IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SMART VOTING USING FINGERPRINT AND FACIAL RECOGNITION

[1]Prof. Prabhakara B. K., [2]Adhya Shetty P, [3]Anushree,[4]Ashwitha,[5]Mayoori P

[1]Professor, [2,3,4,5] Students

[1]Department of ISE, A. J. Institute of Engineering and Technology, Mangaluru.

Abstract: Citizens in India have a duty and a right to vote, but the fundamentals of democracy are being called into question by the alarming drop in voter turnout. The old system, which requires actual presence, risks vote tampering and excludes a large number of people, particularly the physically impaired and those living in remote cities. By incorporating Aadhar-linked biometrics, such as fingerprint and facial scans, Secure Vote provides a novel way to strengthen the democratic process. This breakthrough uses face and fingerprint detection to reduce false votes, improving voting security and accuracy with LBPH (Local Binary Pattern Histogram) algorithms. But protecting privacy, safeguarding data, and accommodating those without Aadhar present significant issues that need to be resolved if this revolutionary strategy to strengthen democracy is to succeed.

I. INTRODUCTION

The Smart Voting System uses Aadhar cards with face and fingerprint scans as personalized keys for secure voting. This minimizes fraud, ensuring each vote is genuine. It's like having a special lock for every vote, making the process fair and transparent. Linking Aadhar with biometrics enhances reliability, building confidence in the system. This system acts as a safeguard, preventing identity fraud and promoting secure elections. It fosters trust, making sure each vote is real and counts, upholding the principles of fairness in governance.

Though the secure voting system that uses facial and fingerprint recognition. This online voting uses image processing to detect voters faces by HAAR Cascade Algorithm. Face and fingerprint image features are exacted and compared with the database. The system proposed in the present paper, shall serve with a set of innovative advantages namely, and reduced rigging and fake/invalid votes, ease of carrying the machine, faster and most accurate voting process.

II. PROBLEM STATEMENT

The existing voting system confronts significant challenges, including issues of voter duplication, fraudulent activities, prolonged queues at polling stations, and the potential for unauthorized voting from different locations. These challenges compromise the integrity and reliability of the democratic process. To address these issues, a fundamental overhaul is proposed: transitioning from conventional voter IDs to Aadhar cards, which incorporate biometric features such as fingerprints for unique identification. This shift aims to enhance the security of the voting process by minimizing the risks associated with duplicate and fake votes. Aadhar-based identification ensures a more precise verification of voters' identities, contributing to a more secure electoral system.Beyond the security aspect, the proposed solution targets operational inefficiencies in the voting process. The introduction of Aadhar-based identification not only strengthens security but also streamlines the voting process, eliminating the need for extensive queues at polling stations. This not only enhances the overall efficiency of the electoral system but also facilitates greater

III. OBJECTIVES

To create an application which performs the following functionalities

- Enhanced Security: Implement advanced biometric features, such as face and fingerprint scans, to strengthen voter identification and authentication.
- Integration with Aadhar Database: Integrate the voting system with the Aadhar database, leveraging its comprehensive and secure repository of citizen information.
- Streamlined Authentication: Simplify and streamline the voter authentication process using biometric data linked to Aadhar cards. This not only ensures accuracy but also facilitates a smooth and efficient voting experience for citizens.
- Tamper-Proof Voting: Develop a system that prevents tampering and manipulation of votes. By utilizing the Aadhar database as a secure foundation, the project seeks to eliminate vulnerabilities and provide a robust defense against any attempts to compromise the integrity of the voting process.
- Transparency and Trust: Foster transparency in the electoral process by utilizing advanced technology and the Aadhar database. The project aims to build trust among voters by providing a secure, transparent, and reliable platform for expressing their democratic rights.

IV. EXPECTED OUTCOME

This application utilizes biometric authentication to significantly reduce voter fraud, ensuring only eligible individuals participate and enhancing election accuracy. The voting system promotes confidence, encouraging greater participation. Biometric identification aids those struggling with traditional forms, and a secure, location-flexible system minimizes errors, reducing costs while promoting convenience and accessibility.

