International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Fingerprint Based Voting System Using Deep Learning

BANDARI MITHUN YADAV
B. Tech
School of Engineering
Computer Science – AI&ML
Malla Reddy University, India.

ADLA VISHNU VARDHAN
B. Tech
School of Engineering
Computer Science – AI&ML
Malla Reddy University, India.

BITTUKOLU ANANTH KUMAR
B. Tech
School of Engineering
Computer Science – AI&ML
Malla Reddy University, India.

SURAKANTI MANITEJA
B. Tech
School of Engineering
Computer Science – AI&ML
Malla Reddy University, India.

Guide: J. SOFIA
Asst Professor
School of Engineering
Computer Science – AI&ML
Malla Reddy University, India.

1. ABSTRACT

Fingerprint-based voting systems have gained significant importance in ensuring secure, transparent, and tamper-proof electoral processes. Traditional voting methods are vulnerable to impersonation, duplicate voting, and manual errors, which compromise election integrity. This paper presents a robust deep learning-based biometric authentication framework for secure voting using fingerprint recognition. A comprehensive dataset of fingerprint images collected from registered voters is utilized for training and evaluation. Advanced deep learning models such as Convolutional Neural Networks (CNN) and pre-trained architectures are employed to extract discriminative fingerprint features automatically. Image preprocessing techniques including normalization and noise reduction are applied to improve fingerprint quality and matching accuracy. The extracted deep features are integrated into a secure voting module that verifies voter identity before allowing vote casting. Once authenticated, the system updates the voting status to prevent duplicate voting. The proposed system works by capturing the voter's fingerprint using a fingerprint sensor and comparing it with the stored fingerprint database during the registration phase. Image processing and machine learning techniques are used to enhance fingerprint features and accurately perform matching. Once the fingerprint is verified, the voter is authenticated and allowed to access the voting interface. The system also

checks whether the voter has already voted to prevent duplicate voting. All voter details and voting records are securely stored in a database, ensuring data integrity and privacy. Additionally, the system provides quick verification and reduces the need for manual supervision. This project improves the overall voting experience by making the process faster, more accurate, and less dependent on human involvement. It minimizes fraud, reduces paperwork, and enables efficient vote counting with immediate result generation. The integration of biometric technology with artificial intelligence enhances system reliability and scalability, making it suitable for future smart election environments. The Fingerprint-Based Voting System demonstrates how

modern technology can be used to strengthen election security, increase voter trust, and promote a transparent and efficient digital voting infrastructure.

Keywords- *fingerprint, CNN, Deep Learning, Voting.*

2. INTRODUCTION

Voting is one of the most important processes in a democratic country, allowing citizens to elect their representatives and participate in governance. A transparent and secure voting system is essential to maintain the integrity of elections. Traditional voting systems such as paper ballots and Electronic Voting Machines (EVMs) have been widely used in many countries. Although these systems have improved the efficiency of elections compared to manual methods, they still face several challenges related to voter authentication, security, and transparency. One of the major problems in traditional voting systems is voter impersonation, where an unauthorized person may attempt to vote on behalf of another registered voter. Another issue is duplicate voting, where a voter may attempt to vote multiple times. Manual verification methods also require significant human effort and may introduce errors.

Biometric authentication has emerged as a reliable method to enhance the security of modern voting systems. Biometrics refers to the use of unique biological characteristics such as fingerprints, iris patterns, facial features, or voice patterns to identify individuals. Among these methods, fingerprint recognition is one of the most widely used biometric technologies because fingerprints are unique for every individual and remain stable throughout a person's lifetime. Recent advancements in Artificial Intelligence (AI) and Deep Learning have significantly improved the accuracy and efficiency of biometric recognition systems. Deep learning models are capable of learning complex patterns in biometric data and can provide more accurate identification compared to traditional pattern recognition methods.

This project proposes a Fingerprint Based Voting System using Deep Learning, which authenticates voters based on stored fingerprint data without relying on internet connectivity. The system captures a fingerprint input, compares it with the stored fingerprint database using deep learning techniques, and determines whether the voter is authorized to vote. If the voter is successfully verified, the system allows the voter to cast a vote and stores the voting information in a local file. In the current implementation, the system is developed as a simulation model, where fingerprint inputs are simulated rather than captured using actual hardware devices. In future developments, the system can be integrated with real fingerprint scanners and enhanced with additional security measures such as encryption and secure data storage. The objective of this project is to demonstrate how deep learning techniques can improve the reliability and security of voting systems while reducing dependency on internet connectivity and external infrastructure.

