ijamrsd.com
ISSN: 2583-6404
Journal of Advanced Multidisciplinary Research Studies and Development
Peer Reviewed Referred Journal
Bi-monthly
Open Access

REAL TIME FACE RECOGNITION BASED ELECTRONIC VOTING MACHINE USING RASPBERRY PI

Mr. Pandharinath Baban Bichkule[1], Ms. Waghmode K.H[2]
[1] *ME/MTech in IOT, Dattakala Group of Institution, College of Engg, Bhigwan, Pune.*
[2] *HOD (E&TC Dept), Dattakala Group of Institution, College of Engg, Bhigwan, Pune.*

Abstract
With the introduction of electronic voting systems, the efficiency, transparency, and accuracy of the voting process can be significantly improved. However, the conventional Electronic Voting Machines (EVMs) involve a manual verification of the voter's identity. This makes the system highly susceptible to voter impersonation and duplicate voting. This paper presents a real-time face recognition-based electronic voting system using a Raspberry Pi to improve the accuracy of the voter verification process. In this paper, the authors have designed a face recognition-based electronic voting system that includes a raspberry pi camera to acquire the voter's face images, a face detection system that uses the Haar Cascade Classifier algorithm, and a face recognition system that uses the Local Binary Pattern Histogram (LBPH) algorithm. After successful verification of the voter's identity, the voter will be allowed to cast their vote through a touchscreen interface. The system was able to attain a recognition accuracy of up to 92% under bright lighting conditions, as well as 90% under normal indoor lighting, with an average authentication time of approximately 1.3 seconds. Functional testing was equally successful, with the system being able to prevent duplicate voting attempts by 100%, as well as store the votes in the database. This shows that the proposed system is effective for use in institutional voting scenarios
Keywords: Electronic Voting Machines, Local Binary Pattern Histogram, Face Recognition, Raspberry Pi.

► *Corresponding Author: Mr. Pandharinath Baban Bichkule*

I. Introduction

Elections are a fundamental component of democratic governance, and the reliability of the voting process plays a critical role in ensuring transparency and public confidence. Traditional voting methods based on paper ballots require extensive manpower, time-consuming counting procedures, and are vulnerable to human errors and manipulation. To overcome these challenges, Electronic Voting Machines (EVMs) were introduced to automate the voting process and improve the efficiency and accuracy of elections [17], [18].

Although EVMs significantly improve the voting process, most existing systems rely on manual verification of voter identity using voter identification cards or electoral rolls. This approach is susceptible to several security challenges such as voter impersonation, proxy voting, and duplicate voting attempts. Ensuring reliable voter authentication is therefore essential to maintain the integrity of electronic voting systems [6], [7].

Biometric authentication techniques have emerged as effective solutions for enhancing the security of voting systems. Biometric technologies such as fingerprint recognition, iris scanning, and facial recognition use unique physiological characteristics to verify the identity of individuals. Among

these techniques, facial recognition has gained significant attention due to its contactless operation, ease of deployment, and compatibility with low-cost camera devices [1], [5].

Recent advances in computer vision and deep learning have significantly improved the accuracy and reliability of facial recognition systems. Several researchers have explored face recognition–based authentication systems for security and identification applications. Techniques such as Local Binary Pattern Histogram (LBPH), Eigenfaces, and deep learning–based models like FaceNet and DeepFace have demonstrated strong performance in facial recognition tasks [25], [26].

The development of embedded computing platforms such as Raspberry Pi has enabled the deployment of real-time image processing applications in low-cost hardware environments. Raspberry Pi supports various computer vision libraries such as OpenCV, making it suitable for implementing biometric authentication systems for embedded applications [9], [12].

Several studies have proposed electronic voting systems based on facial recognition technology. For example, Khan et al. [15] developed a Raspberry Pi–based voting system that used facial recognition for voter verification. Similarly, Sharma et al. [16] implemented a face recognition–based voting system to reduce impersonation and unauthorized voting. However, many existing systems lack robust security mechanisms such as encrypted vote storage and effective duplicate vote prevention.

