BIOMETRIC-ENABLED VOTING SYSTEM DESIGN USING IOT

[1]USHA M, [2]ANANYA L PATIL, [3]KAVYASHREE K N, [4]BHAVYASHREE HARTHI T
Students
Department of CSE
East West Institute of Technology
Visvesvaraya Technological University, Belgaum-50018

Abstract—This study delves into the paradigm shift introduced by a Biometric-Enabled Voting System, emphasizing the integration of pragmatic face and fingerprint detection for enhanced voter authentication. The abstract outlines the fundamental principles behind this design, its applications in electoral settings, and the implications for election security. Through a synthesis of current advancements and practical considerations, the paper highlights the potential of biometric technology to revolutionize the voting experience while addressing concerns related to identity verification. The findings contribute to the discourse on modernizing electoral processes and fortifying democratic systems.

This study explores the integration of pragmatic face and fingerprint detection in a Biometric-Enabled Voting System, aiming to enhance voter authentication in electoral processes. The abstract summarizes the fundamental principles, applications, and transformative potential of this design. Through a synthesis of advancements and practical considerations, the paper emphasizes the role of biometrics in revolutionizing the voting experience while addressing identity verification concerns. The findings contribute to the discourse on modernizing electoral processes, fortifying democratic systems, and fostering trust and transparency in elections.

Keywords—This term emphasizes the incorporation of biometric technologies into the design of a keyboard specifically tailored for use in a voting system, enhancing security and accuracy through features like pragmatic face and fingerprint detection.

I. INTRODUCTION

In the ever-evolving landscape of electoral processes, the integration of advanced technologies becomes paramount to ensure the integrity and security of voting systems. This paper explores the design and implementation of a Biometric-Enabled Voting System, leveraging pragmatic face and fingerprint detection for robust voter authentication. As nations strive for transparent and secure elections, the fusion of biometrics with the traditional Electronic Voting Machine (EVM) emerges as a promising avenue. This introduction sets the stage for a comprehensive examination of the transformative potential and challenges associated with such a design.

The Biometric-Enhanced Voting Keyboard Design represents a pioneering approach in electoral technology, fusing traditional input methods with advanced biometric features. This introduction sets the stage for a discussion on the integration of pragmatic face and fingerprint detection into a keyboard designed for secure and efficient voter authentication in electronic voting systems. Imperative for proactive safety measures. The allure of creative and innovative architectural ideas, while shaping mesmerizing structures, simultaneously amplifies the challenges associated with disaster management.

1. Biometric Integration:

The design centers on seamlessly incorporating pragmatic face and fingerprint detection capabilities into the voting keyboard. This integration aims to enhance the accuracy and reliability of voter authentication during elections.

2.Secure Voter Authentication:

The primary goal is to elevate the security of the voting process by leveraging biometric data. Pragmatic face and fingerprint detection offer a robust means of ensuring that only authorized voters can participate, mitigating the risk of fraudulent activities.

3. Efficient and User-Friendly Design:

The voting keyboard is engineered for user convenience, ensuring that the biometric authentication process is intuitive and swift. The design prioritizes an accessible interface to accommodate a diverse range of voters.

4. Interoperability with Voting Systems:

The keyboard is designed to seamlessly integrate with existing electronic voting systems, creating a harmonious and efficient electoral process. Compatibility and interoperability are essential aspects to streamline the adoption of this technology.

5. Data Security and Privacy:

The design addresses concerns related to data security and privacy, implementing robust measures to safeguard biometric information. Encryption and secure storage protocols are integral components of the overall system architecture.

6. Advancing Electoral Technology:

The Biometric-Enhanced Voting Keyboard Design represents a significant step forward in the evolution of electoral technology. By marrying biometrics with traditional input methods, the design aims to contribute to more secure, transparent, and user-friendly elections.

