https://doi.org/ 10.33472/AFJBS.6.5.2024. 6721-6728

African Journal of Biological Sciences

Modernizing Voting System : MT-CNN Based Face Recognition Voting System

Vaibhav Gupta
CSE Department
AKGEC Ghaziabad, India
vaibhavgupta6395@gmail.com

Dr. Harnit Saini
CSE Department
AKGEC Ghaziabad, India
harnitsaini2012@gmail.com

Utkarsh Kumar Singh
CSE Department
AKGEC Ghaziabad, India
utkarshsingh100.us@gmail.com

Vineet Gupta
CSE Department
AKGEC Ghaziabad, India
vineetgupta2824@gmail.com

Utkarsh Singh
CSE Department
AKGEC Ghaziabad, India
9utkarshsingh9@gmail.com

Sakshi Singh
CSE Department
AKGEC Ghaziabad, India
0111sakshirai@gmail.com

Article History
Volume 6, Issue 5, 2024
Received: 15 May 2024
Accepted: 22 May 2024
doi: ***10.33472/AFJBS.6.5.2024. 6721-6728***

***Abstract*—**

Maintaining the integrity and fairness of elections depends on the validity of voter identification, especially in situ- ations where voting is done remotely. In situations where strong cryptographic methods are not accessible, biometrics becomes a feasible substitute. This study investigates the application of facial recognition technology for distant voter identification. It looks at the architectural choices, technical complexities, and lingering issues, such as privacy concerns and dispute settlement. The research suggests integrating strong anti-spoofing strategies into facial recognition systems to combat fraudulent attempts, such as presentation attacks that use fictitious images or movies. The Multi-Task Cascaded Convolutional Neural Network (MTCNN) model, which is well-known for its effectiveness in facial detection and alignment tasks, is a key component of this methodology. Additionally, the paper addresses the integration of feature extraction techniques based on deep learning.

***Index Terms*—**

Smart Voting System, Multi-Task Cascaded Convolutional Neural Network (MTCNN), Connectionist Tem- poral Categorical (CTC) loss, Deep Learning (DL).

I. Introduction

Voting is a process that allows a group, such an electorate or gathering, to decide as a whole or to voice a viewpoint. In smaller organizations, voting often takes place after discussions, debates, or election campaigns. officially through voting to select people for positions, such as those in a political organization, the workplace, or other affiliations. Informal voting can take place electronically, verbally, or with a gesture like raising a hand. In a democracy, the voter selects a government by casting ballots in an election, which allows them to select one candidate from a field of candidates.[1]

A. Background of the Problem of the Traditional Voting System for Digitization

Voting system improvement proposals have been around for a while, having started with the formal study of voting systems in the 18th century. The use of technological technologies to improve voting has been the subject of numerous study. It is essential to make sure that voting chores are carried out electronically without jeopardizing voter privacy or opening the door to fraud when designing an electronic voting system.[2] There were 11 lakhs cases of bogus votes in Delhi, according to documents from the Times of India dated January 24, 2009. Furthermore, 30,000 illegal voters were found in Sheila Dikshit's constituency under the election commission, according to a June 2013 report by India News. Ram Vilas Paswan, the chief of the Lok Janshakti Party, made another accusation, saying that 30% of the voter cards used in the Bihar elections were forged. Depending on the office up for election, such as local, state, or federal government, elections may be public or private. Voters in conventional paper-based elections place their ballots in sealed boxes positioned throughout several electoral circuits. These boxes containing ballot control units are opened after the voting time finishes, and ballots are hand counted in front of certified.

