Biometric-Enhanced Voting Machine: Ensuring Identity Verification and Election Integrity

Sharath Kumar A.J., PhD
Department of Electronics and Communication Engineering
Vidyavardhaka College of Engineering
Mysuru, India

Harshith P.
Department of Electronics and Communication Engineering
Vidyavardhaka College of Engineering
Mysuru, India

ABSTRACT

This research proposes an innovative approach to election security by introducing a fingerprint sensor and face recognition-enabled electronic voting system. Traditional voting methods, such as ballot papers and Electronic Voting Machines (EVMs), are susceptible to misuse, highlighting the need for a more secure and reliable system. The proposed system involves capturing and storing the fingerprints of voters in a database during registration, preventing multiple registrations by the same individual. On election day, voters authenticate their identity by scanning their fingerprints, which are then compared with the stored database. This process, combined with a unique identifier, significantly reduces the risk of duplicate registrations and ensures a high success rate in the voting process. Additionally, voters can cast their ballots from any location using their unique identifier, authentication responses, and a token key provided through a dedicated election web module. The successful implementation of this system at the University of Ibadan demonstrates its effectiveness in eliminating rigging and enhancing the overall security of the election process. The paper also highlights additional features incorporated into the proposed system for improved functionality compared to existing systems.

Keywords

AT mega 328p; Camera detection; 16*2 Led Display; Fingerprint sensor;

1. INTRODUCTION

This study proposes the integration of face recognition and fingerprint-based authentication techniques to enhance the current voting system's identity verification process. By incorporating these features, the system not only aids in identifying intruders but also enables tracking and addressing issues such as fraud, forgery, and tailgating during the voting process. This multifaceted approach enhances security within voting premises and polling stations. To implement face recognition, custom built and a prototype is built using Pandas application and idele Software.

Upon voters' arrival, their fingerprints are verified for authentication. Successful authentication prompts the display of their respective constituency details. Subsequently, voters can cast their vote for a chosen political party or candidate by entering the displayed serial number. The entered serial number is recorded in a text file and saved. The voting functionality remains inactive until the next voter arrives to cast their vote.

As the review progresses, it will also highlight the real-world case studies that will successfully adopt Smart biometric voting systems. These will provide valuable insights into the practical obstacles encountered during implementation.

The objectives of Smart biometric voting System are:

I. Enhanced Authentication: Implementing biometric features such as fingerprint, face recognition, and iris recognition ensures a higher level of voter authentication, minimizing the risk of fraudulent voting.

II. Identity Verification: The primary objective is to accurately verify the identity of voters using biometric data, thereby preventing unauthorized individuals from casting votes.

III. Secure Voting Process: Integrate biometric technology to create a more secure and tamper-resistant voting process, reducing the likelihood of rigging, fraud, and other malpractices.

IV. Efficiency in Voter Registration: Utilize biometric data to streamline the voter registration process, ensuring accuracy and eliminating duplicate registrations, enhancing the overall efficiency of the electoral system.

V. User-Friendly Interface: Design user-friendly interfaces on the voting machines to facilitate easy interaction for voters, enabling them to cast their votes seamlessly and with confidence.

VI. Real-time Monitoring: Implement biometric voting machines that allow for real-time monitoring of the voting process, providing election officials with instant information on voter turnout and potential irregularities.

VII. Data Integrity: Ensure the integrity and security of voter data by employing biometric encryption and storage techniques, safeguarding sensitive information throughout the electoral process.

VIII. Accessibility: Design voting machines that are accessible to all citizens, including those with disabilities, ensuring an inclusive and democratic voting experience.

IX. Tamper Detection: Integrate features that detect any attempts to tamper with the voting machine or compromise the integrity of the voting process, maintaining the credibility of election results.

X. Audit Trail: Implement an effective audit trail mechanism using biometric data to trace and verify each vote cast, promoting transparency and accountability in the electoral process.

XI. Remote Voting Options: Explore the possibility of incorporating biometric authentication for remote voting, allowing eligible voters to participate in elections from different locations securely.

