*International Research Journal of Innovations in Engineering and Technology (IRJIET)*

**ISSN (online): 2581-3048**

**Volume 10, Issue 4, pp 303-307, April-2026**

https://doi.org/10.47001/IRJIET/2026.104043

# Digital Voting System with Anti-Duplicate Voting Mechanism

**[1]Bhumesh K Parihar, [2]Janaki Kandasamy, [3]Jit Mozumder Anik, [4]Sandipan Bairagi, [5]Wasim Ahamed Samani**

[1,3,4,5]Student, Department of CSE-AI, Jain Deemed To Be University, Banglore 562112, India

[2]Associate Professor, Department of CSE-AI, Jain Deemed To Be University, Banglore 562112, India

E-mail: [1]22btrca006@jainuniversity.ac.in, [2]k.janaki@jainuniversity.ac.in, [3]22btrca062@jainuniversity.ac.in, [4]22btrca066@jainuniversity.ac.in, [5]22btrca068@jainuniversity.ac.in

***Abstract* - Voting is a basic human right for the people. By voting people can choose their preferred candidate or leader for any kind of social leadership. But nowadays voting is quite hectic and costly. The Election committee has to work long hard for the preparation. It took long time and many human labours and it is quite costly. In our study we tried to make the full voting system into online basis. The system will be able to make voting system online. With online voting system security of the system and people data came in first. So in this study it introduces a method for digital voting that prevents duplicate submissions. By combining facial recognition with one-time password checks, identity confirmation becomes more reliable. What sets it apart is how verification links to existing records for consistency. Ensuring each individual casts only one ballot forms the central aim. Transparency remains visible throughout the process without slowing performance down. This study introduces a method for digital voting that prevents duplicate submissions. By combining facial recognition with one-time password checks, identity confirmation becomes more reliable.**

***Keywords:*** Online Voting System, Face Recognition, OTP Authentication, Security, Duplicate Vote Prevention, Testing.

## I. INTRODUCTION

One way people shape government involves casting votes, a core part of democracies. Though common, older voting techniques bring problems like mistakes by hand, slow counting, lines that last hours. Issues also arise from fake identities at polls or multiple ballots cast by one person. Trust weakens when results take too long or tampering occurs behind closed doors. These flaws open space for doubt about fairness in outcomes determined this way. As digital tools progress, machines that count votes electronically now offer a different method meant to speed up elections while making them easier to access. Still, several of these setup's struggle with serious issues - keeping user identities verified, protecting information from changes, avoiding repeated ballots by single voters.

This study introduces a method for digital voting that prevents duplicate submissions. By combining facial recognition with one-time password checks, identity confirmation becomes more reliable. What sets it apart is how verification links to existing records for consistency. Ensuring each individual casts only one ballot forms the central aim. Transparency remains visible throughout the process without slowing performance down.

Should issues arise, immediate detection becomes possible due to continuous monitoring built into the framework. Trust grows when outcomes appear without long waits, a result achieved through instant tallying of ballots. Because safeguards are woven into each step, unauthorized changes face strong resistance across the network. User access remains protected by layered authentication methods that adapt to emerging threats. Interfaces respond clearly, guiding voters with minimal confusion throughout the procedure.

## II. LITERATURE SURVEY

Years passed brought many ideas meant to strengthen how secure and dependable e-voting can be, especially when confirming identities or blocking dishonest actions.

In 2020, R. Chandramohan designed an electronic voting method relying on fingerprint-based biometrics for security. Despite enhancing voter eligibility control, reliance on physical scanning devices creates barriers for distant participation. Each ballot gets tied to a distinct biological identifier, which minimizes repeated submissions along with unapproved entries. Still, absence of adaptability in digital or isolated environments emerges due to equipment requirements.

A. Kumar in 2021 introduced a digital voting method using facial identification alongside one-time passwords. Instead of relying on just one check, it confirms identity through physical traits as well as electronic access. Because both layers must align, unauthorized attempts are less likely to succeed. When tested, this combination proved stronger than systems using only biometrics or codes alone.

