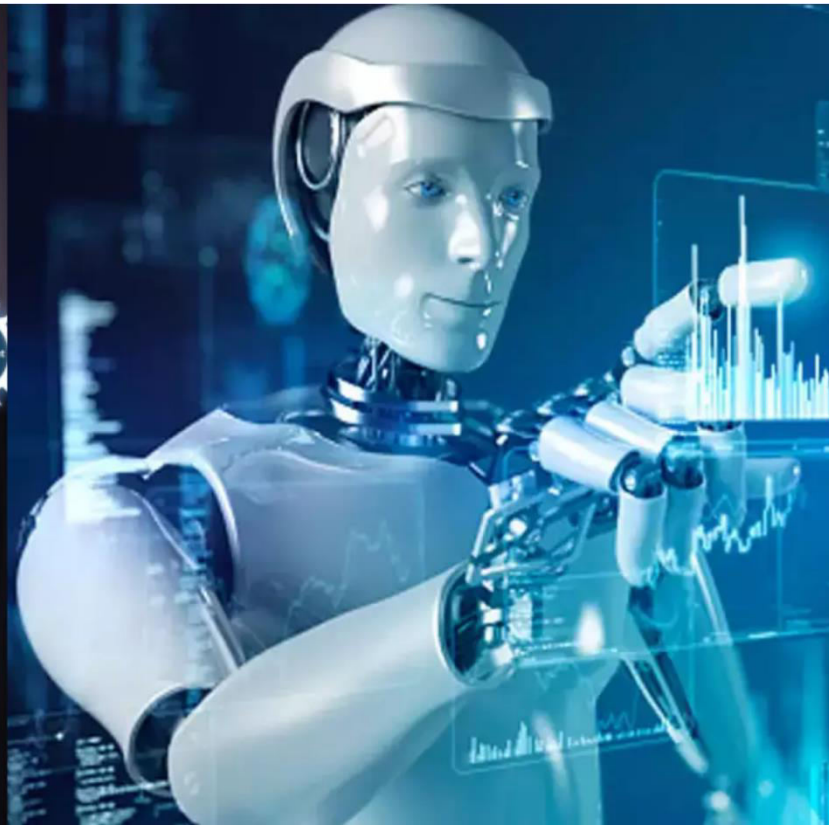
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503125|

Cast My Vote: Pilot Scale Online Voting System through Biometrics (Facial Recognition)

Mr. Shaik Nagur Vali, B. Pranavaditya, A. Shiva Sai Tarun Kumar, M. Praveen Kumar, D. Sravan Kumar

Assistant Professor, Department of CSE (Data Science), Ace Engineering College, Ghatkesar, Telangana, India

U.G. Student, Department of CSE (Data Science), Ace Engineering College, Ghatkesar, Telangana, India

U.G. Student, Department of CSE (Data Science), Ace Engineering College, Ghatkesar, Telangana, India

U.G. Student, Department of CSE (Data Science), Ace Engineering College, Ghatkesar, Telangana, India

U.G. Student, Department of CSE (Data Science), Ace Engineering College, Ghatkesar, Telangana, India

ABSTRACT: The rapid growth of digital technologies has enabled the transformation of traditional voting systems into secure, convenient, and reliable online platforms. This project presents Online Voting Using Face Recognition and Robust Voter ID Verification, a system designed to enhance election integrity by integrating biometric authentication with secure voter identification mechanisms. The proposed system leverages face recognition algorithms like CNN (Convolutional Neutral Networks), LBPH (Local Binary Pattern Histogram) to verify voter identity, thereby reducing the risk of impersonation, duplicate voting, and fraudulent access. In addition, it incorporates a robust voter ID verification module, which verifies unique, tamper-resistant identifiers using cryptographic hashing and randomization techniques, ensuring authenticity and traceability. The core concept that alludes the project is Deep Learning. It canopies the modules of python like pandas, scikit learn, Stream-lit, open-cv and media pipe.

KEYWORDS: CNN, LPBH, python libraries, Deep learning.

I. INTRODUCTION

An online voting system that integrates facial recognition, multifactor verification, and blockchain technology represents a modern, secure, and efficient approach to digital elections. As traditional voting methods often face challenges such as long queues, human errors, impersonation, and ballot tampering, this advanced system offers a reliable alternative that enhances both accessibility and trust. Facial recognition serves as a primary biometric layer to accurately authenticate voters by analyzing unique facial features, ensuring that only legitimate individuals gain access to the voting platform. To strengthen security further, multifactor verification—such as OTPs, device authentication, or PIN codes—adds an additional defense against unauthorized access and identity fraud.

