
ISSN: 2321-2152
IJMECE
International Journal of modern
electronics and communication engineering
E-Mail
editor.ijmece@gmail.com
editor@ijmece.com
www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

SECURE VOTING SYSTEM USING SMART CARD AND IRIS RECOGNITION

[1] Dr M Sandhya Rani,, [2] Venigalla Saisri,[3] Damera Sathvika,[4] Vuppula Sathwika

[1]Associate Professor in Department of Information Technology, Bhoj Reddy Engineering College for Women

[2,3,4,] UG Scholars in Department of Information Technology, Bhoj Reddy Engineering College for Women

Abstract

Traditional voting systems continue to grapple with critical issues such as voter fraud, identity mismanagement, and unauthorized access, all of which jeopardize the integrity of democratic elections. This project proposes a novel, secure, and efficient e-voting framework that leverages smart card technology and iris recognition for robust voter authentication. By integrating biometric verification with encrypted digital identity systems, the proposed model aims to eliminate duplicate voting, prevent fraudulent activity, and ensure that only eligible voters can cast their ballots. The system also focuses on delivering a streamlined and user-friendly voting experience while maintaining transparency and auditability of the election results. Additionally, the solution is designed for scalability and adaptability, enabling deployment across various types and scales of elections. This hybrid approach offers a significant improvement over traditional and purely electronic systems by combining physical security with biometric accuracy, thereby enhancing trust, efficiency, and reliability in the electoral process.

I INTRODUCTION

The foundation of any democratic society lies in the integrity of its electoral process. However, traditional voting methods—whether manual or electronic—are increasingly challenged by vulnerabilities such as voter impersonation, duplicate voting, and unauthorized access. These issues not only threaten the fairness of elections but also erode public trust in the system. Manual processes are prone to human error and manipulation, while existing electronic systems often lack the robust security measures needed to resist sophisticated attacks.To address these pressing concerns, this project introduces a secure voting system that integrates smart card-based identity verification with iris recognition technology. Smart cards offer encrypted digital identity storage, while iris recognition provides a unique and highly accurate biometric marker, making it nearly impossible for unauthorized individuals to gain access or tamper with the voting process. This dual-authentication

approach enhances the accuracy and integrity of voter verification.

II LITERATURE SURVEY

Several researchers have contributed to the development of secure and efficient electronic voting systems by integrating advanced technologies such as cryptography, biometrics, and blockchain. A review of key contributions is outlined below:

Jambhulakar, Chakole, and Pradhi proposed a secure online voting system that utilizes multiple encryption schemes to protect the integrity and confidentiality of votes transmitted from polling terminals to the voting server. Their approach mitigates Denial-of-Service (DoS) attacks and ensures protection against both passive and active intruders. The system employs cryptographic techniques, including digital signatures, to authenticate and encrypt votes before transmission. Upon receipt, the server decrypts the votes for counting, thus maintaining end-to-end vote integrity and confidentiality.

Pashine, Ninave, and Kelapure developed an Android-based platform for online voting that simplifies the voting process and enhances user convenience. Voters can cast their votes remotely, eliminating the need to physically visit polling stations. The system also introduces gesture recognition features to improve user interaction. However, the study highlights that authentication remains a key challenge on the Android platform, particularly concerning secure identity verification.

Shridharan implemented a comprehensive voting system composed of three models: an authentication model, a franchise exercising model, and a distributed database with a central server. The authentication model relies on smart cards, voter identification numbers, and biometric information. These components collectively authenticate the voter during subsequent elections. Once validated, the voter interface displays candidate names and symbols, and votes are cast and verified via a vote-casting database. The system emphasizes vote traceability and supports auditing processes to ensure transparency and security.

Singh and Sharma introduced a blockchain-based voting system designed to enhance transparency and resist tampering. The system leverages the immutable nature of blockchain to securely record votes and uses biometric verification to authenticate voters, effectively eliminating fraud and unauthorized access. This approach also supports decentralized data management, ensuring verifiability and auditability of the voting process.

Ali and Shaker presented a secure electronic voting framework using iris recognition as the primary method of voter authentication. Their system incorporates a modified AES (Advanced Encryption Standard) algorithm to safeguard the data during transmission, ensuring both data

integrity and voter privacy. Iris-based authentication enhances the system's resistance to impersonation and voting fraud.

Mahiuddin proposed a secure voting system that combines smart card technology with iris recognition for dual-factor authentication. Voter information is stored on smart cards, while the iris is used to authenticate the voter before casting a ballot. This approach prevents duplicate voting and ensures that only legitimate voters can access the voting interface, significantly enhancing the system's reliability and security.