To address these challenges, this paper proposes a Real-Time Face Recognition Based Electronic Voting Machine using Raspberry Pi**.** The proposed system integrates biometric authentication with a secure electronic voting interface to ensure that only authorized voters can cast their votes. The system captures live images using a Raspberry Pi camera, performs facial recognition using the LBPH algorithm, and securely records votes in a database. By combining biometric authentication with embedded computing technology, the proposed system provides a low-cost and secure solution for electronic voting systems.

II. Related Work

Electronic voting systems have been widely studied to enhance the transparency, reliability, and efficiency of election processes. Early electronic voting machines focused primarily on automating vote casting and counting; however, they lacked strong mechanisms for verifying voter identity. As a result, these systems were vulnerable to issues such as voter impersonation, duplicate voting, and unauthorized access. To address these challenges, researchers have explored biometric authentication techniques and advanced security mechanisms for electronic voting systems.

Biometric authentication has been widely adopted in secure identification systems due to its ability to uniquely identify individuals based on physiological characteristics. Among the commonly used biometric techniques are fingerprint recognition, iris scanning, and facial recognition. Facial recognition has gained significant attention because it allows contactless authentication and can be implemented using low-cost cameras and embedded computing platforms [1], [5]. In recent years, several studies have focused on improving the reliability and robustness of face recognition systems through advanced computer vision and machine learning techniques.

Traditional face recognition algorithms such as Eigenfaces and Fisherfaces were among the earliest approaches used for facial identification. Turk and Pentland introduced the Eigenfaces method using principal component analysis (PCA) to represent facial features in a reduced dimensional space [24]. Later, Ahonen et al. proposed the Local Binary Pattern Histogram (LBPH) algorithm, which extracts local texture features from facial images and has demonstrated strong performance in face recognition tasks with relatively low computational requirements [25]. Due

to its simplicity and efficiency, LBPH is widely used in embedded applications such as Raspberry Pi–based systems.

With the advancement of deep learning, more sophisticated face recognition techniques have been developed. Deep neural network models such as FaceNet and DeepFace have achieved high accuracy in large-scale face recognition applications by learning complex facial feature representations [26], [29]. Similarly, Parkhi et al. introduced deep learning–based facial recognition models that significantly improved recognition accuracy under varying lighting conditions and facial expressions [27]. Although deep learning methods provide superior performance, they often require high computational power and specialized hardware such as GPUs, which makes them less suitable for low-power embedded devices.

Researchers have also explored facial recognition systems for embedded and edge computing platforms. Kumar and Ramya [9] demonstrated a real-time face recognition system implemented on Raspberry Pi using OpenCV and machine learning algorithms. Their work highlighted the feasibility of performing real-time facial recognition on low-cost hardware platforms. Similarly, Pascual et al. [12] proposed a lightweight facial recognition framework designed specifically for edge devices, showing that optimized models can achieve efficient performance on embedded systems.

Several studies have investigated the application of biometric authentication in electronic voting systems. Khan et al. [15] proposed a smart electronic voting machine using Raspberry Pi and facial recognition technology to authenticate voters before allowing them to cast their votes. Their system demonstrated the effectiveness of biometric authentication in preventing unauthorized voting. Sharma et al. [16] also developed a face recognition–based electronic voting system that integrates camera-based authentication with a digital voting interface. While these systems improve voter authentication, they often lack advanced security features such as encrypted vote storage and tamper-resistant audit mechanisms.

In addition to biometric authentication, researchers have proposed the use of blockchain technology to improve election transparency and security. Faruk et al. [6] developed a blockchain-based electronic voting system integrated with biometric identification to ensure vote immutability and transparency. Similarly, Hajian Berenjestanaki et al. [7] reviewed blockchain-based voting architectures and highlighted their ability to provide decentralized vote storage and improved election security. However, blockchain-based voting systems typically require complex infrastructure and high computational resources, making them difficult to implement on embedded platforms such as Raspberry Pi.