Once a voter is authenticated, their vote is recorded and stored on a blockchain network, which provides immutability, transparency, and protection from tampering due to its decentralized structure. Each transaction, or vote, is encrypted and distributed across multiple nodes, making it virtually impossible to alter or delete. This combination of biometrics, layered verification, and distributed ledger technology helps build a robust voting environment that enhances voter confidence, improves electoral integrity, and supports fair, transparent, and tamper-proof democratic processes in a digital age. As traditional voting methods often face challenges such as long queues, human errors, impersonation, and ballot tampering, this advanced system offers a reliable alternative that enhances both accessibility and trust.

II. LITERATURE SURVEY

Recent research explores combining biometrics, multifactor authentication (MFA), and distributed ledgers to improve the security and transparency of electronic voting. Reviews show promise in these combinations but also

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503125|

highlight practical, privacy, and security challenges that remain unresolved. [1] A. Ayed, "A conceptual secure blockchain-based electronic voting system," Int. J. Netw. Secur. Appl., vol. 9, no. 3, pp. 1–9, 2017. [2] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in Fin. Cryptogr. Data Secur., Springer, 2017, pp. 357–375. [3] P. Noizat, "Blockchain electronic vote," in Handbook of Digital Currency, Academic Press, 2015, pp. 453–461. [4] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit., 2015, pp. 815–823. [5] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition," in Proc. IEEE/CVF Comput. Vis. Pattern Recognit., 2019, pp. 4690–4699. [6] F. Aloul, S. Zahidi, and W. El-Hajj, "Two-factor authentication using mobile phones," in Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl., 2009, pp. 641–644. [7] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes," in Proc. IEEE Symp. Secur. Privacy, 2012, pp. 553–567. [8] M. Specter, J. Koppel, and J. A. Halderman, "The ballot is busted before the blockchain: Security analysis of Voatz," in USENIX Secur. Symp., 2020. [9] S. Park, "Going from internet voting to blockchain voting: The security pitfalls," J. Cybersecurity, vol. 7, no. 1, pp. 1–12, 2021. The literature flags serious privacy questions: biometric templates are sensitive and non-revocable, so template protection, secure storage, and legal compliance (data protection laws) are vital. Research also documents demographic biases in face recognition accuracy and recommends fairness evaluation across population groups before deployment.

III. METHODOLOGY

The methodology describes the complete workflow followed to design, develop, and test the proposed secure online voting system. It includes a step-by-step approach beginning from data collection and system design to implementation, integration, testing, and deployment. The development of the proposed online voting system follows a structured methodology consisting of several phases to ensure security, efficiency, and reliability. The process begins with requirement analysis, where both functional and non-functional requirements of the system are identified and defined. In this stage, existing voting systems, security protocols, biometric technologies, and blockchain platforms are studied to understand current limitations and possible improvements. User roles such as Voter, Administrator, Auditor, and System Nodes are defined, and system constraints related to privacy laws, security standards, and performance expectations are established. After identifying the requirements, the system design phase is carried out, where a high-level architecture integrating facial recognition, multifactor authentication (MFA), and blockchain technology is developed. Various UML diagrams including Use Case, Sequence, Activity, Class, Component, and Deployment diagrams are created to represent the system structure and interactions. The data flow of the system is modeled to illustrate the sequence of operations from voter registration to biometric storage, authentication, vote casting, and secure storage of votes on the blockchain. A suitable blockchain platform such as Hyperledger Fabric or Private Ethereum is selected, and a database schema is planned to manage user profiles, election data, and system logs. The next phase involves data collection and preprocessing, where facial images are collected from public datasets or controlled environments for training and testing the recognition model. The images are preprocessed through face detection, cropping, normalization, and lighting adjustments to improve accuracy, and facial features are extracted using deep learning models such as FaceNet or ArcFace. For privacy protection, the system stores encrypted biometric templates instead of raw facial images. Following this, the facial recognition module is developed using CNN-based feature extraction techniques, and face matching is performed using similarity measures such as Euclidean distance or cosine similarity. Liveness detection is integrated to prevent spoofing attempts using photos or videos, ensuring that only real users are authenticated. To enhance security further, a multifactor authentication mechanism is implemented using methods such as OTP via SMS or email, PIN or password verification, and device-based authentication. The authentication process follows a sequence where facial recognition is performed first, followed by MFA verification, and security mechanisms like throttling are applied to prevent brute-force attacks. In the next phase, blockchain integration is implemented by deploying a permissioned blockchain network with multiple nodes. Each vote is recorded as an encrypted transaction along with a timestamp, and smart contracts are used to validate voter authenticity, prevent duplicate voting, and manage election sessions while ensuring immutability and decentralized verification. A secure voting interface is then developed to allow voters to log in, verify their identity, and cast their votes easily through a user-friendly platform that provides real-time feedback for authentication success or failure and allows voters to verify their vote using a blockchain transaction ID. Finally, an admin panel and monitoring system are created to manage voter registrations, configure elections, enforce MFA policies, and monitor system logs, statistics, and blockchain node status.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