V. LITERATURE SURVEY

Although there are many research works on online/smart voting systems, here in this chapter we have critically analysed and summarized several research works and projects, which are more recent and relevant and similar to project. This literature survey will logically explain the system.

1. Smart Online Voting System: Ganesh Prabhu S, et al. system approach [1] to voting systems by leveraging face recognition technology to develop a secure internet voting system. The paper proposes an advanced voting system addressing traditional limitations through online/offline options, face recognition, and OTP authentication. Eliminating the need for election officers and paper ballots, it enables location-independent voting with real-time result viewing. Emphasizing efficiency and security, the authors advocate for a more accessible democratic process. Published in 2017, it signifies a significant contribution to voting technology discourse and potential future advancements.

2.Biometric Based Secured Remote Electronic Voting System: Samarth Agarwal, et al. system approach [2] presents the development of system to address issues such as rigging and fake voting in elections .The paper introduces an electronic voting system using a fingerprint sensor, Arduino, and matrix keypad for secure elections. It verifies voter identities, preventing duplicates. Featuring a comprehensive literature review, methodology, and real-life case studies, it recommends national-level implementation. The paper contributes to biometric-based electronic voting systems' understanding and development, offering a detailed overview of Arduino and fingerprint sensor integration.

3. A Secured Biometric Voting System Using RFID Linked with the Aadhar Database: P.M. Benson Mansingh, et al. approach [3] a system to develop a secured biometric voting system by integrating RFID technology with the Aadhar database. The project addresses voting system limitations by advocating a biometric-based approach using RFID tags, fingerprint scanning, IoT, Raspberry Pi, and future integration of face and IRIS technology. It aims to enhance security, efficiency, and accuracy in voting, potentially revolutionizing the process. The paper demonstrates a deep understanding of biometric recognition advancements.

4. Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection on Image Processing and CNN: Chandra Keerthi Pothina, et al. approach [4] presents an innovative online smart voting system that leverages biometrics-based facial and fingerprint detection for secure and convenient voting. This web-based voting system employs image processing and Convolutional Neural Networks for precise face and fingerprint recognition, reducing duplicate votes globally. Aimed at improving efficiency

and accessibility, it addresses limitations in India's voting system. The methodology involves capturing and comparing facial and fingerprint images, integrating Haar Cascade and Adaboost algorithms. The article discusses potential improvements and references related studies, emphasizing enhanced security, efficiency, and accessibility.

5. Fingerprint Based Secured Voting: Khadija Hasta, et al. presents [5] a Fingerprint Based Biometric Voting Machine using Arduino, which employs SHA-1 encryption to safeguard data and a fingerprint-based voting system to ensure secure and accurate voting. The tested system proves effective and user-friendly, suggesting improvements with additional biometric features and advanced algorithms. It addresses online voting challenges through fingerprint authentication, a matching algorithm, and Captcha for security. Drawing on past research, it offers a secure and reliable online voting platform with biometric authentication, encryption, and security measures, promising a modernized voting process.

6. Smart and Secure Voting System Using Biometrics :A. BalaMurali, et al. approach [6] creates a comprehensive solution to address the challenges of the existing voting system in India. The proposed smart voting system integrates GSM, SMS, GPS, fingerprint, image scanners, LCD, EVM, and cloud-based databases for secure and efficient elections. Utilizing biometric verification, confirmation messages, and cryptographic techniques, it enhances security. The inclusion of GPS and cloud databases strengthens reliability. The paper concludes with results, future improvements, and references, presenting a promising solution for India's voting process.

7. Facial Recognition and detection using OpenCV: Maliha Khan, et al. approach [7] gives a comprehensive overview of the application of OpenCV for face detection and recognition. The paper explores facial recognition algorithms such as Haar cascade, Eigenfaces, Fisher face, and LBPH, detailing their significance. It delves into the practical implementation and application of these algorithms, highlighting the role of PCA. Emphasizing ongoing research, future work, and references, the paper serves as a valuable resource for researchers and practitioners in face detection and recognition using OpenCV and related algorithms.