Another important challenge in facial recognition systems is the possibility of spoofing attacks, where attackers attempt to bypass biometric authentication using printed photos, videos, or masks. To address this issue, researchers have proposed face presentation attack detection techniques. Yu et al. [1] conducted a comprehensive survey of deep learning–based face anti-spoofing techniques and demonstrated their effectiveness in detecting presentation attacks. Similarly, Wang et al. [2], [3] developed deep learning–based anti-spoofing models that analyze temporal facial patterns to detect fraudulent authentication attempts. Deng et al. [4] further proposed a dual-stream neural network architecture for multimodal face anti-spoofing, achieving high detection accuracy under different spoofing scenarios.

Despite significant progress in biometric authentication and secure voting technologies, several challenges remain in implementing efficient biometric voting systems on embedded devices. Many existing systems either require expensive hardware components or rely on computationally intensive algorithms that are difficult to deploy on resource-constrained platforms. Therefore, there

is a need for a lightweight, cost-effective, and secure biometric voting solution that can operate efficiently on embedded hardware.

The proposed system addresses this research gap by developing a real-time face recognition–based electronic voting machine using Raspberry Pi and the LBPH algorithm**.** By combining efficient facial recognition techniques with embedded computing and secure vote storage, the system aims to provide a practical and secure solution for electronic voting in small-scale and institutional election environments.