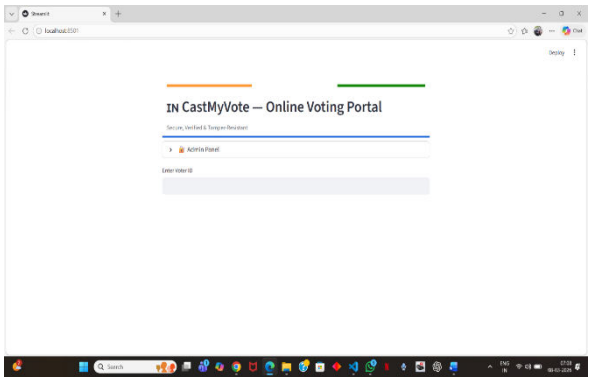
Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503125|

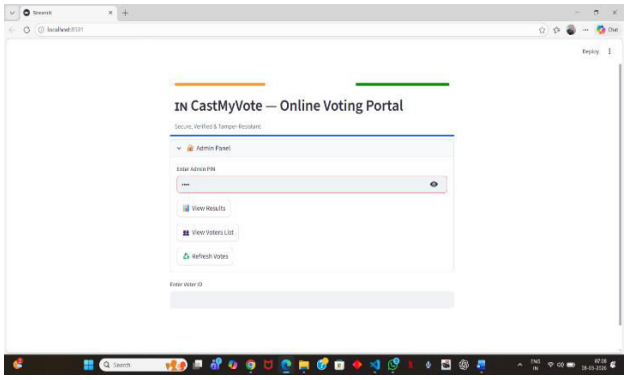
Role-based access control is implemented to ensure that only authorized administrators can perform sensitive operations, thereby maintaining the integrity and transparency of the entire voting system.

IV. EXPERIMENTAL RESULTS

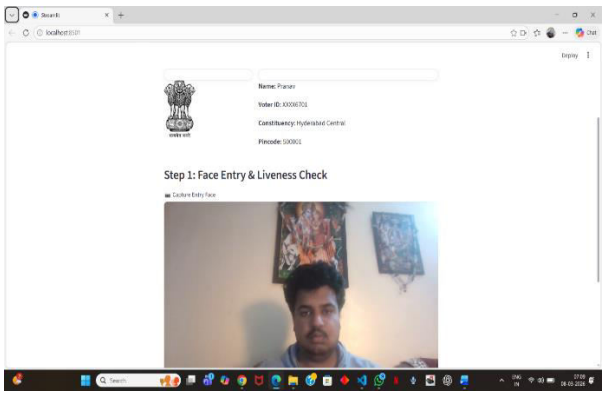
The below images showcase the output screens that have been obtained from the code implementation and thus rendering the desired results.



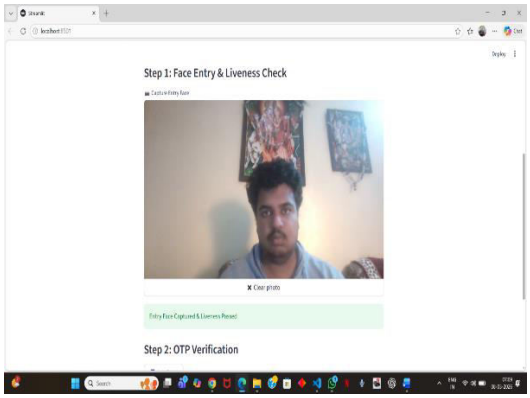
(a)