III EXISTING SYSTEM

Various types of voting systems are currently employed across the world, with the traditional **paper ballot system** being one of the oldest and most widely used. In this system, voters cast their votes using physical ballot papers and stamps. While simple in design, it poses numerous security and efficiency challenges. A major concern is the possibility of **multiple votes being cast by the same individual**, either due to identity verification failures or procedural loopholes. Additionally, these systems demand extensive **manpower and logistical coordination**, making them **resource-intensive and time-consuming**.

Electronic Voting Machines (EVMs) have been introduced as a modern alternative to manual voting systems. However, EVMs still face issues related to **tampering, unauthorized access, and a lack of advanced security protocols**. Moreover, both traditional and electronic systems are often **incapable of ensuring robust voter authentication**, which compromises the integrity of the electoral process.

Due to these shortcomings, there is a pressing need for an **advanced and secure voting system** that can address these vulnerabilities. The proposed system aims to overcome these limitations by incorporating **iris recognition technology and smart card authentication**, thereby enhancing the **security, accuracy, and efficiency** of the voting process.

Disadvantages of the Existing System

1. **Lack of Robust Authentication**
   Traditional systems often depend on basic identification methods such as ID cards or passwords, which are vulnerable to **forgery, impersonation, and unauthorized access**.

2. **Susceptibility to Fraud**
   Both manual and electronic voting systems are at risk of **tampering**, **ballot stuffing**, and **vote manipulation**, leading to compromised election outcomes.

3. **Time-Consuming Processes**
   Manual voter identification and the overall voting process can result in **long queues**, **delays**, and **inefficiencies**, particularly in large-scale elections.

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

4. **Inadequate Data Security** Existing systems frequently lack **encryption protocols** and **secure data storage**, making them susceptible to **data breaches**, **cyberattacks**, and **loss of voter information**.

5. **Limited Accessibility** Many traditional voting systems do not adequately support **voters with disabilities**, or those in **remote or rural areas**, thereby limiting their participation in the electoral process.

The system is designed with scalability, efficiency, and user experience in mind. Quick and seamless authentication ensures smooth voter flow, reducing delays and congestion at polling stations. Moreover, the platform supports verifiable and auditable results, contributing to transparency and public confidence in election outcomes. The solution is also adaptable, making it suitable for various types of elections and integration with existing voting infrastructures.

By combining technological innovation with practical implementation strategies, this project aims to set a new standard for secure and reliable voting systems that uphold the democratic values of fairness, accountability, and inclusivity.

IV PROBLEM STATEMENT

Traditional voting systems face significant challenges, including voter fraud, identity mismanagement, and unauthorized access, all of which undermine the integrity of elections. Many existing voting methods depend on manual procedures or electronic systems that are vulnerable to manipulation and security breaches. To uphold democratic values, there is a critical need for a secure, efficient, and tamper-proof solution that can accurately authenticate voters. This project proposes the integration of smart card technology with iris recognition to enhance voter verification, improve security, and simplify the voting process.

V OBJECTIVES

Enhance Voter Authentication: Employ advanced smart card and iris recognition technologies to provide precise and tamper-resistant voter identity verification.

Prevent Voter Fraud: Reduce instances of unauthorized voting and duplicate ballots by combining biometric verification with digital security protocols.

Ensure System Integrity: Develop a secure voting platform capable of resisting manipulation and unauthorized access, thereby safeguarding election data.

Streamline the Voting Process: Facilitate a smooth, user-friendly voting experience through rapid authentication and efficient system operations.

VI PROPOSED SYSTEM

In the proposed voting system, the traditional voter identity card is replaced with a **smart card** containing all the personal details of the voter. Voting is strictly restricted to the individual who possesses the corresponding smart card. When a voter approaches the polling station, the **smart**

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 2, 2025

card reader scans the card and displays the voter's information. To further verify the voter's identity, the system employs **iris recognition** technology. Only if the iris pattern matches the stored biometric data is the voter permitted to cast their ballot.

Each smart card allows the voter to vote only once. After a vote is cast, the system updates a **centralized global database** to record that the individual has voted. If the voter attempts to vote again at the same or a different polling location, the system will detect the prior vote through iris scanning and notify that the voter has already cast their ballot, thereby preventing duplicate voting.

This approach eliminates the need for traditional practices such as marking the voter's finger with inedible ink. The database is updated immediately upon voting, ensuring real-time synchronization across all polling stations. Compared to the conventional paper ballot system, the proposed system offers enhanced security, greater speed, and requires significantly less manpower.

