represents the result of the testing conducted among 20 sample voters.

Table 2. Result of Testing

Voter	Trial 1	Trial 2
1	TP	TN
2	FN	TN
3	TP	TN
4	TP	TN
5	TP	TN
6	TP	TN
7	TP	FP
8	TP	TN
9	TP	FP
10	TP	TN
11	TP	TN
12	TP	TN
13	TP	TN
14	TP	TN
15	TP	FP
16	TP	TN
17	TP	TN
18	TP	TN
19	TP	TN
20	TP	TN

Based on the results of the testing, a confusion matrix table is generated. The evaluation metrics, including accuracy, precision, recall, and F1-score, are calculated using the values of TP, TN, FP, and FN. The formula shown in Figure 4 is used to calculate the evaluation metrics.



$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

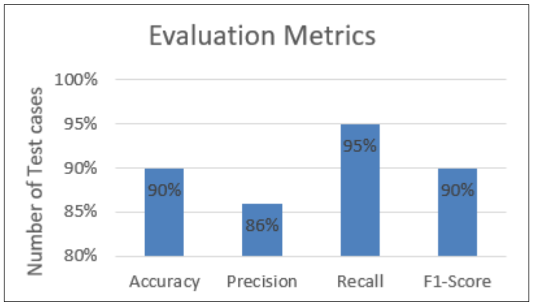
$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F_1 = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}$$

Figure 4. Formula of the evaluation metrics

By using the formula, the evaluation metrics are calculated, and graph 2 is illustrated.



Graph 2. Result of evaluation metrics

According to the results generated, the system has demonstrated an accuracy of approximately 90% in authenticating legitimate voters.

5. CONCLUSION

In this study, the development of a secure online voting system that utilizes face recognition technology is proposed. To provide a secure environment for voting, biometric-based access control has been implemented for the voting system's authentication. By using this proposed system, voters are able to cast their ballots in a secure setting as well as in a comfortable manner, as it is not necessary to visit a polling booth, and the issue of time and energy consumption could be eliminated. The implementation process includes the collection of datasets, image preprocessing, CNN based face recognition model training, and real time face recognition tasks in the voting system. With this implementation, an average recognition accuracy of 90% is achieved. It can be concluded that a secure voting system with CNN-based face recognition technology is able to authenticate the identity of an authorized voter, thereby preventing an unauthorized user from casting a vote. It also ensures the voter's legitimacy and the security of the voting process.

References

[1] K. Okokpujie et al., “A secured automated bimodal biometric electronic voting system,” IAES International Journal of Artificial Intelligence, vol. 10, no. 1, p. 1, 2021. doi:10.11591/ijai.v10.i1.pp1-8.

[2] J. Sharma, “Introduction to supervised deep learning algorithms,” Analytics Vidhya, https://www.analyticsvidhya.com/blog/2021/05/introduction-to-supervised-deep-learning-algorithms (accessed Jul. 4, 2023).

[3] R. Awati, “What are convolutional neural networks?: Definition from TechTarget,” Enterprise AI, https://www.techtarget.com/searchenterpriseai/definition/convolutional-neural-network (accessed Jul. 4, 2023).

[4] S. Domakonda, D. Nishitha, A. Y. Kumar, A. S. Rao, and A. Sindhu, “E-Voting System Using Facial Recognition,” The International journal of analytical and experimental modal analysis, vol. XIV, no. VI, June/2022, pp. 1191–1201.

[5] H. Alamleh and A. A. AlQahtani, “Analysis of the design requirements for remote internet-based E-Voting Systems,” 2021 IEEE World AI IoT Congress (AIIoT), 2021. doi:10.1109/aiiot52608.2021.9454194.

[6] A. K. Kothawade, A. V. Bhopale, A. Y. S. Patil, P. Shewale, and D. Mahajan, “A Novel Method of E-Voting System Using Biometrics Thumb Impression and Face Recognition,” International Journal on Data Science and Machine Learning with Applications, vol. 1, no. 1, May 2021, pp. 37–40.

[7] M. M. Rasheed, “Secure Electronic Voting System using swarm intelligence,” Journal of Physics: Conference Series, vol. 1999, no. 1, p. 012137, 2021. doi:10.1088/1742-6596/1999/1/012137.

[8] E. Fernando, D. Andwiyan, D. Fitria Murad, D. Touriano, and M. Irsan, “Face recognition system using deep neural network with Convolutional Neural Networks,” Journal of Physics: Conference Series, vol. 1235, no. 1, p. 012004, 2019. doi:10.1088/1742-6596/1235/1/012004.

[9] M. Mehta, M. Lalwani, and A. Harle, “Online voting system,” International Journal for Research in Applied Science and Engineering Technology, vol. 10, no. 5, pp. 1471–1476, 2022. doi:10.22214/ijraset.2022.42552.

[10] M. M. K M. M. Sulaiman, et al. "An Online Voting System using Face Recognition for Campus Election." Journal of Advanced Computing Technology and Application 3.1, 2021, pp. 39-46.

[11] V. Ganesh, R. Sansare, T. Padelkar, and V. Shinde, “Real Time Face Recognition System Using Convolutional Neural Network,” International Journal of Creative Research Thoughts, vol. 10, no. 4 April 2022.

[12] S. Ganesh Prabhu et al., “Smart online voting system,” 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021. doi:10.1109/icaccs51430.2021.9441818.

[13] M S Sruthi and K Shanjai, “Retraction: Automatic voting system using Convolutional Neural Network (J. Phys.: Conf. Ser. 1916 012074),” Journal of Physics: Conference Series, vol. 1916, no. 1, p. 012314, 2021. doi:10.1088/1742-6596/1916/1/012314.

[14] A. Behrainwala, A. Saxena, A. Navlani, S. Sahay, N. Tarapore, “Smart voting system using facial recognition,” International Journal for Research in Applied Science and Engineering Technology, vol. 10, no. 1, pp. 308–313, 2022. doi:10.22214/ijraset.2022.39810