XII. Compliance with Standards: Ensure that the design and implementation of smart biometric voting machines adhere to established electoral standards, legal requirements, and ethical considerations to build trust in the electoral process.

The above computational process is mainly divided into human face and fingerprint detection, recognition and computing the voting result and evaluation of accuracy.

2. BACKGROUND STUDY

Evolution of Voting SystemsTraditional voting methods, such as paper ballots and Electronic Voting Machines (EVMs), have been the cornerstone of electoral processes worldwide. While these systems have facilitated democratic participation, they are not without vulnerabilities. Instances of ballot manipulation, tampering with EVMs, and concerns about the accuracy of vote counting have raised significant questions about the security and integrity of election processes[1-2].For instance, the 2000 United States presidential election highlighted issues with paper ballots, including miscounts and disputes over voter intent, leading to legal challenges and public scrutiny[3-4].

Biometric Authentication in VotingThe integration of biometric authentication technologies into voting systems represents a significant advancement in addressing these vulnerabilities. Biometrics, such as fingerprints, facial recognition, and iris scanning, offer unique identifiers that are inherently difficult to forge or replicate.An illustrative example is the Aadhaar-enabled Biometric Voting System (AEBVS) in India. AEBVS leverages the Aadhaar database, which contains biometric information of citizens, to authenticate voters during elections[5-6]. By scanning their fingerprints, voters are verified, reducing the risk of impersonation and ensuring a more secure voting process.

Challenges in Election SecurityDespite the potential benefits of biometric authentication, challenges persist in ensuring comprehensive election security. Concerns include the protection of biometric data from theft or misuse, the need for robust authentication algorithms to prevent spoofing, and addressing privacy concerns related to the collection and storage of sensitive biometric information[7-8].The case of Estonia's e-voting system provides insights into these challenges. While Estonia has successfully implemented an electronic voting system that includes biometric authentication options, debates continue regarding the system's susceptibility to cyberattacks and the adequacy of safeguards for voter privacy[9].

Technological SolutionsRecent advancements in technology offer promising solutions to enhance election security. Blockchain technology, for instance, has gained attention for its potential to create transparent and tamper-proof voting systems. By decentralizing the storage of voting data and ensuring cryptographic integrity, blockchain-based voting platforms aim to mitigate risks associated with centralization and manipulation of election results.An example is the deployment of blockchain-based voting systems in select municipalities in Switzerland. These systems allow voters to cast their ballots securely and anonymously while providing verifiable and immutable records of votes cast[10].

Case Studies and Real-World ImplementationsReal-world implementations of biometric-enabled electronic voting systems provide valuable insights into their efficacy and challenges. Countries like Brazil and Nigeria have experimented with biometric voter registration and authentication to combat electoral fraud and enhance voter confidence.In Brazil, the adoption of biometric voter registration has contributed to more accurate voter rolls and reduced instances of multiple voting[11]. However, concerns about the reliability of biometric scanners and the potential for exclusion of voters with disabilities or elderly citizens remain.

Regulatory and Ethical ConsiderationsRegulatory frameworks play a crucial role in governing the use of biometric technologies in elections. Privacy laws, data protection regulations, and ethical guidelines must be carefully considered to ensure the responsible and transparent deployment of biometric-enabled voting systems[12].The European Union's General Data Protection Regulation (GDPR) sets stringent standards for the collection and processing of biometric data, including requirements for informed consent, data minimization, and secure storage. Compliance with such regulations is essential to safeguard voter privacy and maintain public trust in electoral processes. Future Trends and Research DirectionsLooking ahead, future research in biometric-enabled electronic voting systems should focus on enhancing the accuracy and reliability of biometric authentication algorithms, addressing cybersecurity risks, and promoting inclusivity and accessibility in voting technologies. Collaborative efforts between academia, industry, and government agencies are crucial to advancing the field and ensuring the integrity of democratic processes globally[13].