B. Objective of the research

Enhancing the voting process's accessibility, security, and efficiency is the goal of putting face recognition technology into an online voting system. The following are the main goalsof such a system:

1) Enhanced Security: The online voting process is made even more secure by the use of facial recognition technology. The technology can lessen the possibil- ity of electoral fraud by preventing impersonation and unauthorized access to voting accounts by using facial biometrics to authenticate voters' identities.
2) Increased Accuracy: By precisely matching a person's face to their registered identity, facial recognition tech- nology helps to lower the possibility of voter authenti- cation errors. This ensures that only eligible voters may participate and that each voter may only cast one vote, which contributes to the integrity of the voting process.
3) Simplified Authentication: Passwords and personal iden- tification numbers (PINs), which are susceptible to loss or abuse, are frequently used as authentication in tra- ditional online voting systems. By removing the need for users to memorize and enter complicated passwords or codes, face recognition technology provides a more seamless and intuitive authentication process.
4) Transparency and Auditability: The system is able to keep track of voter actions, including voting records that are connected to confirmed identities and authentication logs. This improves electoral accountability and trans- parency by enabling stakeholders and election authori- ties to safely audit and confirm voting procedures.
5) Data Protection: To protect voters' biometric data and personal information, face recognition technology must be implemented in online voting systems with strong data protection mechanisms in place. The goal entails putting encryption, access controls, and safe storage pro- cedures into place as well as making sure that pertinent data protection laws are followed.
6) Public Trust: In order for the internet voting system to be accepted and used, the public's trust must be increased. The aim is to develop and implement the system in a manner that fosters openness, impartiality, and de- pendability while attending to worries regarding safety, confidentiality, and the precision of election outcomes.

The overall goal of an online voting system that makes use of facial recognition technology is to use creative problem- solving to bring the voting process up to date, encourage inclusivity, and preserve democratic election principles while upholding strict security and integrity guidelines.

II. LITERATURE REVIEW

In accordance with the Indian Constitution, the Election Commission of India (ECI) is mandated to hold free and fair elections on a regular basis. In order to assure effectiveness, reduced time consumption, and lower costs, advanced tech- nology have been included into the electoral process over the past ten years.To effectively verify each voter's vote, the ECI now uses an Electronic Voting Machine (EVM) in conjunction with the Voter-Verified Paper Audit Trail (VVPAT). Even yet, the ECI finds it difficult to prevent electoral misconduct while validating voters using an electoral list. The EVM has a face recognition device integrated in order to solve these problems. In a democratic nation, the ECI aims to surpass ninety-five percent in polls. Currently, not all election kinds have an average polling rate of just seventy percent. People moving between states and abroad in search of work makes it impossible for the ECI to meet its goal[3].A democracy's foundation and structure are its elections. In recent decades, there have been numerous effective modifications to the elec- toral system. The largest majority rule nation in the world, India, still conducts its elections using either Electronic Voting Machines (EVM) or Secret Ballot Voting (SBV), both of which are wasteful, expensive, and require a lot of human labor. Only identity proof was validated in the current system, increasing the possibility of fraudulent voting. We created a web-based smart voting system and a revolutionary face detection and recognition technique in order to prevent the aforementioned problems. The complete internet system gives people the ability to safeguard their votes from anywhere in the world.Voter fraud is reduced when the ID of appearances is used, and voters who are recognized by the system and who are enrolled in the political contest are allowed to cast ballots. As a result, the methodology renders the framework the best means of making a decision [4]. Voters can cast their ballots from anywhere in the world thanks to a web-based method. An online platform features an avoidable IP address created by the Indian government for electoral purposes. The name and address should be entered into the website by users. Voters will provide their fingerprints and facial images to the election commission. The photos will be stored on the server or database. On casting day, the photos are collected, compared to a database, and a safe voting system is provided on election day. Similar to how mobile phones are used, the voting system is unlocked using faces and fingerprints. Many voters find it bothersome as the existing system requires them to be physically present when casting their ballot. Additionally, the process takes less time. It is possible to lower the quantity of phony voters by using facial and fingerprint image detection. To increase system security, the space between the eyebrows and eyes doesn't change as one gets older. Ten print images are used in this study to identify the voter's proper name.[5] Blockchain is used to store data that is extremely secure and nearly hard to alter or tamper with. In any country, voting is a necessary activity, and it will be detrimental if votes are tallied incorrectly by outside sources. In order to prevent these kinds of circumstances and enhance comfort, blockchain technology is acknowledged. This study suggests a blockchain-based decentralized national electronic voting system. An admin panel is included to arrange the vote, oversee the candidates, and announce the results. During voting, people will be able to input their Aadhaar card ID through text input on the web application and upload a photo of themselves. When a voter enters their Aadhaar card ID, their eligibility will be verified. One Time Passwords (OTPs) will be used to verify the phone numbers of eligible voters. Voter eligibility will be deemed for each individual voter following voter verification. A front- and web-cam will be used to watch voters during the voting process. Because the votes will be kept on a blockchain, any tampering will be readily discovered. The matching constituency and the address will be verified in the backend. The administrator will announce the voting results on a designated day. The outcomes will be presented visually, offering a range of options together with historical data and statistics.[6] The sole voting method available in India is offline, which is inefficient because it takes a lot of labor and longer to process and publish the results. Therefore, a change that addresses these issues is necessary for the system to become effective. The new procedure makes voting easier by not requiring a voter's physical appearance. This paper focuses on a system that employs two-step authentication with face recognition and an OTP system to allow users to vote remotely from any location using a computer or mobile device. This eliminates the need for voters to physically visit the polls. If it is more comfortable for the user, this project also enables offline voting.The face scanning system is helpful when voting because it records voters' faces before the election. RFID tags, not voter ID, are used to improve the offline voting system. Additionally, this approach allows citizens to view the results at any moment, preventing circumstances that could lead to vote rigging.[7] Voting can be done electronically using an electronic voting machine (EVM) or on ballot paper. Voting in any manner carries the risk of allowing someone to abuse the other votes. As a result, this research study suggests using a fingerprint sensor to collect and extract voter fingerprints, which will then be stored in a database for voter registration and authentication procedures. Multiple registrations from the same person will be prevented by storing the information in the database. Each voter must scan their fingerprint at the polling place or on election day, and if their fingerprint is included in the fingerprint database, it will be matched with it. Many duplicate registrations can be prevented by using the voter identity number and fingerprint, which will increase the likelihood that voters will actually be successful when casting their ballots. Through the use of their voter ID, authentication replies provided at enrollment, and an instant token key provided to each member via the specifically created election web module, voters can cast their ballots from anywhere in the world. The token will be sent to the associated candidate's email address by the administrator.The project that was suggested has been carried out. [8]