II. LITERATURE SURVEY

The literature survey conducted for this study is summarized in a tabular format, providing a comprehensive overview of relevant research works. The table encompasses crucial details such as the name of the study, author(s), publication year, research objectives, and key advantages and disadvantages identified in each word

Title	Authors	Year	Objectives	Advantages	Disadvantages
Fingerprint Liveness Detection Using an Improved CNN With Image Scale Equalization [1]	C Yuan, Z Xia, L Jiang, Y Cao, QMJ Wu, X Sun	2019	1. Implementing image scale equalization techniques to address variations in fingerprint image quality and ensure robust performance across diverse conditions. 2. Enhancing the accuracy of fingerprint liveness detection to distinguish between genuine and fake fingerprints. .	Enhanced Accuracy: The improved CNN, coupled with image scale equalization, enhances the accuracy of fingerprint liveness detection, reducing the likelihood of false positives and negatives. 2.Adaptability to Varied Conditions: Image scale equalization allows the system to adapt to variations in fingerprint image quality, ensuring consistent performance in diverse environmental conditions.	1Data Dependency: The performance of the system may be contingent on the availability and quality of the training dataset, and variations in real-world data may pose challenges. 2.Limited Generalization: While the proposed method may excel in certain scenarios, its generalization across all possible spoofing techniques and environmental conditions may be limited.
Face Detection and Recognition Using OpenCV [2]	Maliha Khan; Sudeshna Chakraborty; Rani Astya; Shaveta Khepra	2019	1Implement face recognition techniques to identify and authenticate individuals based on their facial features using OpenCV. 2.Aim for real-time processing capabilities, enabling quick and seamless face detection and recognition for various applications.	1.OpenCV is a comprehensive computer vision library with a wide range of functionalities, making it a versatile choice for face detection and recognition projects. 2. Being an open-source library, OpenCV benefits from a large and active community, ensuring continuous development, updates, and support.	1.In certain challenging conditions, such as low lighting, occlusions, or variations in facial expressions, OpenCV's face recognition may face limitations in accuracy. 2. Face recognition technology raises privacy concerns, and the implementation of such systems should adhere to ethical standards and privacy regulations to avoid potential misuse. .
Multimodal Biometrics Based on Convolutional Neural Network by Two-Layer Fusion [3]	Hui Xu; Miao Qi; Yinghua Lu	2019	1.Develop a two-layer fusion method that combines features extracted from different modalities at different stages of the network, optimizing the utilization of multimodal information. 2. Design the system to be scalable and capable of generalizing across diverse datasets, accommodating variations in biometric data and environmental conditions. .	1.Utilizing multiple modalities allows for more comprehensive biometric identification, increasing the chances of successful recognition and reducing the susceptibility to spoofing or false identifications. Multimodal biometrics can adapt to varied environmental conditions and potential changes in individual biometric characteristics, providing a more adaptable and reliable identification system.	1. Integrating multiple biometric modalities and optimizing the two-layer fusion approach may present challenges, particularly in terms of compatibility, synchronization, and parameter tuning. 2. The effectiveness of the CNN-based two-layer fusion approach may depend on the availability of large and diverse datasets for training, which might pose challenges in certain scenarios

Title	Authors	Year	Objectives	Advantages	Disadvantages
Can a CNN Automatically Learn the Significance of Minutiae Points for Fingerprint Matching. [4]	Anurag Chowdhury; Simon Kirchgasser; Andreas Uhl; Arun Ross	2020	1Explore whether a CNN can autonomously learn and extract meaningful features, particularly focusing on the significance of minutiae points in fingerprint images 2.Assess the scalability and generalization capabilities of a CNN-based approach, determining its effectiveness across a diverse range of fingerprint datasets and conditions. .	1A CNN can adapt to diverse fingerprint datasets and conditions, making it suitable for real-world applications with variations in image quality, orientation, and other factors. 2. By leveraging the automated learning capabilities of a CNN, there's potential for increased matching accuracy, especially in scenarios where traditional methods may struggle with variations in fingerprint images.	1.The effectiveness of a CNN for learning minutiae point significance is contingent on the availability and quality of diverse training data. Limited or biased datasets may impact generalization. 2. CNNs, especially deeper architectures, can be computationally intensive, requiring substantial processing power and resources for training and inference, which could be a limitation in certain environments.
Towards More Accurate Contactless Fingerprint Minutiae Extraction and Pose-Invariant Matching [5]	Hanzhuo Tan; Ajay Kumar	2020	1. Investigate methods to enhance the precision of contactless fingerprint minutiae extraction, aiming for more accurate and reliable identification of minutiae points. 2. Develop techniques to address variations in fingerprint poses during matching, allowing for consistent and accurate identification across different orientations of fingerprint images.	1.The system aims to provide more accurate minutiae extraction, contributing to improved reliability in fingerprint-based identification. 2. Improved accuracy and robustness contribute to enhanced security in contactless fingerprint-based identification, making it more resistant to spoofing attempts and unauthorized access. .	1. Advanced minutiae extraction and pose-invariant matching techniques may introduce increased computational complexity, requiring more processing power and resources. 2. The system's performance may be highly dependent on the availability and diversity of training data, and limitations in the dataset may affect generalization to unseen scenarios.
Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection on Image Processing and CNN [6]	S.JEHOVAH JIREH ARPUTHAMONI; A.GNANA SARAVANAN	2021	1..Incorporate Convolutional Neural Networks to automatically learn and extract features from facial and fingerprint data, enhancing the system's ability to recognize and authenticate voters. 2. Design an efficient and user-friendly online voting platform that leverages biometric authentication for a seamless and secure voting experience.	1.The online voting system increases accessibility, allowing eligible voters to participate in the democratic process conveniently from any location. 2.Leveraging image processing and CNNs can enable real-time processing of biometric data, contributing to the efficiency of the voting system.	1.Biometric data, being sensitive information, raises concerns about privacy. Implementing robust privacy protection measures is crucial to address potential apprehensions among voters. 2.The integration of image processing and CNNs introduces technical complexity, requiring expertise in both computer vision and deep learning for system development and maintenance.