 

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 10, Issue 4, pp 303-307, April-2026

https://doi.org/10.47001/IRJIET/2026.104043

Just as before, S. Singh in 2022 introduced a voting method using face recognition technology. With an emphasis on confirming voter identity, it works by identifying and comparing facial traits to block unauthorized participation. Although capable of minimizing false identities, duplication remains possible once access is granted. Despite accuracy gains, repeated votes slip through after initial validation.

In 2021, M. Patel examined a voting method based on facial features to reduce fraudulent activity. Security takes priority during access through identity confirmation prior to entry into the ballot process. Despite stronger checks at initial entry, safeguards beyond verification remain underdeveloped. Once logged in, controls that limit actions are not effectively maintained throughout the procedure.

In 2019, K. Zhang proposed a voting method using blockchain alongside one-time password checks. With blockchain's unchangeable nature, votes are stored securely while allowing full visibility. After entry, each ballot remains fixed - no changes possible afterward, which blocks unauthorized edits or repeated submissions. Still, due to high processing demands and intricate setup, applying such systems may prove difficult when scaled down.

**Table 1: Literature Survey Review**

| No. | Author & Year | Tittle | Method Used | Security Feature | Result |
|---|---|---|---|---|---|
| 1 | R. Chandramohan, 2020 | Secured Electronic Voting System Using Biometrics | Biometric Authentication | Fingerprint verification | Prevents duplicate voting and unauthorized access |
| 2 | A. Kumar, 2021 | Online Voting System Using Face Recognition and OTP | Face Recognition and OTP | Two-factor authentication | Only authorized users can vote |
| 3 | S. Singh, 2022 | Smart Voting System Using Face Recognition | Facial Detection | Identity verification | Prevents fake voters |
| 4 | M. Patel, 2021 | Biometric Voting System | Facial recognition | Fraud prevention | Secure authentication |
| 5 | K. Zhang, 2019 | Blockchain Based Voting System | Blockchain and OTP | Secure vote storage | No duplicate voting |

It becomes clear through examining these studies that progress in authentication and vote security exists, yet numerous systems handle identity checks and blocking repeat votes independently. Not every framework links voter proofing with action oversight effectively. A cohesive method stands necessary - one confirming who votes while managing how voting occurs. Integration of layered login methods alongside a database-backed system to stop multiple submissions forms the core response here. Security at entry combined with regulated casting emerges as the outcome.

## III. PROPOSED METHODOLOGY

The proposed system consists of multiple modules working together to ensure secure and duplicate-free voting.

### A. System Overview

The system follows a layered architecture:

- User Authentication Layer
- Voting Layer
- Data Storage and Security Layer
- Admin and Result Layer

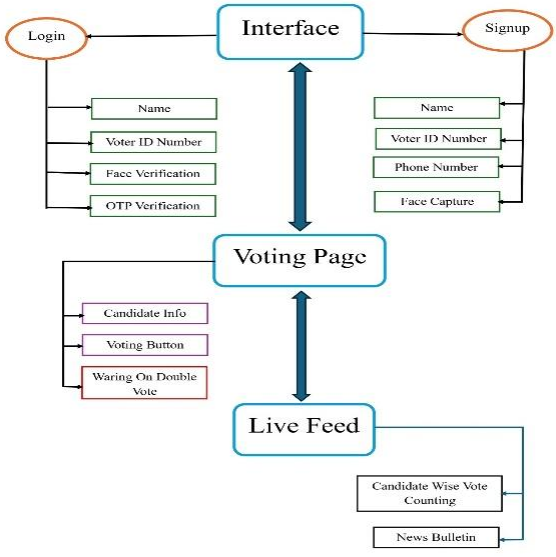


**Figure 1: System Architecture**

 

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 10, Issue 4, pp 303-307, April-2026

https://doi.org/10.47001/IRJIET/2026.104043

In Figure 1, It shows the whole structure of the System. How each page works with its individual material to provide the best experience and safety.