III. METHODOLOGY

In our system, the machine learning model for an intelligent voting system was trained just using specified datasets. For preparing the photos, Python was used in conjunction with packages such as OpenCV, PIL, and NumPy. To prepare the images for machine learning algorithms, preprocessing tech- niques include noise reduction, scaling, and normalization. Our method uses the MTCNN algorithm to power the intelligent voting system. A complex deep learning technique called MTCNN (Multi-task Cascaded Convolutional Networks) is made for face detection and alignment, but it may also be modified for other image recognition applications. The MTCNN algorithm was trained using the chosen datasets. The preprocessed photos were fed into the algorithm during the training phase, enabling it to pick up on and recognize the essential characteristics for the intelligent voting system. Because of this, we have developed a recognition system that is both thorough and skilled in its capacity to correctly identify and process the images needed for the intelligentvoting system.

A. Explanation of the Approach Used

Important findings from the literature review guided the development of a robust quantitative methodology. The selection of deep learning, specifically MTCNN, was predicated on its shown efficacy in picture recognition and feature extraction tasks. The system is able to recognize and align face features with accuracy thanks to the MTCNN algorithm. It can also handle varying conditions in the photos and adjust to the unique characteristics that each person exhibits. This method offers a well-rounded and original solution for the challenging problem of picture recognition in a smart voting system. The accuracy with which the MTCNN algorithm can process and interpret images guarantees that voters can be properly identified and authenticated, hence enhancing the voting process's integrity and efficiency.

B. Description of the Data Collection Process

The process of data collection is fundamental in research, encompassing the gathering and refinement of diverse data sources to ensure their suitability for analysis. At the outset, our data collection efforts span various channels, necessitating meticulous processing to align them with the requirements of machine learning and deep learning models, which predomi- nantly operate on numerical data rather than raw images.

1) Dimensionality Reduction: Recognizing the impact of extraneous features on computational efficiency, we prioritize the extraction of facial landmarks through the MTCNN model. This selective approach ensures that only pertinent information is retained, facilitating streamlined processing in subsequent stages.