3. LITERATURE REVIEW

Many researchers have worked on improving voting systems by using modern technology. In earlier days, voting was mainly done using paper ballots and manual verification. These methods often caused problems such as counting errors, fraud, and a lot of time required to complete the election process. To improve the efficiency of elections, Electronic Voting Machines (EVMs) were introduced. EVMs helped reduce manual work and made vote counting faster. However, these systems still depend on identification methods such as voter ID cards, which can sometimes be misused by unauthorized individuals. To overcome these problems, researchers started using biometric authentication systems in voting. Biometric systems identify a person using unique physical features such as fingerprints, iris patterns, or facial recognition. Among these methods, fingerprint recognition is widely used because fingerprints are unique for every individual and remain the same throughout a person's life. Some previous voting systems were developed using IoT (Internet of Things) technology. In these systems, fingerprint data is captured using biometric sensors and sent to a cloud server through the internet. The server then checks the fingerprint with the voter database and verifies whether the person is eligible to vote.

Although IoT-based systems improve the voter verification process, they also have some disadvantages. These systems require continuous internet connectivity, which may not be available in rural or remote areas. In addition, sending biometric data over the internet can create security risks, such as data theft or unauthorized access. With recent advancements in Deep Learning, biometric recognition systems have become more accurate and efficient. Deep learning models, especially Convolutional Neural Networks (CNNs), are very effective in analyzing images and identifying patterns. These models can learn important fingerprint features automatically and improve the accuracy of fingerprint matching.

Many studies have shown that deep learning can recognize fingerprints even when there are variations such as different angles, lighting conditions, or partial fingerprints. The proposed project builds on these ideas by developing a deep learning-based fingerprint voting system that works offline. Unlike IoT-based systems, this system does not depend on internet connectivity. Instead, it verifies fingerprints using data stored locally in the system. This approach increases system reliability, reduces network-related risks, and ensures that the voting process can work securely even in areas with limited internet access.

4. PROBLEM STATEMENT

Ensuring a secure and transparent voting process is a major challenge in modern electoral systems. Traditional voting methods face multiple issues related to voter authentication, system reliability, and security.

One of the primary problems is voter impersonation, where unauthorized individuals attempt to vote using someone else's identity. Another significant issue is multiple voting, where the same voter may attempt to vote more than once. These problems can compromise the fairness and integrity of elections.

Existing biometric voting systems often rely on IoT infrastructure and internet connectivity to verify voter identity through remote servers. However, dependence on internet connectivity introduces several limitations. Network failures, slow connectivity, or cyber attacks may disrupt the voting process. Additionally, transmitting sensitive biometric data over the internet increases the risk of data theft or misuse.

Therefore, there is a need for a secure and efficient voting system that can authenticate voters accurately without depending on internet connectivity. The system should ensure that:

- Only registered voters can access the voting system.
- Each voter can vote only once.
- Unregistered or unauthorized users are denied access.
- The voting data is stored securely for result analysis.

To address these challenges, this project proposes a Deep Learning based Fingerprint Voting System that performs offline biometric authentication using stored fingerprint data.

5. PROPOSED SYSTEM

5.1 System Architecture

The overall architecture of the proposed **Fingerprint Based Voting System using Deep Learning** consists of several modules including fingerprint acquisition, preprocessing, feature extraction, voter authentication, voting module, and data storage. The system processes fingerprint images using deep learning techniques to verify voter identity and ensure secure voting.

The architecture diagram below illustrates the workflow of the system from fingerprint input to vote storage and result monitoring.

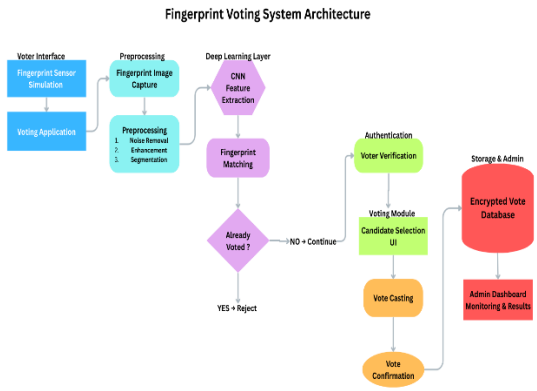

Fig1:- System Architecture

The system begins with the voter interface, where the fingerprint is captured using a simulated fingerprint sensor. The captured fingerprint image is then sent to the preprocessing module, where noise removal, enhancement, and segmentation are performed to improve image quality. Next, the processed fingerprint image is passed to the deep learning layer, where a Convolutional Neural Network (CNN) extracts important fingerprint features. These features are used in the fingerprint matching process to verify the voter.