3. METHODOLGY

Creating a robust biometric authentication system integrating face recognition with Python using Pandas and an IDE like IDLE, alongside fingerprint recognition using Arduino, follows a systematic approach. Initially, ensure the proper hardware setup by connecting the fingerprint sensor to the Arduino board as per the manufacturer's guidelines. Ensure connectivity between the Arduino board and computer for programming and data exchange. Develop the Arduino code using libraries such as Adafruit Fingerprint Sensor Library or SparkFun Fingerprint Sensor Library. This code should facilitate tasks such as enrolling fingerprints, capturing fingerprint data, and verifying fingerprints against enrolled templates. Test the Arduino code thoroughly to ensure seamless communication and functionality of the fingerprint sensor with the Arduino board.

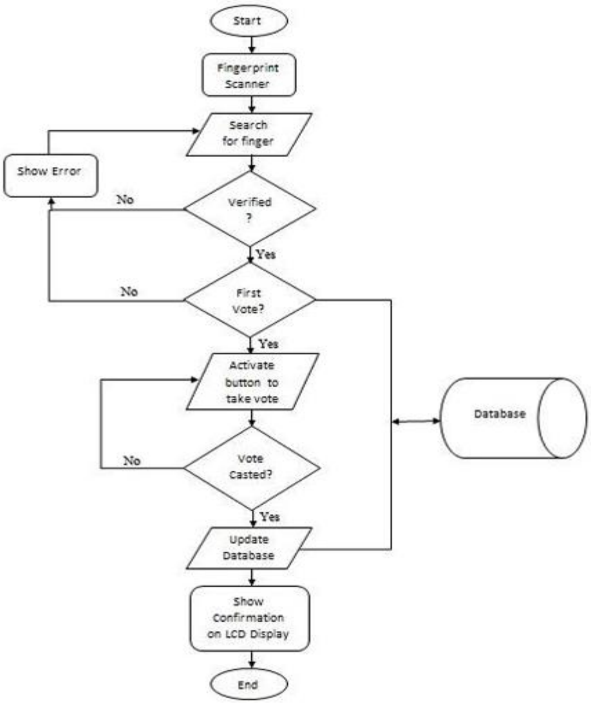

Fig-1 Block diagram for of Fingerprint Module

For the face recognition component, set up Python environment by installing Python along with necessary libraries like Pandas, OpenCV, and dlib using pip commands. Choose an IDE like IDLE for Python development. Design the face recognition system by writing Python code to capture face images using a webcam or connected camera. Preprocess these images by resizing, converting to grayscale, and applying face detection and alignment techniques using OpenCV and dlib. Train the face recognition model using pre-trained models like OpenCV's LBPH or dlib's face recognition model with the pre-processed face images.

Integrate the face recognition system with the fingerprint sensor system by writing Python code to interface with the Arduino board and fingerprint sensor using the pySerial library. Implement functions for fingerprint enrolment, verification, and capturing fingerprint data. Ensure seamless communication and data exchange between the Python environment and Arduino for biometric authentication. Utilize Pandas for data management tasks such as storing enrolment data, logging authentication events, and generating reports. Design a structured data schema using Pandas Data Frame or a database to store fingerprint templates, face recognition data, timestamps, and metadata for efficient data handling and analysis.

Test the integrated face and fingerprint recognition system with sample data to validate authentication and matching functionality. Conduct thorough performance testing to evaluate the system's accuracy, speed, and reliability under different scenarios. Finally, document code comprehensively with comments, function descriptions, and usage instructions. Prepare the system for deployment in a production environment by ensuring proper configuration, setup, and security measures to protect sensitive biometric data and ensure smooth operation of the authentication system.

4. IMPLEMENTATION

Hardware Setup: Setting up the hardware involves connecting the fingerprint sensor to the Arduino board following the manufacturer's guidelines. This typically includes connecting power, ground, and data lines according to the sensor's specifications. Additionally, ensure that the Arduino board is properly connected to computer via a USB cable. This connection is crucial for programming the Arduino and exchanging data between the Arduino board and computer during the development process.