III. Proposed Methodology

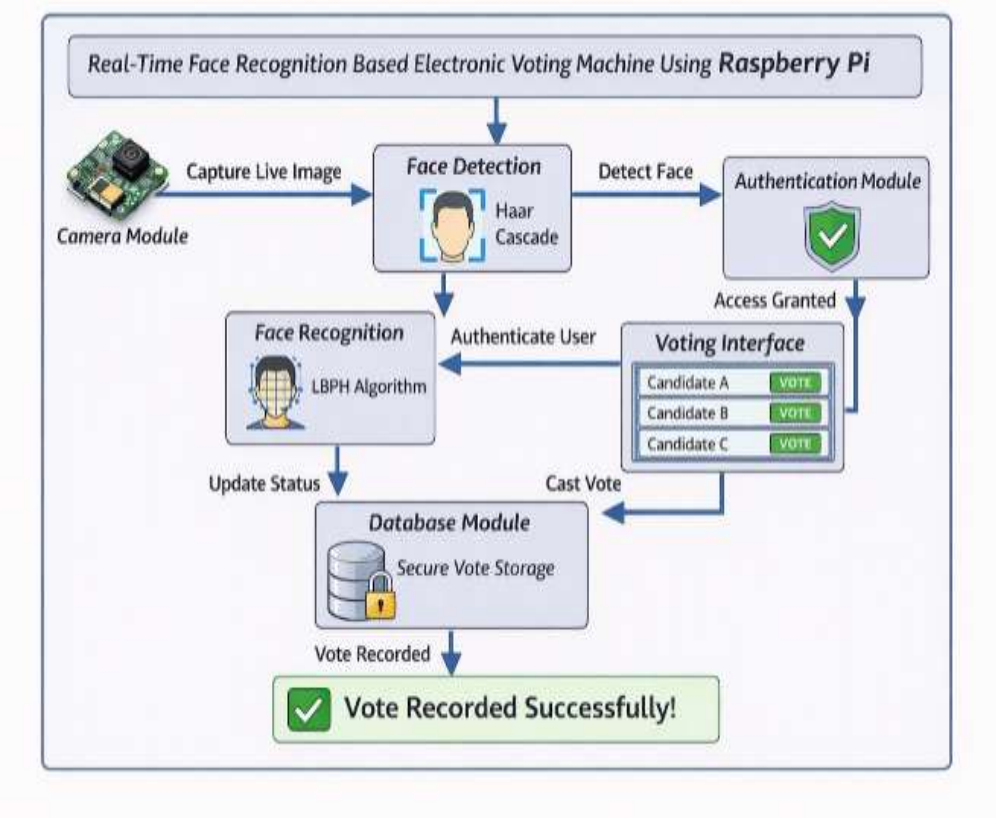

Fig.1 Proposed Architecture

Figure 1 illustrates the proposed methodology of the real-time face recognition–based electronic voting system implemented using Raspberry Pi. The proposed system integrates facial recognition technology with an electronic voting interface to ensure secure voter authentication and prevent unauthorized voting.

The process begins with the Camera Module, which captures the live image of the voter using the Raspberry Pi camera. The captured image is then forwarded to the Face Detection Module, where the Haar Cascade classifier is used to detect the presence of a human face in the image frame. This step ensures that only the facial region of the captured image is processed for further recognition.

Once the face is detected, the system performs Face Recognition using the Local Binary Pattern Histogram (LBPH) algorithm. The LBPH algorithm extracts unique facial features from the detected face and compares them with the facial templates stored in the system database. This process verifies whether the voter is registered in the database.

If the facial features match with a registered voter record, the system proceeds to the Authentication Module, which confirms the identity of the voter. After successful authentication, access to the Voting Interface is granted. The voting interface displays the list of candidates on the touchscreen display, allowing the voter to select their preferred candidate.

After the voter casts their vote, the selected vote is transmitted to the Database Module, where it is securely stored. The database records the vote while simultaneously updating the voter's status to prevent duplicate voting attempts. This ensures that each registered voter can cast only one vote during the election process.

Finally, once the vote is successfully stored in the database, the system displays a confirmation message indicating that the vote has been recorded successfully, marking the completion of the voting process.

Overall, the proposed methodology integrates face detection, facial recognition, secure authentication, and electronic vote recording to provide a reliable and secure voting mechanism using a low-cost Raspberry Pi platform.