Title	Authors	Year	Objectives	Advantages	Disadvantages
Arduino based Electronic Voting System with Biometric and GSM Features [7]	Venkateswara Rao Ch; M V Pathi A; B S Sailesh A	2022	**1.**Implement biometric features, such as fingerprint recognition, for secure and accurate voter authentication, ensuring that only eligible voters can cast their votes. 2. Design an electronic voting mechanism using Arduino, allowing voters to cast their votes electronically through a user-friendly interface.	1.The electronic voting system streamlines the voting process, making it more efficient and reducing the time required for both voting and result compilation. 2. The use of electronic voting with biometric features and GSM capabilities can make the voting process more accessible and inclusive, accommodating individuals with varying needs.	1. The electronic voting system and GSM modules require a stable power source, and ensuring uninterrupted power supply may be challenging in certain environments. 2. Biometric data and real-time data transmission raise privacy and security concerns, necessitating robust measures to protect voter information and maintain the integrity of the system.
RFID based secure voting system with biometric authentication [8]	M. Vanitha; M. Sathyapriya; P. Vishnuvardhan	2022	1.Implement RFID technology for secure and efficient voter identification, allowing authorized voters to access the voting system using RFID cards or tags. 2.Design the voting system to be tamper-resistant, protecting against fraudulent activities, unauthorized access, or attempts to manipulate the voting data. .	1RFID technology provides a secure and reliable means of voter identification, reducing the risk of unauthorized individuals participating in the voting process. 2.Biometric authentication adds an additional layer of security, ensuring that the person presenting the RFID card is the legitimate voter associated with that card.	1. Implementing both RFID technology and biometric authentication can introduce technical complexity, requiring expertise in hardware, software, and security. 2.The integration of RFID and biometric technologies may involve additional costs, including the acquisition of specialized hardware and software, which can impact the overall project budget.

Title	Authors	Year	Objectives	Advantages	Disadvantages
Smart Voting System Through Face Recognition [9]	Chandra Keerthi Pothina , Atla Indu Reddy, Ravikumar CV	2022	1. Introduce real-time monitoring capabilities to detect and prevent unauthorized access or fraudulent activities during the voting process. 2. Develop a smart and efficient authentication system that relies on facial features, streamlining the voter identification process and minimizing the potential for errors	1. . The technology could potentially allow for remote voting through secure facial detection mechanisms, increasing accessibility for voters who may face challenges attending polling stations. 2.The use of facial detection streamlines the voting process, reducing the time required for identification and enabling a more efficient and convenient experience for voters.	1. The accuracy of facial detection can be influenced by factors such as lighting conditions, 2. Image quality, and variations in facial expressions, introducing technical limitations that may impact performance .
IoT Based Secured Smart Voting System Using Diffie Hellman Algorithm [10]	Vidhya S; Rajesh R; Rohith P; Miruthyunj Sanjay S; Pradeep R; Jeevanantham S	2023	1Implement the Diffie-Hellman key exchange algorithm to establish secure communication channels between devices in the IoT-based voting system. 2.Enable real-time monitoring of the voting system through IoT devices, allowing administrators to receive alerts in case of any suspicious activity or security breaches.	1The use of the Diffie-Hellman algorithm enhances the security of communication channels, protecting sensitive voter data from eavesdropping and unauthorized access. 2. The IoT-based system provides convenience by allowing voters to cast their votes using a variety of devices, enhancing accessibility and participation. .	1.The effectiveness of an IoT-based system is dependent on stable internet connectivity, which may be a limitation in certain regions or during unforeseen circumstances. 2.Deploying an IoT-based system with robust security features may involve additional costs, including hardware, software, and maintenance expenses.