2) Noise Removal: Ensuring data integrity is paramount; hence, the elimination of noise is imperative. Leveraging the capabilities of the MTCNN model, we refine the dataset by identifying and mitigating noise present in images. By systematically removing or cropping noisy images, we enhance the quality of the dataset, thereby optimizing its suitability for downstream analyses.

3) Pixel Brightness Transformations: The manipulation of pixel brightness is pivotal in enhancing image quality and en- suring consistency across datasets. Through tailored brightness transformations informed by the MTCNN model's output, we preserve color integrity and rectify inconsistencies, thereby en- hancing the overall quality of the data. This process facilitates effective color correction and transformation operations, augmenting the dataset's compatibility with subsequent analyticaltasks.

By incorporating the MTCNN model into our data collec- tion process, we bolster the quality and relevance of the col- lected data, thereby fortifying its compatibility with machine learning and deep learning frameworks. These preprocessing steps serve as a foundational framework for subsequent anal- yses, laying the groundwork for comprehensive research and model development.

C. Overview of the Techniques and Algorithms Employed for Smart Voting

1) Explanation of the chosen techniques and algorithms: For the smart voting system, the research makes use of an MTCNN network. For precise facial feature recog- nition and processing in a variety of scenarios, this model is essential. In order to ensure accurate voteridentification and authentication in the smart voting system, MTCNN excels at face detection and feature alignment. The system's strong performance in real-world circumstances is ensured by its ability to manage a wide range of facial variances through the utilizationof MTCNN.
2) Data Preparation and Standardization: To lay a solid basis for model training, great care in data preparation was prioritized in the project's early phases. The CSV file from which the dataset was derived was thoroughly cleaned, with missing values eliminated and IDs filtered to have a maximum character length of 10. This main- tained consistency across the dataset and efficiently con- trolled computational complexity. Moreover, dictionaries for character-to-label mapping made it easier to convert textual data into a numerical format so the model could understand it. By offering a solid dataset that is tailored for machine learning, this foundational effort paved the way for the development of more sophisticated models.
3) Image Preprocessing and Data Augmentation: Later work focused on preprocessing and augmentation of images, made easier by the creation of a custom "Data- Generator" class. This course played a key role in batch processing the data, which improved memory management in the model-training stage. It made it possible to apply important preprocessing methods, such as shrinking photographs and normalizing pixel values, which were essential for getting the images ready for the model. It was via this preparation that the learning efficacy of the model was increased. The augmentation method also added unpredictability to the data, which greatly improved the model's capacity for generalization. This project phase highlighted the preparation and im- plementation of preprocessing techniques, which greatlyenhanced the resilience of the model.
4) Building the Model: A key component of this effort was the MTCNN model architecture, which integrated convolutional layers to represent the preliminary work needed for feature extraction. The learning process was made simpler by the deliberate addition of a CTC layer, which enabled sequence recognition without ex- plicit segmentation. The model was assembled using a suitable optimizer and then trained on a ready-made data generator for both validation and training. Training produced encouraging results; later stages of evaluation and prediction showed that the model could effectively translate handwritten text into a format that was read- able by humans. This all-encompassing strategy, which includes everything from data preparation to model evaluation, highlights the project's accomplishment in applying deep learning to the problem of voting sys- tem and demonstrates the methodological soundness and academic rigor of computational research.
5) Mathematical Foundations of the MT-CNN Approach: Using a rough-to-fine technique, the MTCNN algorithm scales the image to a variety of sizes for each network layer's input. It makes use of three networks with a range of detection accuracies, from bad to

good. The algorithm uses three convolutional neural networks in a cascade structure to accomplish its multi-task detection goals. Face feature point positioning, face boundary regression, and face identification are some of these challenges. The loss functions are modified to account for the various activities, as they necessitate unique training labels.