IV. System Work Flow

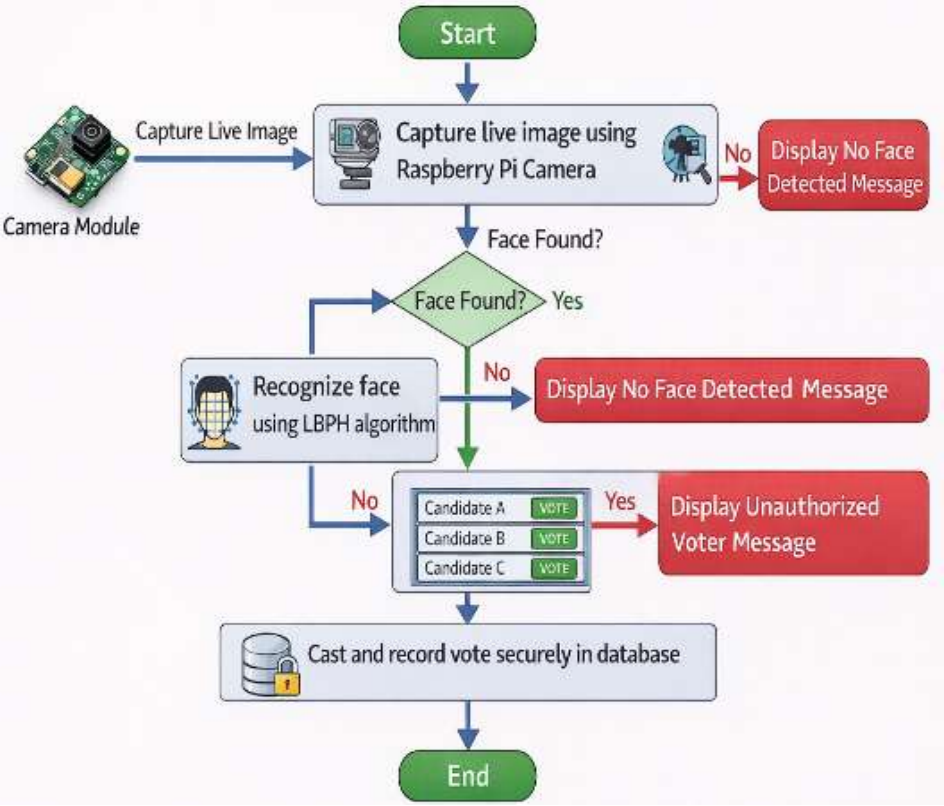

Fig.2 Proposed System flow chart

Figure 2 illustrates the system flowchart of the proposed real-time face recognition–based electronic voting system implemented using Raspberry Pi. The flowchart explains the step-by-step operational procedure of the system from voter authentication to secure vote recording.

The process begins with the Start stage, where the voting system is activated. Once the system is initialized, the Raspberry Pi camera module captures a live image of the voter. The captured image is then processed to detect the presence of a human face using a face detection algorithm.

After capturing the image, the system checks whether a face is detected in the frame. If no face is detected, the system displays a "No Face Detected" message and prompts the user to position themselves correctly in front of the camera.

If a face is successfully detected, the system proceeds to the face recognition stage, where the facial features of the detected face are analyzed using the Local Binary Pattern Histogram (LBPH) algorithm. The algorithm extracts unique facial features and compares them with the facial data stored in the voter database.

If the detected face does not match any registered voter, the system displays an "Unauthorized Voter" message, preventing unauthorized access to the voting interface. This step ensures that only registered voters are allowed to participate in the election process.

If the face recognition process successfully matches the voter's identity with the registered database, the system grants access to the voting interface. The voting interface displays the list of candidates on the touchscreen, allowing the voter to select their preferred candidate.

Once the voter selects a candidate, the system securely records the vote in the database. The system also updates the voter's status to indicate that the vote has been cast, which prevents the voter from voting again.

Finally, after the vote is securely stored, the system reaches the End stage, indicating that the voting process has been successfully completed.

Overall, the system flowchart demonstrates how the proposed system integrates face detection, facial recognition, voter authentication, and secure vote recording to ensure a reliable and fraud-resistant electronic voting process.

V. Hardware Implementation

Figure 3 illustrates the hardware implementation of the proposed real-time face recognition–based electronic voting system using Raspberry Pi. The hardware architecture integrates several components such as the Raspberry Pi board, camera module, touchscreen display, voting buttons, and power supply to perform secure voter authentication and electronic vote recording.

At the core of the system is the Raspberry Pi 4, which acts as the main processing unit responsible for executing the face recognition algorithm, controlling the voting interface, and managing communication between hardware components. The Raspberry Pi runs the operating system and Python-based application programs that handle image processing, voter authentication, and vote recording.