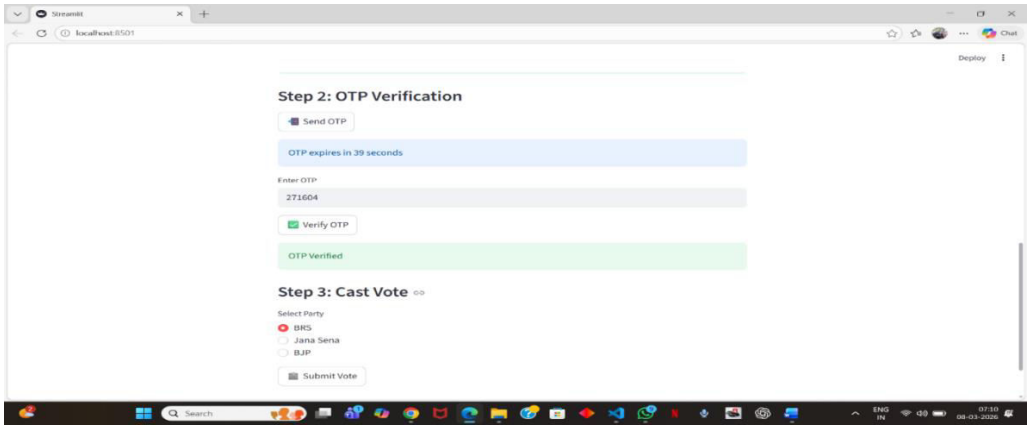
(b)



(c)



(d)



(e)

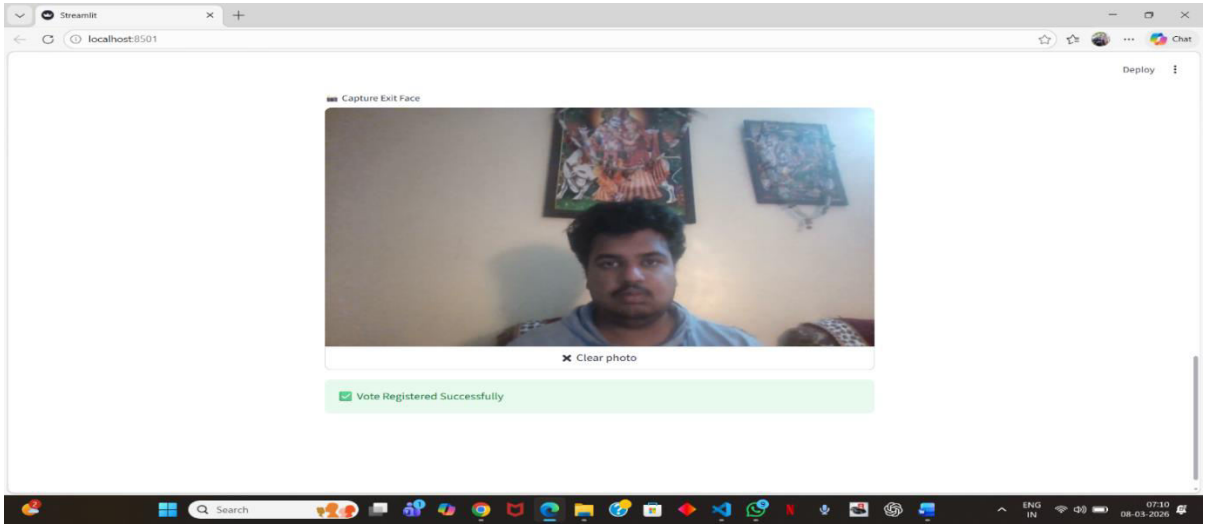
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

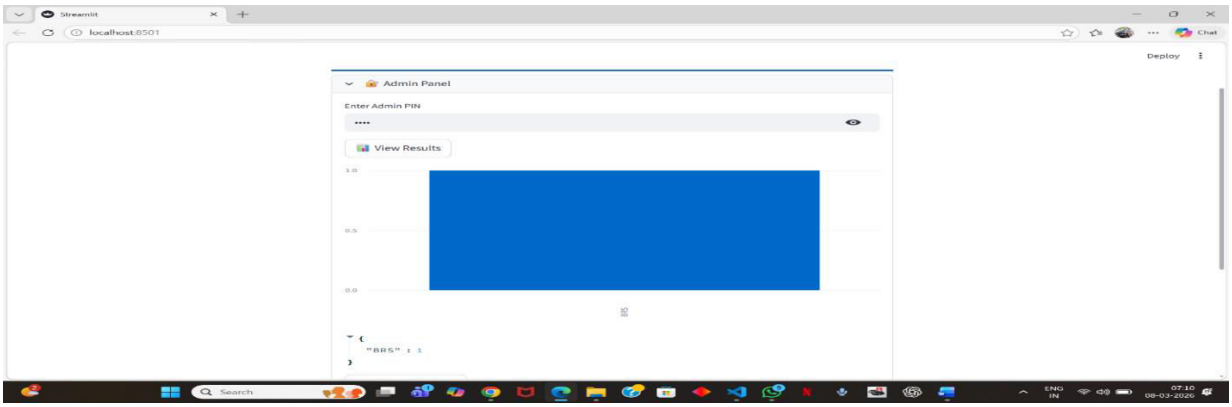
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