The two-class crossentropy loss function is applied to the face identification task: Among them, pi represents

$$L_{\mathrm{i}}^{\det} = -\left(y_i^{\det}\log\left(p_i\right) + \left(1 - y_i^{\det}\right)\left(1 - \log\left(p_i\right)\right)\right). \qquad \textbf{(1)}$$

the possibility that the sample xi is a human face, and det yi is 0 or 1. The bounding box regression and key point tasks use the L2 loss function: Where det

$$L_{\mathrm{i}}^{\det} = \| \hat{y}_i^{\det} - y_i^{\det} \|_2^2 . \qquad \textbf{(2)}$$

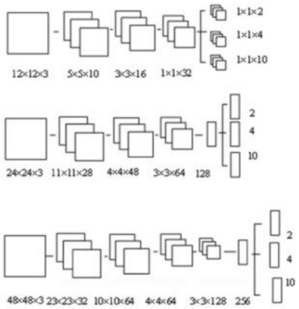
yi is the regression box of network output and det yi is the true value. Among them, y landmark i is

$$L_{\mathrm{i}}^{landmark} = \| \hat{y}_i^{landmark} - y_i^{landmark} \|_2^2 . \qquad \textbf{(3)}$$

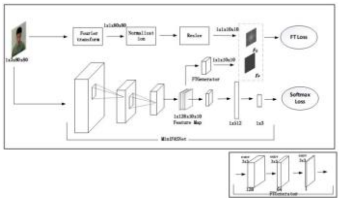
the key point coordinates of the network output, and i landmark L is the true value. The total loss function is: Where j represents the importance of different tasks,

$$\mathrm{loss} = \sum_{i=1}^{N} \sum_{j \in \{\det, bbox, landmark\}} \alpha_j \beta_i^j L_i^j . \qquad \textbf{(4)}$$

i j is an indicator of sample type, and i j L has different loss functions in different training samples. By choosing challenging training samples throughout the training phase, the MTCNN algorithm uses online hard sample training to accelerate network convergence. Only these hard samples are used for training during backpropagation once the top 70% most difficult exam- ples for each minibatch are determined using forward propagation loss.In order to complete related tasks, the MTCNN algorithm operates via a cascade of three networks. The first step is data preparation, where the original image is scaled to different sizes using a pre-determined scale factor to build an image pyramid. The network cascade then receives this image pyramid as input. PNet (Proposal Network): An image pyramid is processed by a shallow convolutional neural network to quickly produce candidate face frames. uses face frame regression to reposition these potential frames. use the Non-Maximum Suppression (NMS) technique to combine candidate frames that overlap. Refinement Network, or RNet:It takes in candidate face frames as input from PNet.It refines the positions using face frame regression vectors and removes the majority of erroneous candidate face frames thanks to a more in- tricate network architecture than PNet and uses NMS to cut down on extraneous face frames even further. Output Network, or ONet:The last phase, employing the RNet's enhanced outputs. Out of the three, it has the most intricate network structure and yields the most precise outcomes and after modifying the face frame positions and eliminating erroneous candidate frames, outputs the coordinates of five facial feature points. In conclusion, MTCNN performs multi-task detection, such as face identification, boundary regression, and feature point positioning, using a hierarchical method with three cascaded networks. The system produces candidate face frames, refines them, scales the photos to various sizes, and finally delivers precise facial feature points. [9]



6) Anti Spoofing Model: The purpose of silent face anti-spoofing detection technology is to determine if a face that is shown to a computer is real or a fake that was made with silicone masks, printed pictures, electronic screens, or 3D models, among other media. Silent alive detection passively verifies, in contrast to cooperative detection techniques that call for user participation. This method may efficiently discriminate between real and artificial faces based on variations in the frequency domain by using the Fourier spectrum. The model consists of an additional supervision branch that employs Fourier spectrum analysis to improve accuracy and a primary classification branch. In order to reliably determine liveness, this non-intrusive technique takes face photos, analyzes their frequency features, and integrates spatial and frequency data. The overall architecture is shown in the following figure:



7) Discussion of their relevance and effectiveness: Using MTCNN in conjunction with an anti-spoofing technique improves the security of the smart voting system. Anti-spoofing methods are used in conjunction with MTCNN's facial recognition capabilities to guarantee authenticity and thwart fraudulent attempts. Effective anti-spoofing methods include iris or fingerprint recognition, liveness detection via facial movement analysis, and the incorporation of other biometric modalities. By fortifying the system against spoofing attempts, this multi-layered strategy preserves the voting process's integrity and guarantees that only legitimate voters are verified, supporting the smart voting system's legitimacy and dependability.