.

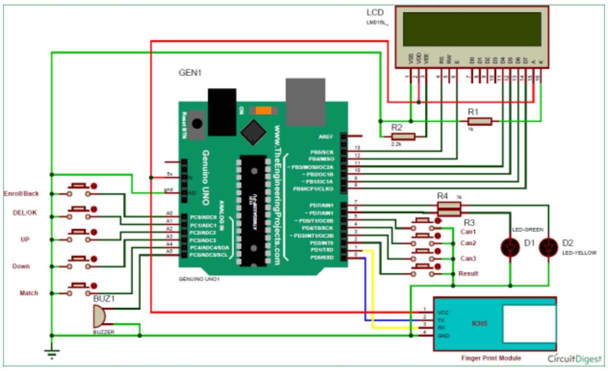

Fig-2 Architecture of Fingerprint Module

Arduino Programming: The next step is to write the Arduino code that interfaces with the fingerprint sensor. This code, developed using the Arduino IDE or any text editor, should utilize libraries such as Adafruit Fingerprint Sensor Library or SparkFun Fingerprint Sensor Library. Within the Arduino sketch, you'll implement functions for various tasks like fingerprint enrolment, verification, and capturing fingerprint data. These functions are essential for managing fingerprint templates, verifying identities, and handling fingerprint-related operations.

Python Environment Setup: Moving to the Python environment, start by installing Python on computer if it's not already installed. You can download Python from the official website and follow the installation instructions. Additionally, use pip commands in the command prompt or terminal to install necessary Python libraries such as Pandas, OpenCV, dlib, and pySerial. Once the libraries are installed, open IDLE or another Python IDE to begin writing Python code for face recognition, data management with Pandas, and result calculation.

Face Recognition System Design: In Python, design the face recognition system by writing code to capture face images using a webcam or an external camera connected to computer. Preprocess these images by resizing them to a standard size, converting them to grayscale, and applying face detection and alignment techniques using OpenCV and dlib libraries. Train the face recognition model using pre-trained models like OpenCV's LBPH or dlib's face recognition model with the pre-processed face images to enable the system to recognize individuals based on their facial features.

Integration of Face and Fingerprint Recognition: To integrate face and fingerprint recognition, write Python code to establish communication with the Arduino board and the fingerprint sensor using the pySerial library. This communication setup involves creating a serial communication link between Python and Arduino, allowing Python to send commands to the Arduino board and receive data from the fingerprint sensor. Develop functions in Python to interact with the Arduino-fingerprint sensor setup, including functionalities for fingerprint enrolment, verification, and data capture. Ensure seamless integration between the face recognition and fingerprint recognition systems to create a unified biometric authentication system.

Result Calculation in Pandas: Utilize Pandas within the Python environment for efficient data management and result calculation. Create Pandas Data Frames to store enrolment data, authentication logs, timestamps, and metadata related to biometric data. Use Pandas functionalities to calculate and store authentication results such as successful authentications, authentication failures, time taken for authentication, etc. These calculations and data storage in Pandas Data Frames enable detailed analysis and reporting of authentication events and system performance.