### B. Module-wise Algorithm

#### 1. User Registration Module

Algorithm:

- Enter voter information including ID number phone number and email address
- Capture facial image
- FaceNet extracts facial features
- Store Embeddings and User Data in Database

Current voting status = NOT VOTED

#### 2. Face Recognition Module

Algorithm:

- Capture live image
- Preprocess image
- Extract facial features
- As opposed to referencing saved vector representation

If match → proceed, Else → reject

#### 3. OTP Verification Module

Algorithm:

- Generate 6-digit OTP
- Send OTP to registered user
- User inputs OTP
- Verify OTP

If correct → authentication successful,

Else → deny access

#### 4. Anti-Duplicate Voting Module

Algorithm:

- Check if you are registered as voter,

If status = NOT VOTED (allow voting)

After vote submission:

- Store vote securely
- Update status = VOTED,

If status = VOTED (block voting)

#### 5. Voting and Counting Module

Algorithm:

- Display candidate list
- Accept single vote
- Store encrypted vote
- Update vote count
- Display real-time results

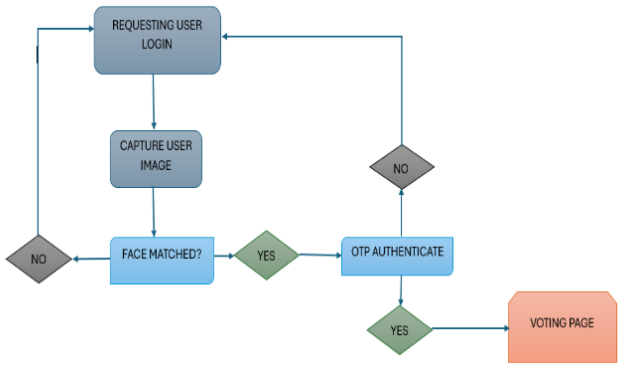


**Figure 2: System Workflow**

In Figure 2, it shows the system working flow. During Login the system first check the user facial data with the existing data and if it is successful then otp sent to the user registered phone is verified. In case of not fulfilling those can reject the login.

## IV. RESULTS

During the testing, tests covered many real-world scenarios. In everyday conditions, how well it worked and how steady it performed got recorded. Face recognition hit between 90 and 95 percentage, depending on light levels, sensor interference, or picture sharpness. Rather than just racing through steps, single-use code validation held strong, identifying true users without delays worth mentioning. Most times, each ballot moved through in less than two seconds. Still the system stopped anyone from voting twice just like it was meant to do.

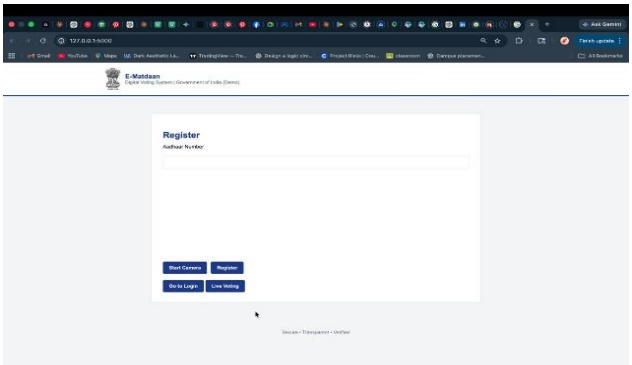


**Figure 3: Main Interface**

 

*International Research Journal of Innovations in Engineering and Technology (IRJIET)*

**ISSN (online): 2581-3048**

**Volume 10, Issue 4, pp 303-307, April-2026**

https://doi.org/10.47001/IRJIET/2026.104043

In Figure 3, it is the main interface of the System. From this page user can easily access the login, signup and the live vote counting via a secure verification method.

