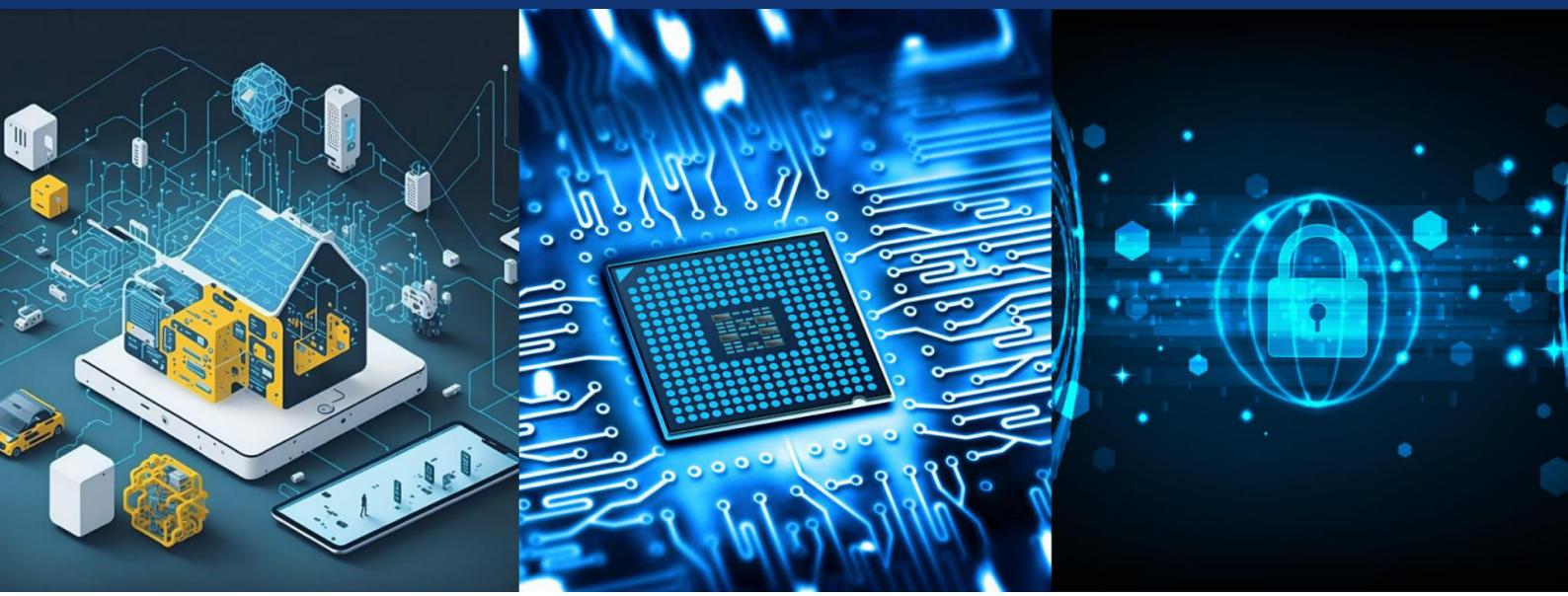
IJIRCCE

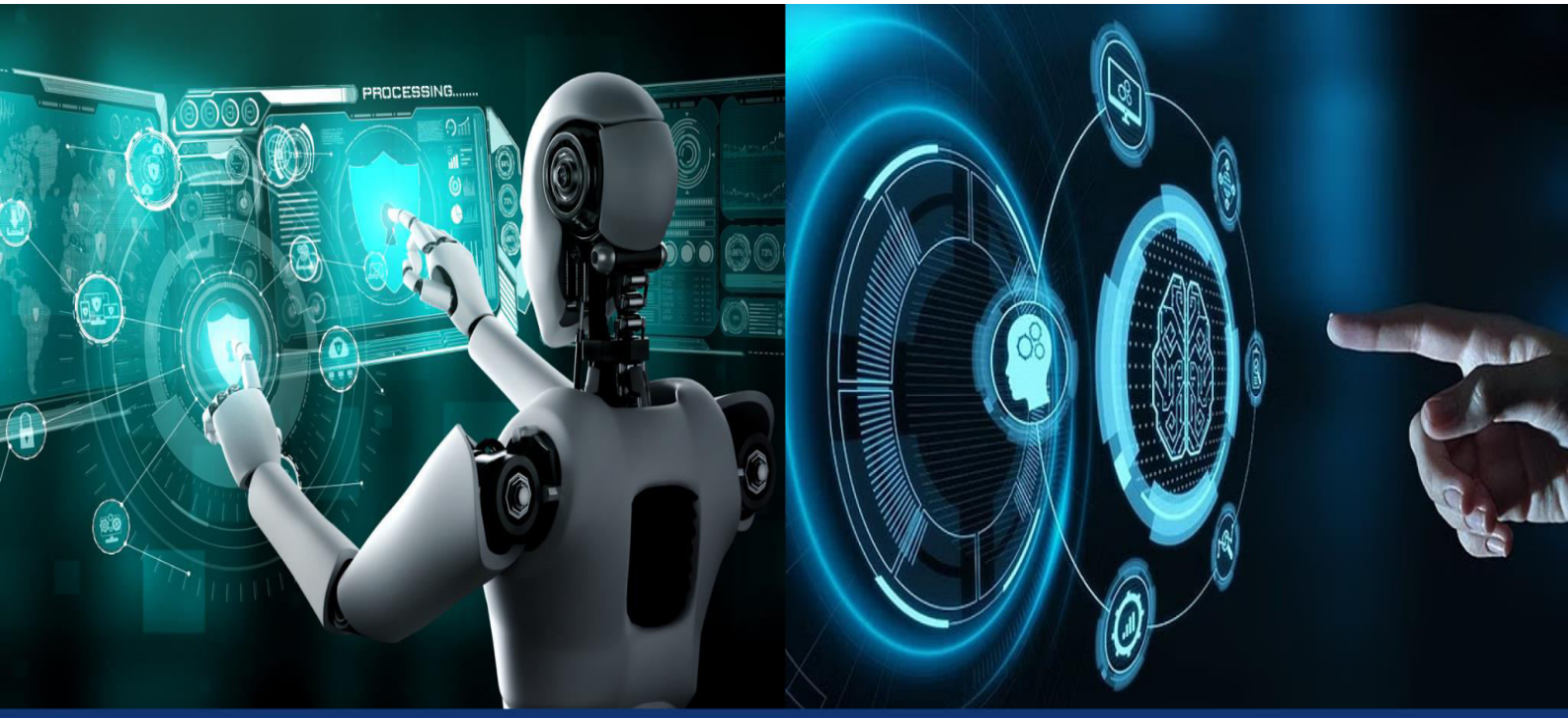
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 5, May 2025

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI: 10.15680/IJIRCCE.2025.1305019

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Smart Voting: Fingerprint Voting System with Biometric

Dr N G Goudru

Professor, Dept. of ISE, Sambhram Institute of Technology, Bangalore, India

Jayappa Jumanal, Deekshith S, Kasaram Karthik, Mohan Rao

Dept. of ISE, Sambhram Institute of Technology, Bangalore, India

ABSTRACT: A digital platform created to improve the security and precision of the voting process is an online voting system that uses facial recognition. To make sure that only eligible voters may cast ballots, the system uses facial recognition technology to confirm voters Object Detection using Haar feature- based cascade classifiers is an effective object detection method. Local Binary Pattern (LBP) is a simple yet very efficient texture operator which labels the pixels of an image. Then the server checks for the data from the database and compares that data which is already existing in database. If the data matches with the already stored information, the person is allowed to poll the vote. If not, a message is displayed on the screen and therefore the person is not allowed to poll the vote. Overall, an online voting system using face recognition technology has the potential to revolutionize the way we conduct elections, making the process more efficient, secure, and accessible for all.

KEYWORDS: Recognition, User Authentication.