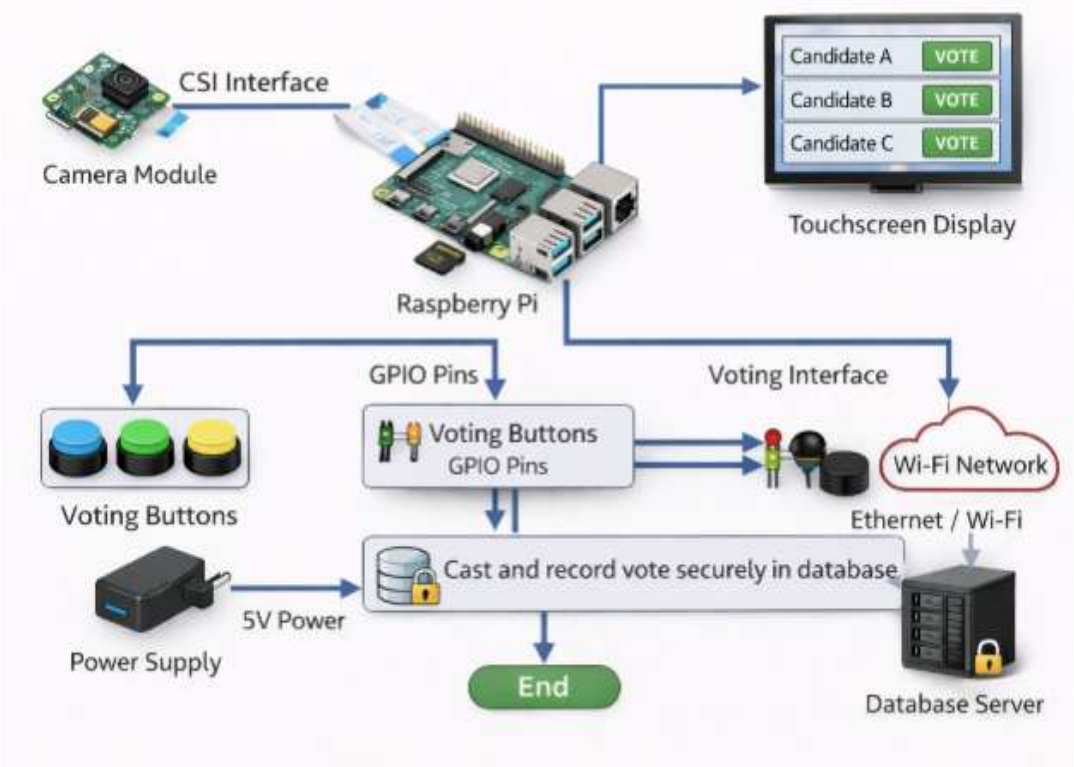

Fig.3 Proposed system hardware implementation

The Raspberry Pi Camera Module is connected to the Raspberry Pi through the CSI (Camera Serial Interface) port. This camera captures real-time images of voters standing in front of the voting machine. The captured images are processed using computer vision algorithms to detect and recognize the voter's face before granting access to the voting interface.A touchscreen display is connected to the Raspberry Pi to provide the voting interface for user interaction. Once the voter is successfully authenticated, the touchscreen displays the list of candidates and allows the voter to select their preferred candidate.

In addition to the touchscreen interface, voting buttons connected to the GPIO pins of the Raspberry Pi can be used to register votes in some system configurations. These buttons provide an alternative input method for selecting candidates and are interfaced with the Raspberry Pi through its general-purpose input/output (GPIO) pins. The system is powered using a 5V regulated power supply, which provides the required operating voltage for the Raspberry Pi and connected peripherals. Reliable power supply ensures stable operation of the voting machine during the election process.

The recorded vote data is stored securely in a database server connected through Ethernet or Wi-Fi communication. The database maintains voter records, authentication status, and voting results while ensuring that each voter can cast only one vote.Overall, the hardware implementation integrates camera-based biometric authentication, embedded processing, user interface components, and secure data storage to create a reliable electronic voting system. The use of Raspberry Pi allows the system to be implemented as a low-cost and portable voting solution suitable for institutional and small-scale elections.

VI. Experimental Results

To evaluate the performance of the proposed real-time face recognition–based electronic voting system, several experiments were conducted using a Raspberry Pi 4 platform integrated with a camera module and touchscreen interface. The system was tested under different lighting conditions and with multiple registered users to analyze the accuracy and reliability of facial recognition and vote recording processes.

The experimental setup consisted of a Raspberry Pi 4 with a camera module for capturing live images and a database containing facial images of registered voters. The Local Binary Pattern Histogram (LBPH) algorithm was used for face recognition. During testing, the system verified voter identity, granted access to the voting interface, and securely stored the selected vote in the database.

The performance of the system was evaluated using parameters such as recognition accuracy, authentication time, and system reliability.