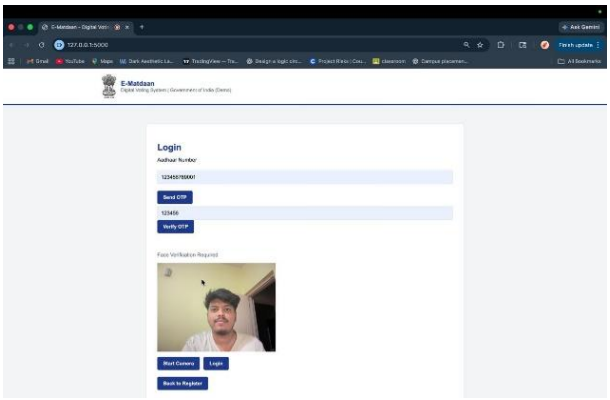


**Figure 4: Face Verification Login**

For making the logging system more secure the face verification process take places in login. It compares previously registered face as shown in the Figure 4.

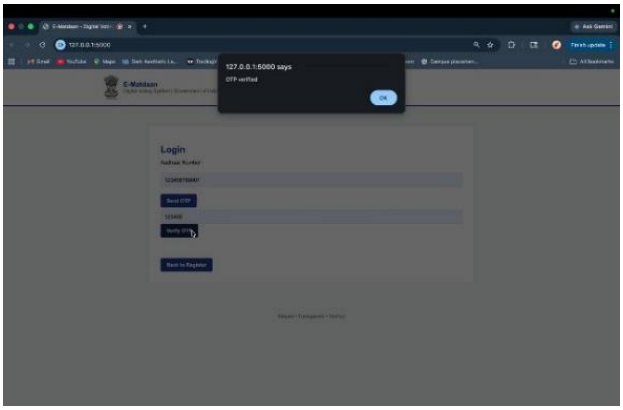


**Figure 5: OTP Verification**

In a part of login process user have to verify a OTP sent to his/her registered phone number with the ID. For keeping the login process secure the OTP Verification happens like Figure 5.

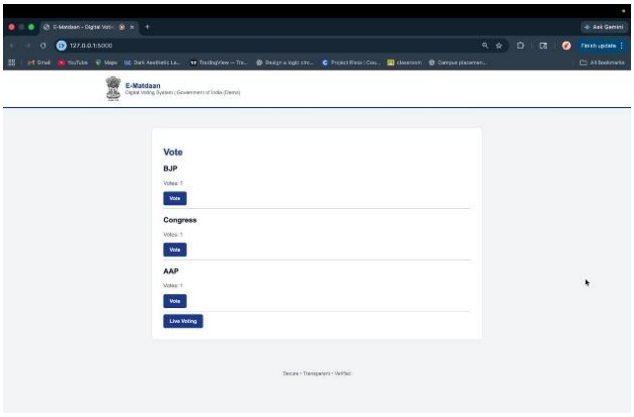


**Figure 6: Voting Page**

In Figure 6, the name of the candidates of each party attending in the election will be there User can only vote once in any of the preferred Candidate.

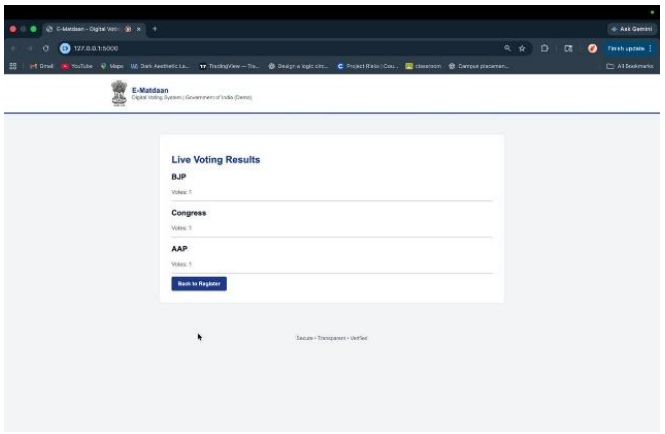


**Figure 7: Vote Counting**

Same as Figure 7, after finishing the allotted time for voting this page will be access able to the public to see the live voting result. Any user can access this page, but user can only vote once.