If the fingerprint matches with a registered voter and the voter has not already voted, the system proceeds to the voting module, where the voter selects a candidate. The vote is then recorded and stored in an encrypted database. Finally, the admin dashboard monitors the voting process and displays the voting results.

5.2 Module Description

The proposed system is designed to provide a secure and efficient voting mechanism using fingerprint authentication and deep learning algorithms. The system

operates without internet connectivity and performs voter verification using locally stored biometric data.

The system consists of several functional components that work together to complete the voting process.

1. Fingerprint Input Module

In this module, the system receives a fingerprint input from the voter. Since the current project is implemented as a simulation, the fingerprint data is provided as a digital input rather than being captured from a physical fingerprint scanner.

2. Preprocessing Module

The captured fingerprint image is preprocessed before being used for recognition. Preprocessing may include image enhancement, noise removal, resizing, and normalization. These steps help improve the quality of the fingerprint image and make it suitable for deep learning analysis.

3. Deep Learning Based Fingerprint Matching

In this stage, the processed fingerprint image is analyzed using a deep learning model. The model extracts unique fingerprint features and compares them with the fingerprint database of registered voters.

If the fingerprint features match with an existing voter record, the system identifies the voter as valid.

4. Voter Authentication

After fingerprint matching, the system verifies whether the voter is registered in the database. If the voter is recognized as a valid voter and has not voted previously, the system allows the voter to proceed to the voting stage.

If the fingerprint does not match any stored record, the system rejects the voter.

5. Voting Module

Once the voter is authenticated, the system displays the available candidates. The voter selects their preferred candidate, and the vote is recorded.

6. Vote Storage

After the vote is cast, the system stores the voting information in a local file. The system also records that the voter has already voted, preventing the voter from voting again.

7. Duplicate Vote Prevention

The system checks the voting history before allowing a vote. If the same voter attempts to vote again, the system detects the previous record and denies the request.

Future Improvements

Although the current system is implemented as a simulation, future improvements may include:

- Integration with real fingerprint scanners
- Implementation of advanced data encryption techniques
- Development of a secure database for voter information
- Deployment of the system in real-world voting environments

5.3 System Workflow

The use case diagram represents the interaction between different users and the fingerprint-based voting system. It illustrates how voters, administrators, and election officers interact with the system to perform different operations.

The diagram identifies the main actors involved in the system and the functions they perform.

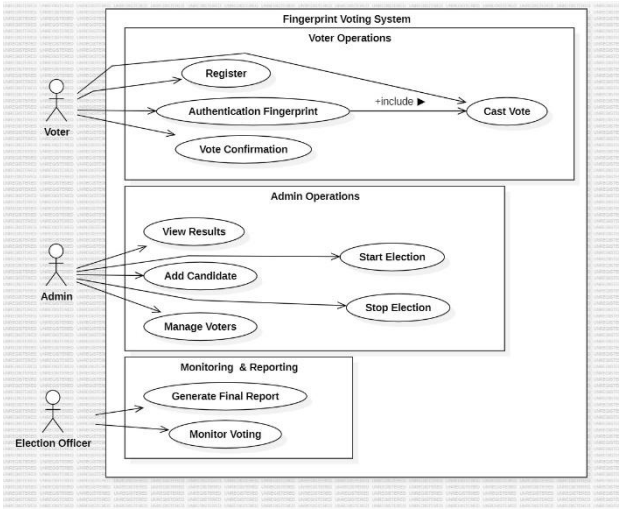

Fig2:- Use Case Diagram

The use case diagram of the fingerprint voting system consists of three main actors: Voter, Admin, and Election Officer.

1. Voter

The voter interacts with the system to perform the following actions:

- **Register** – The voter registers their details and fingerprint in the system.
- **Authentication Fingerprint** – The system verifies the voter by matching the fingerprint with stored data.
- **Cast Vote** – After successful authentication, the voter selects a candidate and casts the vote.
- **Vote Confirmation** – The system confirms that the vote has been successfully recorded.

2. Admin

The administrator manages the overall election process and system data. The admin performs tasks such as:

- **Add Candidate** – The admin adds candidates participating in the election.
- **Manage Voters** – The admin manages voter records in the system.
- **Start Election** – The admin initiates the election process.
- **Stop Election** – The admin stops the election after voting is completed.
- **View Results** – The admin can view the voting results.

3. Election Officer

The election officer monitors the voting process and ensures transparency.

- **Monitor Voting** – The officer supervises the voting process.
- **Generate Final Report** – After the election, the system generates a final report showing voting results.

The use case diagram helps to understand how different users interact with the fingerprint-based voting system and how the system handles various operations.