III. METHODOLOGY

User Face Recognition Using Finger print scanning Connect to server Fetch and Display Aadhaar Card Related details If Face& finger print Matches showing the constituency details and allowing person to vote. After voting the message will be displayed as vote casted successfully. Stored in Database If both doesn't match person will not be allowed to vote.

IV. CONCLUSION

Biometric-Enabled Voting System, anchored by pragmatic face and fingerprint detection, emerges as a promising solution for addressing the perennial challenges associated with voter authentication in elections. The study underscores the transformative potential of integrating biometrics into the electoral framework, providing a secure and efficient means of identity verification. As nations navigate the complexities of modernizing their electoral systems, the adoption of such technology signals a commitment to advancing democracy through technological innovation. This paper calls for continued research, implementation, and refinement of Biometric-Enabled Voting Systems to foster trust, transparency, and accessibility in the democratic process. The Biometric-Enhanced Voting Keyboard Design marks a transformative development in electoral technology. By integrating pragmatic face and fingerprint detection into the voting keyboard, this design addresses key challenges in voter authentication, prioritizing security, efficiency, and user accessibility. The potential impact on the electoral landscape is significant, fostering a more secure and trustworthy democratic process.

REFERENCES

[1] Chandra Keerthi Pothina, Atla Indu Reddy"Smart Voting System using Facial Detection"IEEE Journal, April 2020.

[2] Anurag Chowdhury, Simon Kirchgasser, Andreas Uhl, Arun Ross "CNN Automatically Learn the Significance Of Minutiae Points for Fingerprint Matching?"IEEE Conference, Mar 2020.

[3] Samarth Agarwal, Afreen Haider, "Biometrics Based Secured Remote Electronic Voting System". IEEE Conference, Sep 2020.

[4] Suresh Kumar, Tamil Selvan G M, "Block chain Based Secure Voting System Using Lot", IEEE Journal, JAN 2020. Authorized licensed use limited to: Carleton University. Downloaded on May 31,2021 at 12:46:04 UTC from IEEE Xplore. Restrictions apply.

[5] Hanzhuo Tan, Ajay Kumar, "Towards More Accurate Contactless Fingerprint Minutiae Extraction and Pose-Invariant Matching" IEEE Conference 2020.

[6] Chengsheng, Yuan, Zhihua, Xia, "Fingerprint Liveness Detection using an improved CNN with image Scale Equalization" IEEE Journal 2019.

[7] Hui Xui, Miao Qi, "Multimodal Biometrics Based on Convolutional Neural Networks by Two-Layer Fusion" IEEE Conferences 2019.

[8] Abdelleratif EI Idrissi, Youssef El Merabet, "Plamprint Recognition using state-of the art Local texture descriptors." IEEE Conferences 2020.

[9] Uttam U. deshpande, V.S. Malemath, "A Convolution Neural Network-Based Latent Fingerprint Matching Using the Combination of Nearest Neighbor Arrangement Indexing" IEEE Conference, JAN 2020.

[10] Giulia orru, Roberto Casual, "LivDet in Action Fingerprint Liveness Detection Competition" IEEE Conference 2020.

[11] Chengsheng Yuan, Zhihua Xia, "Fingerprint Liveness Detection using an improved CNN With Image Scale Equalization" IEEE Conference, JAN 2019.

[12] Al Takahashi, Yoshinori Koda, "Fingerprint Features Extraction by combining Texture Minutiae, and Frequency Spectrum using Multi -Task CNN", IEEE Conference, Oct 2020.

[13] Ayushi Tamrakar, Neetesh Gupta, "Low Resolution Fingerprint Image Verification using CNN Filter and LSTM Classifier" IEEE Confernce, Jan 2020.

[14] Ishank Geol, N.B.Puhan, "Deep Convolution Neural Network for Double-Identity Fingerprint Detection", IEEE Conference 2020.

[15] Maliha Khan, Rani Astya, "Face Detection And Recognition Using Opencv" IEEE Conference 2020