Performance plus reliability were assessed through testing in diverse conditions. Under multiple setups the system underwent evaluation for results.

**Key Observations:**

- Accuracy of face recognition ranges between ninety percent and ninety-five percent
- OTP verification success rate: High reliability
- Processing votes takes under two seconds
- Duplicate voting attempts: Successfully blocked

## V. CONCLUSION

By conducting this study it introduces a method for digital voting focused on stopping repeated votes. More than relying on single checks it helps in layering two step identification steps with a live counting system. By using this system, every user is verified before casting a vote. The system blocks reuse by verifying inputs with the existing data base in real time. In the system one main feature is its access depends on user previous voting history. Only those who did not voted yet may proceed

It indicates that when the method is used in controlled environments; both practicality and accuracy may be observed. Beside the limitations, which are related to equipment requirements and reliance on internet connectivity, the main basic functions are essentially running. Under some of the circumstances, performance remains stable beside these limitations.

 

ISSN (online): 2581-3048
Volume 10, Issue 4, pp 303-307, April-2026
https://doi.org/10.47001/IRJIET/2026.104043

Stronger biometrics and closer security analysis may be the top priorities for future developments. When the developer allows for new feature, a new section and security is possible. This method clearly demonstrates the combination of security and usability.

## REFERENCES

[1] R. Chandramohan, G. Nagarajan, and S. Eswaran, "Secured Electronic Voting System Using Biometrics," *International Journal of Engineering Research & Technology (IJERT)*, vol. 9, no. 5, pp. 1–5, May 2020. [Online]. Available: https://www.ijert.org/secured-electronic-voting-system-using-biometrics

[2] A.Kumar and P. Singh, "Online Voting System Using Face Recognition and OTP," *International Journal of Scientific Research in Computer Science*, vol. 8, no. 6, pp. 12–16, 2021. [Online]. Available: https://paperrs.ssrn.com

[3] S. Singh, R. Sharma, and K. Gupta, "Smart Voting System Using Face Recognition," *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, vol. 11, no. 5, pp. 656–660, May 2022. [Online]. Available: https://ijarcce.com

[4] M. Patel and N. Shah, "Biometric Voting System Using Facial Recognition," *International Journal of Innovative Research in Technology*, vol. 7, no. 10, pp. 45–49, 2021. [Online]. Available: https://www.ijert.org/online-voting-system-using-face-recognition-and-fraud-detection

[5] K. Zhang, H. Wang, and Y. Chen, "Blockchain-Based Electronic Voting System," *International Journal of Computer Science and Network Security*, vol. 19, no. 2, pp. 1–6, Feb. 2019. [Online]. Available: https://www.researchgate.net/publication/369615959

[6] P. Jain, A. Jain, and R. Gupta, "Hybrid Biometric Electronic Voting System," *arXiv preprint arXiv:*1801.02430, pp. 1–6, Jan. 2018. [Online]. Available: https://arxiv.org/pdf/1801.02430.pdf

[7] T. Shanthi and R. S. Kumar, "Secure Online Voting System Using Multi-Factor Authentication," *International Journal of Recent Technology and Engineering*, vol. 8, no. 4, pp. 2277–3878, Nov. 2019.

[8] A.K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, Jan. 2004. doi: 10.1109/TCSVT.2003.818.

**Citation of this Article:**

Bhumesh K Parihar, Janaki Kandasamy, Jit Mozumder Anik, Sandipan Bairagi, & Wasim Ahamed Samani. (2026). Digital Voting System with Anti-Duplicate Voting Mechanism. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 10(4), 303-307. Article DOI https://doi.org/10.47001/IRJIET/2026.104043

*******

 