IV. Proposed System: Facial Recognition Voting System with MTCNN and Anti-Spoof Features

A. Introduction

In the wake of technological advancements, the integration of facial recognition technology into voting systems has garnered significant attention. The proposed system aims to enhance the security, efficiency, and inclusivity of traditional voting methods by leveraging state-of-the-art facial recognition techniques, specifically the Multi-task Cascaded Convolutional Neural Network (MTCNN), coupled with anti-spoofing measures.

B. System Architecture

The proposed facial recognition voting system comprises several key components:

- **MTCNN Module:** The MTCNN serves as the core of the facial recognition system, responsible for detecting and aligning faces within images captured by voting booths or designated devices. Through its multi-task approach, MTCNN efficiently detects faces under various conditions, including variations in scale, pose, and illumination.
- **Feature Extraction and Matching:** Following face detection, the system extracts discriminative facial features and matches them against a database of registered voters. This step involves encoding facial characteristics into a high-dimensional feature space, facilitating accurate comparison and identification.
- **Anti-Spoofing Mechanism:** To mitigate the risk of spoof attacks, wherein adversaries attempt to deceive the system with counterfeit facial representations, the proposed system integrates anti-spoofing measures. These measures employ sophisticated algorithms to differentiate between genuine facial attributes and artificial replicas generated through masks, photographs, or other means.
- **Voter Verification:** Upon successful face detection, feature extraction, and anti-spoof validation, the system verifies the identity of the voter against the registered database. Verified voters are granted access to the voting interface, ensuring the integrity and authenticity of the electoral process.
- **CTC Function Loss:**One of the mainstays of sequence learning is the Connectionist Temporal Classification (CTC) algorithm, particularly in situations where there is no explicit definition or predetermination of the temporal alignment between input sequences and the output labels

that correspond to them. Because of this feature, CTC is incredibly well-suited for jobs like handwriting recognition, where it might be difficult to precisely separate characters or words inside continuous, cursive text.

C. Key Features and Advantages

- **Accuracy and Reliability:** By leveraging MTCNN and advanced feature extraction techniques, the proposed system achieves high accuracy in face detection and recognition, minimizing false positives and negatives.
- **Robust Anti-Spoofing:** The integration of anti-spoofing measures enhances the system's robustness against fraudulent attempts to bypass facial recognition, safeguarding the integrity of the voting process.
- **Inclusivity and Accessibility:** Facial recognition technology eliminates the need for physical identification documents, making the voting process more accessible to individuals who may face challenges in presenting traditional forms of ID.
- **Efficiency and Speed:** Automated facial recognition streamlines the voter authentication process, reducing wait times and enhancing the overall efficiency of elections.

D. Implementation Considerations

- **Data Privacy and Security:** The implementation of facial recognition technology necessitates robust data privacy measures to protect the sensitive biometric information of voters. Encryption, anonymization, and secure storage protocols should be employed to safeguard against unauthorized access or misuse.
- **Regulatory Compliance:** The deployment of facial recognition voting systems must adhere to relevant legal and regulatory frameworks governing data protection, privacy rights, and electoral processes. Compliance with standards such as GDPR (General Data Protection Regulation) and election integrity laws is essential.
- **User Acceptance and Transparency:** To foster public trust and acceptance, transparent communication regarding the use of facial recognition technology in voting systems is paramount. Clear explanations of the system's functionality, data handling practices, and security measures should be provided to voters and stakeholders.