Table 1: Face Recognition Performance under Different Lighting Conditions

Lighting Condition	Total Tests	Correct Recognition	Accuracy (%)
Bright Lighting	50	46	92%
Normal Indoor Lighting	50	45	90%
Low Lighting	50	39	78%

Table 1 shows the face recognition accuracy of the proposed system under different lighting conditions. The results indicate that the system performs best under bright lighting conditions with an accuracy of 92%, while recognition accuracy decreases slightly in low-light environments due to reduced image clarity.

Table 2: System Authentication Performance

Parameter	Measured Value
Average Face Detection Time	0.5 seconds
Average Recognition Time	0.8 seconds
Total Authentication Time	1.3 seconds
Duplicate Voting Prevention	100% successful

Table 2 presents the authentication performance of the proposed voting system. The average face detection time was approximately 0.5 seconds, while the recognition process required about 0.8 seconds. Therefore, the total time required for voter authentication was approximately 1.3 seconds, enabling real-time system operation.

Table 3: Voting System Functional Test Results

Test Scenario	Expected Outcome	Result
Registered voter authentication	Access granted	Successful
Unregistered voter detection	Access denied	Successful
Multiple voting attempt	Vote rejected	Successful
Vote storage in database	Vote recorded	Successful

Table 3 shows the functional testing results of the proposed system. The system successfully authenticated registered voters and rejected unauthorized users. Additionally, the system prevented duplicate voting attempts by updating the voter status after the vote was cast.

Experimental Analysis

The experimental results demonstrate that the proposed system provides reliable facial recognition–based authentication with acceptable accuracy and response time. The Raspberry Pi platform was capable of performing real-time image processing and voter authentication without significant delays. The system also successfully prevented duplicate voting and securely stored voting data in the database. Overall, the proposed solution offers a low-cost, efficient, and secure electronic voting system that can be used for institutional elections, student elections, and small-scale voting environments.

VII. Conclusion

In this paper, a real-time face recognition-based electronic voting system using Raspberry Pi has been proposed, aiming to provide security for the voting process. In the proposed voting system, the Raspberry Pi camera, LBPH-based face recognition, and touchscreen voting interface are integrated. Using the experimental results, the voting system has been found to provide a recognition accuracy of approximately 92% for bright lighting conditions, whereas the accuracy is found to be approximately 90% for normal indoor lighting conditions. Moreover, the average authentication time is found to be approximately 1.3 seconds. Furthermore, the voting system has been found to prevent duplicate voting. Thus, the proposed voting system is efficient, reliable, and low-cost, suitable for voting purposes.

References

1. Z. Yu, X. Li, and G. Zhao, “Deep Learning for Face Anti-Spoofing: A Survey,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 45, no. 2, pp. 1234–1256, 2023.
2. Z. Wang, X. Chen, and S. Li, “Learning Multi-Granularity Temporal Characteristics for Face Anti-Spoofing,” *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1254–1269, 2022.
3. Z. Wang, P. Wang, and J. Zhang, “Consistency Regularization for Deep Face Anti-Spoofing,” *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1127–1140, 2023.
4. P. Deng, J. Li, and X. Yang, “Attention-Aware Dual-Stream Network for Multimodal Face Anti-Spoofing,” *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2050–2063, 2023.
5. D. Sharma and A. Selwal, “A Survey on Face Presentation Attack Detection Mechanisms,” *Multimedia Systems*, Springer, vol. 29, pp. 1453–1475, 2023.
6. M. J. H. Faruk, S. Rahman, and M. Hasan, “Transforming Online Voting Using Blockchain and Biometric Identification,” *Cluster Computing*, Springer, 2024.
7. M. Hajian Berenjestanaki et al., “Blockchain-Based E-Voting Systems: A Technology Review,” *Electronics*, vol. 13, no. 1, 2023.
8. M. Pooshideh, A. Hadid, and N. Damer, “Presentation Attack Detection: A Systematic Literature Review,” *ACM Computing Surveys*, vol. 56, no. 3, 2024.
9. M. Kumar and R. Ramya, “Real-Time Face Detection and Recognition on Raspberry Pi,” *Proceedings of the ACM International Conference on Embedded Systems*, 2022.
10. Q. Zhou, Y. Liu, and H. Wang, “Instance-Aware Domain Generalization for Face Anti-Spoofing,” *Proceedings of IEEE CVPR*, pp. 2045–2054, 2023.