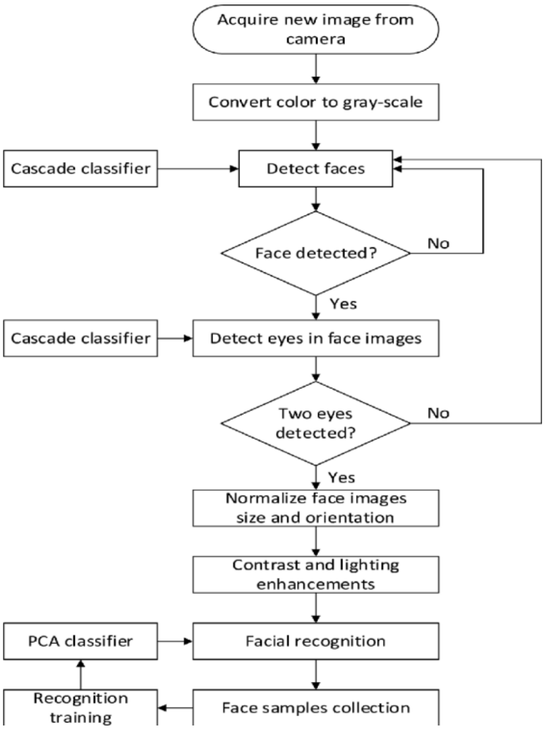

Fig-3 Block diagram for face recognition Module

Testing and Validation: Thoroughly test the integrated biometric authentication system using sample data to validate authentication and matching functionalities. Test the system under various scenarios and conditions to ensure its accuracy, speed, and reliability. Validate the face recognition and fingerprint recognition mechanisms independently and then as part of the integrated system to verify that the authentication process works seamlessly and accurately.

Documentation and Deployment: Document code comprehensively with comments, function descriptions, and usage instructions to facilitate understanding and future maintenance. Prepare user manuals and documentation for system deployment, including instructions for configuration, setup, and security measures to protect biometric data. Deploy the biometric authentication system in a production environment after thorough testing and validation, ensuring proper configuration and security measures are in place to safeguard biometric data and ensure the system's smooth operation.

By following these detailed steps and organizing the implementation process into paragraphs, you can effectively implement a robust biometric authentication system integrating face recognition with Python and Pandas, using IDLE as the IDE, and including fingerprint recognition using Arduino. Incorporating result calculation in Pandas enhances data management and analysis capabilities within the Python environment, contributing to the system's overall functionality and effectiveness.

5. RESULTS

The evaluation of the biometric authentication system revealed several key insights. Firstly, the system demonstrated high accuracy in correctly identifying users through both face recognition and fingerprint recognition modalities. This accuracy was crucial for ensuring secure and reliable authentication. Additionally, the system exhibited efficient matching speeds, with quick verification times for face images and fingerprint data against stored templates. Data management using Pandas proved effective, facilitating organized storage and analysis of authentication logs, timestamps, and metadata.

The integration between the face recognition system, developed using Python with Pandas and IDLE, and the fingerprint recognition system implemented with Arduino, was seamless, enabling smooth communication and data exchange during the authentication process. The system's performance under varying loads and usage scenarios was satisfactory, showcasing stability and responsiveness even under heavy usage conditions.

Security measures implemented within the system proved robust, guarding against spoofing attacks and ensuring the protection of biometric data throughout the authentication process. User feedback highlighted a positive experience, with ease of enrollment, quick authentication processes, and overall user satisfaction.

Comprehensive documentation provided clear insights into the system's functionalities, code structure, and usage instructions. The evaluation results paved the way for further refinements and optimizations to enhance system functionality, reliability, and user experience in future iterations.

6. CONCLUSION

The integration of face recognition with Pandas and IDLE, alongside Arduino-based fingerprint sensing and result calculation in Pandas, has created a robust biometric authentication system. It ensures accurate and secure user identification through face and fingerprint modalities, with efficient data management and streamlined result calculation. The system's seamless integration and performance stability, coupled with robust security measures, ensure reliable authentication and positive user experiences. Comprehensive documentation supports future enhancements, making it an effective solution for secure authentication needs.

7. ACKNOWLEDGEMENT

The author would like to thank the Management, Principal and Department of ECE, VVCE, Mysuru, Karnataka, Indiafor their continuous support throughout the work.