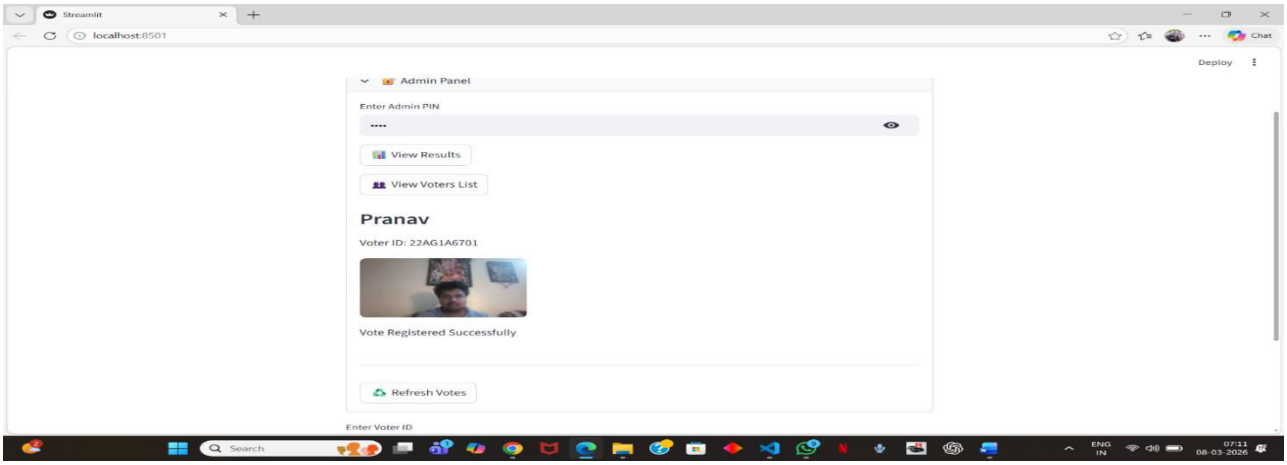
|DOI: 10.15680/IJIRSET.2026.1503125|



(f)



(g)



(h)

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503125|

The first screen (a) shows the **home interface of the CastMyVote Online Voting Portal**, which is developed using the Streamlit framework and runs locally on the browser through localhost:8501. The page displays the title **"IN CastMyVote — Online Voting Portal"** along with a subtitle indicating that the system is **secure, verified, and tamper-resistant**. At the top of the page, design elements resembling the colors of the Indian flag are shown to represent the national context of the voting system. The interface contains an expandable **Admin Panel** section and an input field where the voter can enter their **Voter ID** to begin the authentication process.

In the next screen, the **Admin Panel is expanded**, allowing administrative access to the system. The administrator must enter a secure **Admin PIN** to unlock management features. Once authenticated, the admin is provided with several options such as **View Results**, **View Voters List**, and **Refresh Votes**. These features allow the administrator to monitor the election process, check voting statistics, and reset the voting records when required.

The following screen displays the **voter verification page after entering a valid Voter ID**. The system shows the voter's personal details such as **Name, Voter ID, Constituency, and Pincode** to confirm the identity of the user. Additionally, the page displays the **national emblem of India**, emphasizing the official and secure nature of the voting process. This screen prepares the voter to proceed with biometric verification.

The next stage shows **Step 1: Face Entry and Liveness Check**, where the voter must capture their facial image using the system's camera. The interface displays a live camera preview where the user's face is detected and captured. This step ensures that the voter is physically present during the voting process and prevents the use of static images or spoofing attempts.