11. Q. Zhou, Y. Liu, and H. Wang, "Test-Time Domain Generalization for Face Anti-Spoofing," *Proceedings of IEEE CVPR*, 2024.
12. A. Pascual et al., "Light-FER: Lightweight Facial Recognition for Edge Devices," *Sensors*, vol. 22, no. 23, pp. 9524–9538, 2022.
13. H. Mittal and N. Sengar, "A Blockchain and Face Recognition Based E-Voting System," *International Journal for Research in Applied Science and Engineering Technology*, 2025.
14. S. Paudel, A. Poudel, and S. Paudel, "Enhancing Electoral Integrity Using Blockchain and Facial Recognition," *Information Dynamics and Applications*, vol. 4, no. 2, pp. 85–94, 2025.
15. M. Khan, S. Ahmed, and A. Malik, "Smart Electronic Voting Machine with Face Recognition Using Raspberry Pi," *International Journal of Research Publication and Reviews*, vol. 3, no. 2, pp. 1342–1348, 2023.
16. S. Sharma, R. Patel, and V. Mehta, "Electronic Voting Machine Using Raspberry Pi with Face Recognition," *IJNRD Journal*, vol. 8, no. 6, 2024.
17. A. Thomas and P. Mathew, "Secure Online Voting System Using Face Recognition," *International Journal of Computer Applications*, vol. 182, no. 43, pp. 24–29, 2023.
18. S. Singh and R. Kumar, "Face Recognition Based Online Voting System," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 6, pp. 2208–2212, 2020.
19. S. Patel, P. Kumar, and S. Garg, "Face Recognition Based Smart Attendance System Using IoT," *International Journal of Computer Sciences and Engineering*, vol. 6, no. 5, pp. 871–876, 2018.
20. S. Chakraborty, S. Singh, and K. Kumar, "Facial Biometric System Using Raspberry Pi and LGHP Algorithm," *arXiv preprint arXiv:2101.03413*, 2021.
21. S. Najam Syed, A. Zeb Shaikh, and S. Naqvi, "A Hybrid Biometric Electronic Voting System Using Fingerprint and Face Recognition," *arXiv preprint arXiv:1801.02430*, 2018.
22. N. Tkauc et al., "Cloud-Based Face and Speech Recognition for Access Control Applications," *arXiv preprint arXiv:2004.11168*, 2020.
23. P. Viola and M. Jones, "Rapid Object Detection Using a Boosted Cascade of Simple Features," *IEEE Conference on Computer Vision and Pattern Recognition*, 2001.
24. M. Turk and A. Pentland, "Eigenfaces for Recognition," *Journal of Cognitive Neuroscience*, vol. 3, no. 1, pp. 71–86, 1991.
25. T. Ahonen, A. Hadid, and M. Pietikainen, "Face Description with Local Binary Patterns," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 2037–2041, 2006.
26. F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," *IEEE CVPR*, 2015.
27. O. M. Parkhi, A. Vedaldi, and A. Zisserman, "Deep Face Recognition," *British Machine Vision Conference*, 2015.
28. A. Krizhevsky, I. Sutskever, and G. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," *Advances in Neural Information Processing Systems*, 2012.
29. D. Taigman et al., "DeepFace: Closing the Gap to Human-Level Performance in Face Verification," *IEEE CVPR*, 2014.
30. I. Goodfellow et al., "Deep Learning for Face Recognition and Biometric Security," *MIT Press*, 2016.