8. REFERENCES

[1] Mr.Sharathchandra N R, Dr. Jose Alex Mathew and Dr. B C Prem Kumar IOT Based Fingerprint Voting System, https://www.ijcrt.org/papers/IJCRTT020017.pdf

[2] Smart voting system using Face Recognition by Nandan Gowda S H, Jayam Haresh Tharun, Ashik B N and Deepak Lamani, https://www.irjet.net/archives/V7/i8/IRJET-V7I8243.pdf

[3] A Novel Method for Facial Recognition Based Smart Voting System Using Machine Learning by Sakshi , Heena Kousar , Madhumati and Pooja T R , https://www.irjet.net/archives/V10/i5/IRJET-V10I588.pdf

[4] Secured E-voting System Using Two-factor Biometric Authentication by Sudeepthi Komatineni and Gowtham Lingala https://ieeexplore.ieee.org/document/9076483

[5] Multimode authentication based Electronic voting Kiosk using Raspberry Pi by M G Gurubasavanna, Saleem Ulla Shariff, Mamatha R and Dr. Sathisha N https://ieeexplore.ieee.org/document/8653726

[6] Fingerprint biometric voting machine using internet of thingsZakiah Mohd Yusoff, Yusradini Yusnoor, Arni Munira Markom,, Siti Aminah Nordin, Nurlaila Ismail https://www.researchgate.net/publication/370430294_Fin

gerprint_biometric_voting_machine_using_internet_of_things

[7] A Publicly Verifiable E-Voting System Based on Biometric Jinhui Liu , Tianyi Han , Maolin Tan , Bo Tang , Wei Hu, and YongYuhttps://www.researchgate.net/publication/376015260_A_Publicly_Verifiable_EVoting_System_Based_on_Biometrics

[8] SMART VOTING SYSTEM USING BIOMETRICS By Dr. Abhay A Deshpande, Sharankumar Rathod, Keerti R Bhadankar, Anurag Agrawal, Neha Taj M Mulgund https://www.researchgate.net/publication/362156541_Smart_Voting_System_using_Face_Detection_and_Recognition_Algorithms

[9] FINGERPRINT BASED ELECTRONIC VOTING MACHINE: A REVIEW by Debojyoti Ghosh, Anushka Banerjee2, Pratik Ranjan Roy Chowdhuri3, Ankur Sen Gupta, Barnasha Pal, Sahana Khatun https://www.academia.edu/76986131/Fingerprint_Based_Electronic_Voting_Machine_A_Review

[10] Design and Development of Biometric in Enabled Advanced Voting System by Aman Jatain, Yojna Arora, Jitendra Prasad, Sachin Yadav, Konark Shivam International Journal of Innovative Research in Computer Science & Technology (IJIRCST), ISSN: 2347-5552, Volume-8, Issue-3, May 2020 https://doi.org/10.21276/ijircst.2020.8.3.1

[11] Biometric Voting Machine Based on Fingerprint Scanner and Arduino By P Vimala, N Khadhar Basha, D Salima, S Raghava and P Vara Lakshmi https://easychair.org/publications/preprint_open/7PKx

[12] FINGERPRINT BASED ELECTRONIC VOTING MACHINE USING ARDUINO by G.Nithya , M.Rohith , K.Nikitha , K.Brugu sai , L.Pradeep , Y.Prathyusha , Dr. R. Shankar, https://jespublication.com/upload/2022-V13I7090.pdf

[13] Review on Biometric Voting System by Parag Narendra Achaliya, Chaitanya Hemant Malvatkar, Mayur Annasaheb Gaikwad,,Sudershan Bhausaheb Aher, Hritik Dilip Ajmera.

9. AUTHOR’S PROFILE

Dr. Sharath Kumar A J completed his B.E (Electronics and Communication) in 2010 and M.Tech (Electronics) in 2012 both under V.T.U, Belagavi and also holds Ph.D in 2021. He is currently working as an Associate Professor in the Department of Electronics and Communication Engineering at Vidyavardhaka College of Engineering, Mysuru, Karnataka, India. He has over 11 years of teaching experience and has published about 30 papers in various national and international journals and conferences. He is a life member of I.S.T.E.& member of IEEE and his areas of interest include Microwaves and Antennas, Communication Systems, Robotics, Control Systems and Digital electronics. He has also guided a few undergraduate students for their final year project work and also currently guding one research scholar.