8. An Approach for e-Voting using Face and Fingerprint Verification: Shubham Shinde, et al. created approach [8] requiring voters to register with fingerprint and face images, which are securely stored on a server-side file system. The paper introduces an e-Voting system for India, leveraging Google Firebase for voter data. It addresses challenges faced during prolonged elections, focusing on difficulties for NRIs and service voters. Using fingerprint and face verification, the system streamlines remote voting, ensuring anonymity and preventing candidate access to trends. The scalable design aims to modernize and optimize India's voting process.

9. Paper Ballot System: The era before 2004 used Paper Ballot System. Voters had to go to polling booths and cast their votes by marking on the seal in front of the symbol of a candidate for which they wanted to cast their vote on the ballot paper. It was a very time-consuming process. The advantages of the Paper ballot system include no chance of hacking. Also, a paper ballot is still used internationally.The disadvantages include Paper Ballot is wastage of paper, time-consuming manual ballot counting, booth capturing by means of muscle power, methods of vote manipulation in ballot paper .

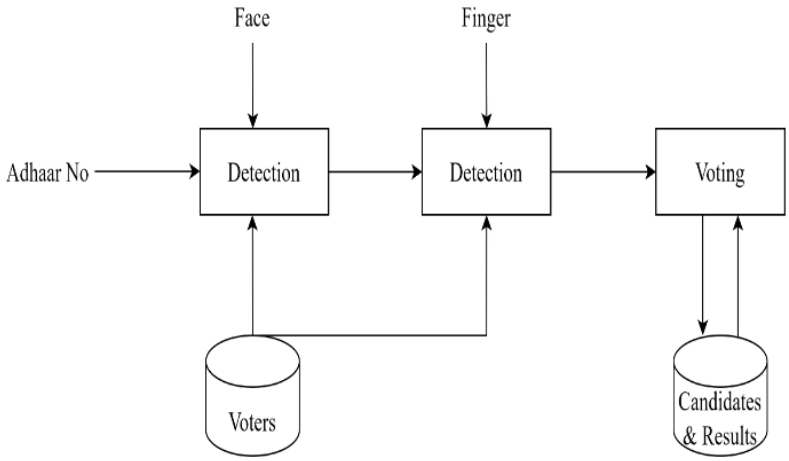
10. Electronic Voting System (EVM) : EVM is made up of two units- control unit and balloting unit, and these two are connected by a five-meter cable. These provide the voter with a button for each choice which is connected by a cable to an electronic ballot box. When a voter presses a button against the candidate he/she wishes to vote for, the machine locks itself. This EVM is a secure machine and can be opened by only one ballot number, which is unique. This feature of the EVM ensures that one voter only votes once , .EVM had a lot of advantages over the Paper Ballot System. According to an estimate, about 10,000 tons of ballot paper is saved due to the use of EVM machine in India. Also, the overall cost of the EVM machine is less as compared to the cost of printing ballot papers.As far as the disadvantages were concerned, EVM malfunctioning during the election process reported resulted in some inherent defects in a particular machine. Also, the EVM tampering is intentional and is not backed by any evidence so far of being possible

VI. SYSTEM DESIGN

Systems design is the process of defining the architecture, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development. The purpose of the system design process is to provide sufficient detailed data and information about the system and its system elements to enable the implementation consistent with architectural entities as defined in models and views of the system architecture.