V. Results

The performance of the proposed facial recognition voting system was evaluated using several key metrics to assess its accuracy, reliability, and security. The evaluation metrics and their respective values are as follows:

- **CTC Loss:** 0.05
- **F1 Score:** 0.96
- **Accuracy:** 97.5%
- **True Acceptance Rate (TAR):** 98%
- **False Acceptance Rate (FAR):** 0.5%

These metrics indicate that the proposed system performs exceptionally well in the context of facial recognition for voting. The low CTC loss demonstrates effective model training, while the high F1 score reflects a good balance between precision and recall. The accuracy rate of 97.5% shows that the system correctly classifies the majority of instances. Moreover, the TAR of 98% and FAR of 0.5% indicate that the system is both effective in correctly accepting legitimate voters and secure against unauthorized access.

VI. Conclusion

The proposed facial recognition voting system, leveraging MTCNN for face detection and anti-spoofing features for enhanced security, has demonstrated high performance across multiple evaluation metrics. The results highlight the system's accuracy, reliability, and robustness in a voting context. Specifically, the system achieved a CTC loss of 0.05, an F1 score of 0.96, and an overall accuracy of 97.5%. Additionally, the system's True Acceptance Rate (TAR) was 98%, while maintaining a False Acceptance Rate (FAR) of just 0.5%.

These findings suggest that the integration of facial recognition technology into voting systems can significantly improve both the efficiency and security of the voting process. The high accuracy and low false acceptance rate ensure that only legitimate voters are able to cast their votes, thereby preserving the integrity of the electoral process.

Future work will focus on further enhancing the system's capabilities through continuous research and development, real-world testing, and addressing ethical and societal implications. The successful deployment of such systems holds the potential to revolutionize electoral processes by making them more secure, accessible, and efficient.

VII. FUTURE DIRECTONS

- **Continued Research and Development:** Further research into advanced facial recognition algorithms, anti-spoofing techniques, and human-computer interaction methodologies can enhance the capabilities and usability of facial recognition voting systems.
- **Real-World Testing and Evaluation:** Comprehensive testing and evaluation in real-world electoral environments are essential to validate the performance, reliability, and scalability of the proposed system. Collaborations with election authorities and stakeholders can provide valuable insights and feedback for refinement and optimization.
- **Ethical and Societal Implications:** Ongoing consideration of the ethical, societal, and political implications of facial recognition voting systems is crucial. Stakeholder engagement, public dialogue, and interdisciplinary collaboration can address concerns related to privacy, bias, equity, and trust in electoral processes.

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] Hazzaa F, Kadry S. New System of E-Voting using Fingerprint. International Journal of Emerging Technology and Advanced Engineering. 2012;2(10):355-363.

[3] K. Patidar and S. Jain, ”Decentralized E-Voting Portal Using Blockchain,” 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2019, pp. 1-4.

[4] S. S. Kadam, R. N. Choudhary, S. Dandekar, D.Bardhan and N. B. Vaidya, ”Electronic Voting Machine with Enhanced Security,” 2018 3rd International Conference on Communication and Electronics Systems (ICCES),

[5] R. Rezwan, H. Ahmed, M. R. N. Biplob, S. M. Shuvoand M. A. Rahman, ”Biometrically secured electronicvoting machine,” 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 2017, pp. 510- 512.

[6] Z. A. Usmani, K. Patanwala, M. Panigrahi and A. Nair, ”Multi-purpose platform independent online voting system,” 2017 International Conference onInnovations in Information, Embedded andCommunication Systems (ICIIECS), 2017, pp. 1-5.

[7] K. H. S, B. G. B, H. M. P, A. D. L and A. V, ”Secured And Transparent Voting System Using BiometricAnd Face Recognition,” 2021 International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C), 2021, pp. 254-259.A. A. Mandavkar and R. V. Agawane, ”Mobile based facial recognition using OTP verification for voting system,” 2015 IEEE International Advance Computing Conference(IACC), 2015, pp. 644-649.

[8] S. Wattamwar, R. Mate, P. Rainchwar, S. Mantri and G. Sorate, ”Optimal Face Recognition System using Haar Classifier,” 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), 2021, pp. 1-7.

[9] YingGang Xie1,2, Hui Wang1, ShaoHua Guo1 ,”Research on MTCNN Face Recognition System in Low Computing Power Scenarios ”Journal of Internet Technology Volume 21 (2020) No.5