I. INTRODUCTION

As per the records of TOI 24 Jan 2009 11 lakhs fake votes were observed in Delhi. Then according to India News June 2013: 30000 illegal voters were found in election commission under Sheila Dikshit constituency. Another news which was alleged by LJP.(Lok Jan shakti Party) Chief, Ram Vilas Paswan saying that Bihar election were having 30% fake voter- cards. Election involves both public or private vote which depends on the position. Local, state, and federal governments are some of the most important positions. In paper based on election, Voters cast their votes by simply depositing their ballots in sealed boxes distributed across the electoral circuits around given country. After ending of election period, the boxes which contains of ballot control unit are opened and votes are counted manually in presence of the certified officials appointed by election commission. So, it is a time-consuming process and requires a lot of resources to conduct voting process. In this paper we have proposed online voting system to cast the vote using fingerprint recognition. The information about the fingerprint is passed to the server unit for the further verification. Then the server checks for the data from the database and compares that data which is already existing in database. If the data matches with the already stored information, the person is allowed to poll the vote. If not, a message is displayed on the screen and therefore the person is not allowed to poll the vote. For voting representatives are appointed by electorates. In current scenario voter needs to show his/her voter ID card to cast the vote on the booth. So, this process is time consuming as the voter ID card needs to be get verified by the officials. Thus, to speed up the voting process and avoid such type of problems, we have proposed the new system.

Voting with Fingerprint Technology

Voting with fingerprint technology is a biometric authentication system that uses an individual's unique fingerprint to verify their identity and cast a vote. This method of voting aims to enhance security, streamline the voting process, and reduce fraud by ensuring that each person can vote only once. , Addresses key issues in traditional voting methods, such as voter fraud, inefficiency, and security vulnerabilities. By integrating biometric verification, the system ensures that each voter can cast only one vote, eliminating duplicate and unauthorized voting

Implementation Strategies

Pilot Projects: Small programs to solve technical or operational problems. Legal Frameworks: Crystallize laws regarding protecting biometric data and ensuring the ethical use of FVT in elections. Education Campaigns: The public should be appraised of how the technology works and address privacy-related concerns. Partnerships:

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Challenges and concerns

Privacy Risks: The collection and storage of biometric data raise concerns about data security and its misuse. Technological Bias: The FVT systems must broaden their accuracy across the broadest demographic groups to avoid disenfranchisement. Required Infrastructure: FVT will have infrastructure demands that will require large upfront investments in hardware, software, and personnel training. Public Confidence: The successful implementation of FVT systems for elections is tied to public confidence in their fairness and trustworthiness.

Global Case Studies

Estonia and India are moving toward the digital and biometric workings of their elections, and their experiences offer an exciting outlook on further technologies to be embraced.

Potential Impact on Democracy

Increase national turnout: FVT makes voting easier through a simplified and secure process. Transparency: Human error and manipulation have decreased in automated systems, making elections more transparent. Inclusivity: Remote voting capabilities will provide a fully participatory platform for the marginalized or differently abled.

Future Directions

- Blockchain integration: Overlapping FVT with blockchain technologies in voting for secure records.
- Multi-Factor Authentication: Addition of other verification layers such as fingerprint or iris scanning.
- Hybrid Voting Systems: Redefining processes by converging FRT with traditional methods to allow for inclusivity and redundancy.
- Continuous Upgradation: Updating algorithms from time to time to ensure minimal biasness and maximum operation over diverse population

II. FINGERPRINT VOTING SYSTEM TECHNOOLOGY

(FVT) means documentations used in voicing ideas to ensure safety, efficiency, and accessibility in voting. By algorithms identifying and verifying voters based on distinct facial features, FVT prevents fraud, for example, double voting and impersonation, to guarantee that only those eligible to vote should cast a vote. Implementation provides a broad range of advantages, from improving accuracy and transparency, speeding of verification, and cost saving by doing away with physical polling stations and manual verification. Other countries that have used biometric and digital technologies well in elections include India, Estonia, and South Korea with a clear indicative advantage and disadvantage on either end. Specific techniques of implementation shall be vital for streamlined work planned by the use of AI-based verification systems, encrypted data storage, and cloud attachment for quick processing. More challenges include cybersecurity threats, privacy concerns, technical failure, and the need for heavy investment in infrastructure and training. The way forward would involve pilot programs, solid legal frameworks, public awareness campaigns, and partnerships with technology and cybersecurity experts. Future directions include FVT integration with blockchain for secure voting records, Ulti- factor authentication for heightened security, and hybrid systems to ensure inclusiveness. After overcoming these hurdles promises to modernize the electoral processes and feel assurance regarding the integrity and public trust.