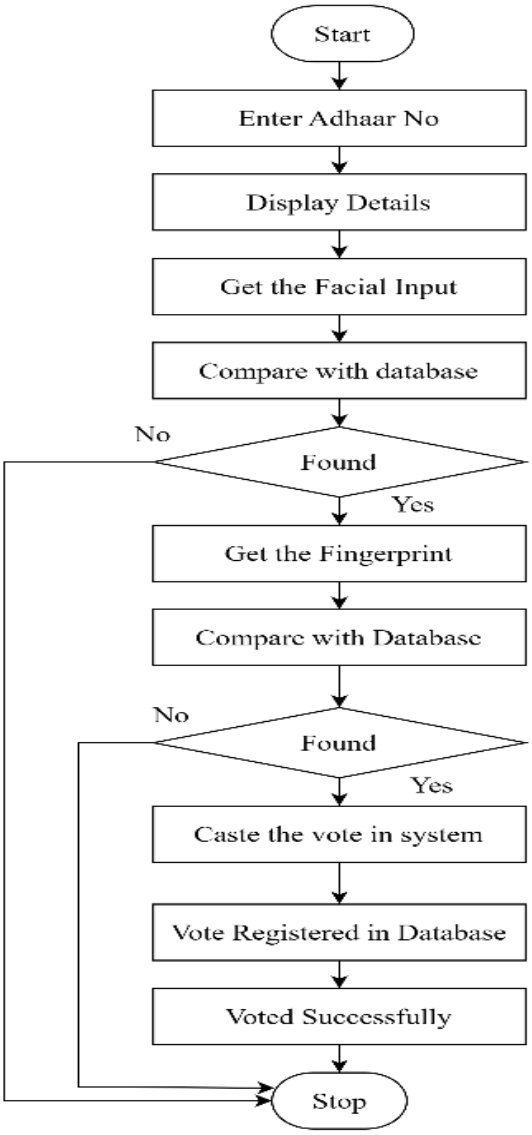
Architecture: The voting system utilizing facial recognition and fingerprint scanning for identification. Voters representing the participants, Face Detection and Finger Detection indicating the use of facial recognition and fingerprint scanning technologies for identity verification, Adhaar Number linking biometric data to unique identification numbers, and Candidates and Results handling the selection process and outcome of the election.

Biometric authentication, particularly through facial recognition and fingerprint scanning, holds the security of voting systems. By requiring individuals to undergo biometric verification, the likelihood of unauthorized voting or fraud can be reduced. These technologies offer unique identifiers that are difficult to replicate, enhancing the integrity of the voting process. Facial recognition analyzes distinct facial features, while fingerprint scanning relies on unique patterns, providing a dual-layered approach to authentication.



Architecture

Flow Chart: The voting system begins with the "Start" step, which initiates the process. The user is prompted to "Enter Aadhaar No," which is a unique identification number issued by the Indian government to its citizens. This step ensures that only authorized individuals can participate in the voting process. Once the Aadhaar number is entered, the system retrieves and "Displays Details" associated with that Aadhaar number from a database. This step helps verify the voter's identity and eligibility to vote. The next step is "Get the Facial Input," where the system captures the voter's facial image or video feed. This facial data is then "Compared with the database" to match it against the facial data stored in the system's database for the entered Aadhaar number. If a match is found, the process proceeds to the next step. If not, the system may prompt the user to try again or terminate the process. Assuming a successful facial recognition match, the system then prompts the user to "Get the Fingerprint." This biometric data is captured and "Compared with the Database" to verify the voter's identity further. Again, if the fingerprint matches the stored data, the process continues; otherwise, it may be terminated or require the user to try again. If both the facial recognition and fingerprint verification steps are successful, the system allows the user to "Cast the vote in the system." This step likely involves presenting the voter with the list of candidates or issues to vote on and recording their choice securely. Once the vote is cast, the system registers it in the database with a "Vote Registered in Database" confirmation. Finally, the process concludes with a "Voted Successfully" message, indicating that the user has successfully completed the voting process. The flowchart mentions that the system uses the LBPH (Local Binary Patterns Histograms) algorithm for facial recognition. This algorithm is a texture descriptor that analyzes the local binary patterns in an image and creates histograms to represent and compare facial images. It's worth noting that the use of biometric authentication methods like facial recognition and fingerprint verification aims to enhance the security and integrity of the voting process by ensuring that only authorized individuals can cast their votes and preventing potential voter impersonation or fraud.