After successfully capturing the face image, the system displays a confirmation message stating **"Entry Face Captured & Liveness Passed."** This indicates that the biometric verification has been completed successfully. The interface then automatically moves to the next stage of authentication.

The following screen shows **Step 2: OTP Verification**, which acts as the second layer of security. The voter can click the **Send OTP** button to receive a One-Time Password on their registered mobile number. A countdown timer appears on the screen indicating the remaining time before the OTP expires. The voter must enter the received OTP in the input field to verify their identity.

Once the OTP is entered correctly, the system displays the message **"OTP Verified."** This confirms that the voter has successfully passed the multi-factor authentication process. After completing this step, the voter is allowed to proceed to the voting section of the application.

The next screen presents **Step 3: Cast Vote**, where the voter can select their preferred political party from the available options. In this example, the options displayed include **BRS, Jana Sena, and BJP**. The voter selects one option using the radio button interface and then clicks the **Submit Vote** button to record their vote in the system.

After submitting the vote, the system performs an **exit face verification** to confirm that the same voter who started the process is completing it. The interface again captures the voter's facial image and compares it with the previously captured entry image. Once the verification is successful, the system displays the message **"Vote Registered Successfully."**

The final screens demonstrate the **administrative monitoring features**. When the admin accesses the **View Results** option, the system generates a graphical representation of the election results using a bar chart. The chart shows the number of votes received by each party. Additionally, the system displays the vote data in JSON format to provide a transparent and verifiable record of the election outcome.

Another administrative screen shows the **View Voters List** feature, where the admin can see details of voters who have successfully cast their votes. The interface displays the voter's name, voter ID, captured image, and confirmation message indicating that the vote has been recorded successfully. This helps administrators monitor voter participation and maintain election transparency.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503125|

V. CONCLUSION

The Online Voting System using Facial Recognition provides a secure, efficient, and modern approach to conducting elections digitally. By integrating facial recognition technology with an online voting platform, the system ensures that only authorized voters can cast their votes, thereby reducing the chances of impersonation, duplicate voting, and electoral fraud.

This system enhances transparency, accuracy, and convenience in the voting process. Voters can authenticate their identity through facial verification, making the process faster and more reliable compared to traditional voting methods. Additionally, it reduces the need for physical polling stations, manpower, and paperwork, making elections more cost-effective and accessible.

However, challenges such as data privacy, security of biometric information, and system reliability must be carefully addressed to ensure safe implementation. With proper encryption, secure databases, and ethical handling of biometric data, facial recognition-based voting systems can become a powerful solution for future digital elections.

In conclusion, the proposed system demonstrates how artificial intelligence and biometric authentication can transform the traditional voting process into a more secure, transparent, and user-friendly digital system.

REFERENCES

1. Hombal, U., et al., **"Online Voting System with Face Recognition and One-Time Password."**
   SSRN, Electronic Journal, 2023.
   This study proposes a secure online voting system using **facial recognition and OTP authentication** to prevent fraudulent voting and ensure voter identity verification.
2. Apurbo, T. H., et al., **"A Biometric Voting Solution: Integrating Face Recognition with Embedded Systems for Secure Offline Elections."**
   Journal of Engineering Research and Reports, 2025.
   The paper presents a biometric voting prototype that uses **face recognition to authenticate voters and improve election transparency**.
3. Halidou, A., **"Voter Authentication Using Enhanced ResNet50 for Facial Recognition."**
   Information Journal, 2025.
   This research uses **deep learning models such as ResNet50 and MTCNN** to improve facial recognition accuracy for voter verification.
4. **"Smart Voting System Using Facial Detection."**
   International Journal of Innovative Technology and Exploring Engineering (IJITEE).
   The paper discusses how facial detection can reduce election fraud and improve efficiency in digital voting systems.
5. **"E-Voting System Using Blockchain and Face Recognition."**
   International Research Journal of Engineering and Technology (IRJET).
   This research integrates **blockchain with facial recognition** to ensure vote security and transparency.
6. Syed, S. N., Shaikh, A. Z., & Naqvi, S., **"A Novel Hybrid Biometric Electronic Voting System: Integrating Fingerprint and Face Recognition."**
   arXiv Research Paper.
   The study combines **facial recognition and fingerprint biometrics** to improve voter authentication accuracy.
7. **"Face Recognition Based Voting System."**
   International Journal of Research Publication and Reviews (IJRPR).
   The system verifies voter identity using biometric facial features to prevent duplicate voting.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details