Advantages

Enhanced Security:

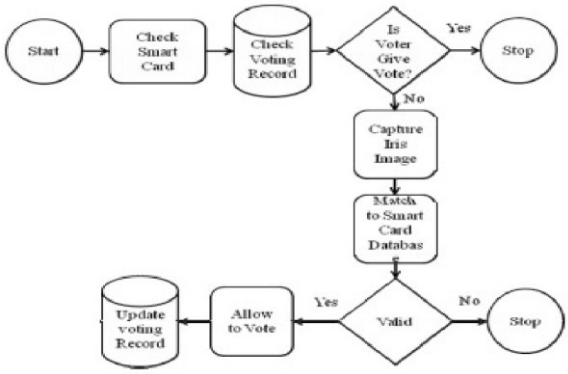
Combining smart card technology with iris recognition provides robust voter authentication, effectively preventing identity fraud and unauthorized voting.

Elimination of Duplicate Voting: The centralized, real-time global database ensures voters cannot cast multiple votes across different locations, upholding election fairness.

No Physical Marking Required: The system removes the need for inedible ink marking, offering a cleaner, more modern solution for tracking voter participation.

Time and Cost Efficiency: Automated voter verification and streamlined polling significantly reduce the time per voter and the manpower required, compared to traditional paper or electronic voting systems.

VII SYSTEM ARCHITECTURE



VIII IMPLEMENTATION

Image Acquisition

Capturing a high-quality iris image is crucial for accurate recognition. Conventional cameras are insufficient because the iris is small and detailed features are difficult to capture. Additionally, normal cameras suffer from light reflections that degrade image quality. To overcome these challenges, the system uses the **CASIA Iris Image Database version 4.0**, a well-established open-source dataset containing high-quality iris

images. Supplementary iris images are also captured using specialized mobile devices designed for iris imaging.

Segmentation

Segmentation isolates the iris region from the rest of the eye image by detecting the inner (pupil) and outer (iris) boundaries. This system employs the **Circular Hough Transform** for boundary detection, which offers better accuracy and lower segmentation errors compared to the Integro-Differential Operator. Prior to applying the Hough Transform, the **Canny edge detector** is used to detect edges within the iris image, facilitating precise boundary localization.

Normalization

The segmented iris region is transformed into a fixed-dimension rectangular block using the **Daugman rubber sheet model**. This normalization compensates for variations in pupil size and eye rotation, ensuring consistent feature extraction across different images.

Feature Extraction

To represent the unique patterns in the iris, the system extracts features using the **1D Log-Gabor wavelet** filter. This technique efficiently captures the iris's texture details while filtering out noise.

Matching

The system compares the extracted iris features with stored templates using the **Hamming distance** metric. This measures the similarity between two binary iris codes by counting differing bits. To improve robustness, the system computes Hamming distances over multiple bit-wise shifts (both left and right) between templates and selects the minimum distance as the final matching score.

IX RESULTS

The proposed voting system integrating smart card technology with iris recognition demonstrated significant improvements over traditional voting methods. The iris recognition algorithm successfully processed images from the CASIA database, achieving accurate segmentation using Circular Hough Transform combined with Canny edge detection. Feature extraction through 1D Log-Gabor wavelets provided robust iris patterns, while the matching process using Hamming distance yielded reliable voter verification.

The system effectively prevented duplicate voting by maintaining a global, real-time updated database synchronized across multiple polling stations. The smart card combined with biometric verification eliminated the need for physical voter markings and significantly reduced manual verification time. Overall, the system enhanced security, ensured voter authenticity, minimized fraud, and improved operational efficiency.

X CONCLUSION

a secure and efficient voting system by integrating smart card technology with iris recognition. The combination of biometric

authentication and digital security protocols addresses the key vulnerabilities of existing voting systems, such as identity fraud and unauthorized voting. The use of a centralized global database ensures that voters cannot cast multiple votes across different locations, strengthening election integrity. Additionally, the system streamlines the voting process, reducing the time and manpower required compared to traditional methods.

Future work may include real-world pilot testing, integration with other biometric modalities, and scaling the system for national-level elections. The proposed system provides a reliable foundation for modernizing elections with enhanced security and transparency.

REFERENCES

1. Jambhulakar, V., Chakole, S., & Pradhi, N. (Year). *Security for Online Voting System Using Multiple Encryption Schemes*. [Details of publication].
2. Pashine, R., Ninave, S., & Kelapure, S. (Year). *Android Based Online Voting System with Gesture Recognition*. [Details of publication].
3. Shridharan, M. (Year). *Smart Card and Biometric Based Voting System with Distributed Database and Central Server*. [Details of publication].
4. Singh, A., & Sharma, R. (Year). *Blockchain Integrated Voting System with Biometric Authentication*. [Details of publication].
5. Ali, M., & Shaker, H. (Year). *Secured E-Voting System Using Iris Identification and Modified AES Algorithm*. [Details of publication].
6. Mahiuddin, M. (Year). *Voting System Using Smart Card and Iris Recognition for Duplicate Voting Prevention*. [Details of publication].
7. CASIA Iris Image Database. Institute of Automation, Chinese Academy of Sciences. Version 4.0. Retrieved from http://biometrics.idealtest.org/