Flow Chart

In this visionary electoral system, the fusion of Aadhaar identification and fingerprint verification creates a robust and secure voting process. By seamlessly integrating biometric data and voter information, it ensures authentic participation, guards against manipulation, and provides a transparent confirmation of each citizen's democratic contribution

VII SYSTEM IMPLEMENTATION

LBPH (Local Binary Pattern Histogram)

The LBP algorithm is a powerful method for extracting texture features from images, making it well-suited for tasks like facial recognition. The process begins by converting the input image to grayscale, where each pixel has a value ranging from 0 (black) to 255 (white). Instead of considering the entire image at once, the LBP algorithm examines small regions or neighborhoods around each pixel. A common approach is to use a 3x3 window, where the central pixel is compared to its eight neighboring pixels. For each neighboring pixel, a binary value (0 or 1) is assigned based on whether its intensity is greater or less than the central pixel's intensity. These binary values are then concatenated clockwise to form an 8-bit binary number, which is subsequently converted to a decimal value and assigned to the central pixel. This process is repeated for every pixel in the image, creating a new representation where each pixel's value encodes the texture information of its local neighborhood. This new representation, known as the LBP image, often provides better discrimination power for tasks like facial recognition compared to the original grayscale image. To perform facial recognition, the LBP image is divided into smaller regions or blocks, and a histogram is computed for each block, capturing the distribution of LBP values within that region. These histograms serve as feature descriptors, capturing the local texture characteristics of different parts of the face. The histograms from all blocks are then concatenated to form a single, high-dimensional feature vector representing the entire face. When comparing two face images, the feature vectors are compared using a distance metric, such as the Euclidean distance. If the distance between the feature vectors is below a certain

threshold, the faces are considered a match, indicating successful recognition. The strength of the LBP algorithm lies in its ability to capture fine-grained texture details while remaining computationally efficient and robust to variations in lighting and scale. By encoding the local texture patterns and comparing histogram features, the algorithm can effectively recognize faces despite variations in pose, expression, or other factors.

Face Database

The face database is created by taking the images from the video recorded using a webcam and then storing these images in the folder which is named as dataset which then consists of facial images of the person that are used for the face recognition.

Figure 5. Database Image

Each person or subject to recognize has 101 images in the database. So if there are 10 different person then 1010 image dataset can be there. So depending upon the no. of person there can be 101 images of each person.

Fingerprint Module

The Fingerprint Module is a versatile biometric device that connects directly to a computer's serial port, enabling seamless fingerprint recognition and authentication. It utilizes the MAX232IC chip to interface with the R305 Fingerprint Sensor, allowing it to be easily integrated with various controllers or microprocessors. This module is capable of capturing, storing, and comparing fingerprint data through its advanced matching algorithm, which compares the user's fingerprint against previously enrolled templates. Its applications span door access control, forensics, personal identification, attendance tracking, and more, leveraging biometrics for enhanced security.

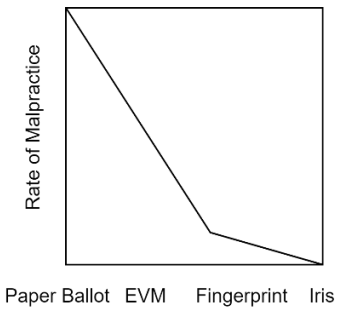
Figure 6 Fingerprint Module

At its core, the module features a powerful DSP processor that handles image processing, computation, feature extraction, and database searching. Its power consumption can be optimized by adjusting voltage, current draw, I/O mode, and clock rate. The module boasts onboard FLASH memory capable of storing up to 162 fingerprint templates, enabling seamless enrollment of new users. A red LED on the lens provides visual feedback during fingerprint capture. Additionally, the module comes with user-friendly Windows software for testing, enrollment, and fingerprint image viewing, streamlining the overall user experience.

VII. RESULT AND ANALYSIS

Fraud is easier with the traditional voting systems such as paper ballot and Electronic Voting Machines (EVM). The difference in accuracy rates between the traditional voting system and modern face recognition voting system is depicted in the given graph. Facial recognition-based voting system overcomes the problem of casting duplicate votes by using Machine Learning algorithm. The suggested technique will unquestionably safeguard voter identity and credentials while also enticing everyone to cast their vote for the

preferred candidate. Facial and Fingerprint biometrics provide several different advantages when used for identification and authentication such as accurate matching performance, it's possible to photograph it. In addition to maintain the number of votes, this technique will produce better and more accurate outcomes than the conventional voting procedure.