6. RESULTS AND DISCUSSION

The proposed Fingerprint Based Voting System using Deep Learning was tested using simulated fingerprint data to evaluate the performance and functionality of the system. Since the current implementation is a simulation model, fingerprint inputs were provided in the form of stored fingerprint images instead of using a physical fingerprint scanner. The purpose of testing was to verify whether the system can correctly authenticate voters, prevent unauthorized access, and maintain a secure voting process.

During the testing phase, multiple fingerprint samples were provided to the system. The system first processed the fingerprint images using the preprocessing module, where the image quality was improved by removing noise, enhancing the image, and isolating the fingerprint region. After preprocessing, the fingerprint image was passed to the deep learning model, which extracted important fingerprint features. These extracted features were then compared with the fingerprint data stored in the system database. If the fingerprint matched with a registered voter in the database, the system successfully authenticated the voter. Once the authentication was completed, the voter was allowed to proceed to the voting module where the available candidates were displayed. The voter could then select a candidate and cast their vote. The testing results showed that the system was able to correctly identify registered voters using their fingerprints. The fingerprint matching process worked effectively, and the system allowed the authenticated voters to vote without any issues. This demonstrates that the use of deep learning techniques can improve the accuracy of fingerprint recognition.

The system was also tested to verify its ability to prevent duplicate voting. After a registered voter successfully cast a vote, the system stored the voting status in the database. When the same voter attempted to vote again using the same fingerprint, the system detected that the voter had already voted. In such cases, the system automatically rejected the second voting attempt. This functionality is very important because it prevents voters from voting multiple times and helps maintain the fairness and integrity of the election process. All the votes cast during the testing process were successfully recorded and stored in a local file or database. The stored voting data can later be used to count the votes and determine the election results. This storage mechanism ensures that voting information is properly maintained for result analysis and reporting. One of the key advantages of the proposed system is that it works without requiring internet connectivity. Many existing biometric voting systems depend on cloud servers and internet connections to verify voter data. However, internet connectivity may not always be reliable, especially in rural or remote areas. The proposed system performs fingerprint verification using locally stored data, which allows the system to operate efficiently even without internet access. This improves the reliability and usability of the system.

The use of deep learning algorithms also improves the overall performance of fingerprint recognition. Traditional fingerprint recognition systems rely on basic pattern matching techniques, which may not always provide accurate results when fingerprint images vary in quality or orientation. Deep learning models, such as Convolutional

Neural Networks (CNNs), can automatically learn important fingerprint features and improve the accuracy of the matching process. However, the current system also has some limitations. Since the system is implemented as a simulation model, it does not use a real fingerprint scanner for capturing fingerprint data. Instead, fingerprint images are provided manually for testing purposes. In a real-world implementation, the system should be integrated with a physical fingerprint sensor to capture fingerprints directly from voters. Despite these limitations, the testing results show that the proposed system performs its main functions successfully. The system can authenticate voters using fingerprint recognition, prevent unauthorized access, and stop duplicate voting attempts. These features make the system

more secure compared to traditional voting systems that rely only on voter ID cards or manual verification.

Overall, the results demonstrate that the Fingerprint Based Voting System using Deep Learning is capable of providing a secure and efficient voting process. By combining biometric authentication with deep learning technology, the system improves voter verification accuracy and reduces the risk of election fraud. With further improvements such as integration with real fingerprint hardware and enhanced data security mechanisms, the proposed system can be developed into a reliable solution for modern electronic voting systems.

7. REFERENCES

1. Jain, A.K., Ross, A., and Prabhakar, S., "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology.

2. Maltoni, D., Maio, D., Jain, A., and Prabhakar, S., *Handbook of Fingerprint Recognition*, Springer.

3. Goodfellow, I., Bengio, Y., and Courville, A., *Deep Learning*, MIT Press.

4. Ross, A., Nandakumar, K., and Jain, A., *Handbook of Multibiometrics*, Springer.

5. Bishop, C.M., *Pattern Recognition and Machine Learning*, Springer.

6. Chollet, F., *Deep Learning with Python*, Manning Publications.

7. Jain, A.K., Flynn, P., and Ross, A., *Handbook of Biometrics*, Springer.

8. O'Gorman, L., "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proceedings of the IEEE.

9. Ratha, N.K., Connell, J.H., and Bolle, R.M., "Enhancing Security and Privacy in Biometrics-based Authentication Systems," IBM Systems Journal.

10. Hong, L., Wan, Y., and Jain, A., "Fingerprint Image Enhancement: Algorithm and Performance Evaluation," IEEE Transactions on Pattern Analysis and Machine Intelligence.