Rate of Malpractice

When the face and fingerprint are scanned, authentication is complete, and the user is locked into login, "Smart Voting" is utilized to identify persons who are attempting to vote a second time. The main objective of this research, face detection, is carried out utilising the Haar Cascade approach. In order to recognise things in an image or video, a Machine Learning object detection technique is used. Data related to the electoral process is captured, saved, and prepared digitally. Both casting ballots and tallying votes are done using an electronic voting system.

VIII. CONCLUSION

In conclusion, the smart voting system represents a significant advancement in electoral processes. Its streamlined approach simplifies and accelerates the voting experience by allowing citizens to cast their votes conveniently using Aadhar cards, reducing queues and wait times. A notable feature of the system is its robust security infrastructure, employing Aadhar biometric authentication to verify voter identities. This multi-layered security strategy, akin to having three locks on a door, effectively mitigates the risks of fraudulent activities such as impersonation or bogus voting, instilling confidence in the integrity of the electoral process. The smart voting system acts as a guardian for democratic principles, akin to a superhero equipped with a formidable shield. This shield, comprised of advanced security measures, protects the sanctity of votes and fosters trust among citizens. The heightened sense of security ensures that the system not only addresses current threats but also remains resilient against potential future challenges. In essence, the smart voting system signifies a transformative upgrade for democracy. It enhances accessibility, efficiency, and security, positioning itself as a beacon for the evolution of democratic practices. It is not merely a change but a comprehensive transformation that elevates the democratic experience, promoting inclusivity, transparency, and the enduring strength of democratic values.

REFERENCES

[1] S. Ganesh Prabhu, A. Nizarahammed., S. Prabu., S. Raghul., R. R. Thirrunavukkarasu and P. Jayarajan, "Smart Online Voting System," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2021, pp. 632-634, doi: 10.1109/ICACCS51430.2021.9441818.

[2] S. Agarwal, A. Haider, A. Jamwal, P. Dev and R. Chandel, "Biometric Based Secured Remote Electronic Voting System," 2020 7th International Conference on Smart Structures and Systems (ICSSS), Chennai, India, 2020, pp. 1-5, doi: 10.1109/ICSSS49621.2020.9202212.

[3] P. M. B. Mansingh, T. J. Titus and V. S. S. Devi, "A Secured Biometric Voting System Using RFID Linked with the Aadhar Database," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020, pp. 1116-1119, doi: 10.1109/ICACCS48705.2020.9074281.

[4] S. J. J. ARPUTHAMONI and A. G. SARAVANAN, "Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection on Image Processing and CNN," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 1-7, doi: 10.1109/ICICV50876.2021.9388405.

[5] K. Hasta, A. Date, A. Shrivastava, P. Jhade and S. N. Shelke, "Fingerprint Based Secured Voting," 2019 International Conference on Advances in Computing, Communication and Control (ICAC3), Mumbai, India, 2019, pp. 1-6, doi: 10.1109/ICAC347590.2019.9036777.

[6] A. BalaMurali; Potru Sarada Sravanthi; B. Rupa, "Smart and Secure Voting Machine using Biometrics" 2020 7th International Conference on Smart Structures and Systems (ICSSS), Chennai, India, 2020, pp. 1-5, doi: 10.1109/ICSSS49621.2020.9202212.

[7] M. Khan, S. Chakraborty, R. Astya and S. Khepra, "Face Detection and Recognition Using OpenCV," 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2019, pp. 116-119, doi: 10.1109/ICCCIS48478.2019.8974493.

[8] S. Shinde, M. Shende, J. Shah and H. Shelar, "An Approach for e-Voting using Face and Fingerprint Verification," 2020 IEEE Pune Section International Conference (PuneCon), Pune, India, 2020, pp. 59-64, doi: 10.1109/PuneCon50868.2020.9362470.

[9] N. Bhuvaneswary, C. V. Reddy, C. Aravind and K. H. Prasad, "Smart Voting Machine using Fingerprint Sensor and Face Recognition," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2022, pp. 1159-1166, doi: 10.1109/ICAAIC53929.2022.9792643.

[10] V. Lalitha, S. Samundeswari, R. Roobinee and L. S. Swetha, "Decentralized Online Voting System using Blockchain," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2022, pp. 1387-1391, doi: 10.1109/ICAAIC53929.2022.9792791.