The incorporation of FVT into the voting process has a number of benefits, including an end to fraudulent activities, quick voter authentication, and voting accessibility for those who are physically challenged or live in remote regions. Global case studies of countries like Estonia, India, and South Korea show how biometric and digital technologies can play a role to improve the way that the election processes get conducted. In Estonia, for example, an online voting system with personal digital ID's is being used and has become a benchmark for e-governance. South Korea adapted AI- powered facial recognition to allow it to hold elections safely during the COVID-19 pandemic proving its adaptability to difficult circumstances.

Despite the promise that FRT holds, its implementation comes with a myriad of challenges such as privacy breaches, cybersecurity threats, biases introduced by the technology, and the most significant challenge, which is the required expenditure on infrastructure as well as employee training. These problems require a comprehensive law for biometric data protection, public education for trust building, and trial programs to work around possible operational challenges from within.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI: 10.15680/IJIRCCE.2025.1305019

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Further refinements may augment the utility of FVT in voting systems. The amalgamation of FVT with blockchain technology would result in secure and unalterable records of votes. In addition, multi-factor authentication that uses additional biometric data such as fingerprints and iris scans can provide an extra level of security. Traditional methods such as voting in person and using FVT systems can create hybrid voting technologies that can be useful for many unique populations and regions.

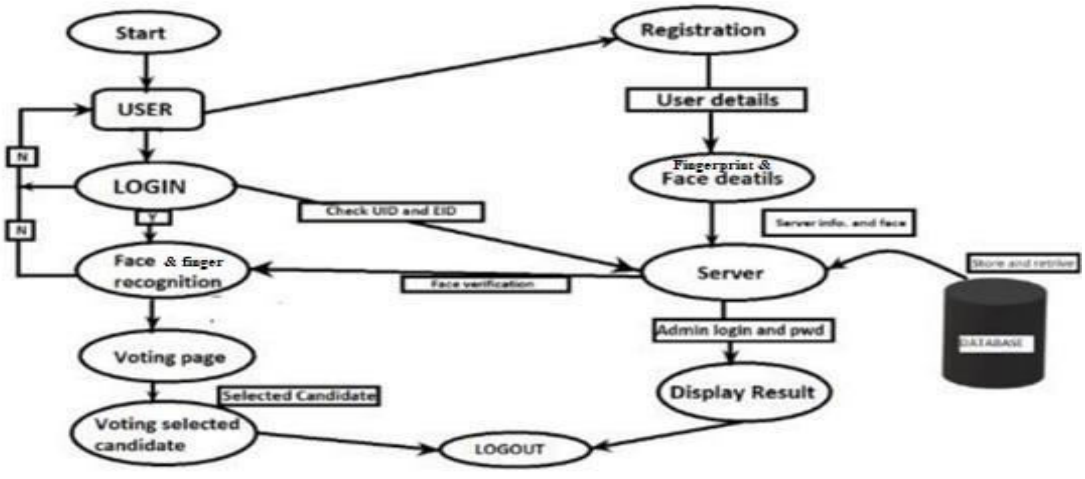
III. LITERATURE REVIEW

Challenges such as voter impersonation, ballot tampering, and logistical inefficiencies, compromising election integrity, have traditionally posed multiple challenges for voting systems. It has turned analysis to appreciate biometric technologies in voter authentication. The fingerprint recognition and iris recognition have come under review, but physical contact and specialized equipment are often a barrier to their extensive use.

With its ability to analyze unique facial features in real time and provide prompt voter authorization, while not requiring physical contact with anyone, facial recognition can, indeed, provide a non-invasive and scalable solution. With the advancements in AI and machine learning further improving the accuracy and reliability of facial recognition, their realization as tools of modernizing elections becomes brighter.

Real-time monitoring and analytics have been incorporated into election management, giving authorities insights into voter turnout and probable irregularities. This combination of facial recognition and real-time monitoring enhances election security by ensuring immediate identification of discrepancies and improving operational.

While the efficacy of facial recognition technology is unquestionable, concerns over privacy, as well as the regulations designed for data protection of voters, ought to be addressed in its implementation. Therefore, literature becomes favorable for adopting facial recognition as an enabler of election security, transparency, and efficiency.



Problem Statement

In traditional election frameworks, challenges such as voter impersonation, ballot tampering, and an inefficient manual verification process have been experienced. These vulnerabilities shake election integrity and erode public trust. The present modes of voter authentication, such as ID cards, are easily subjected to fraud; delayed counting of votes and non- real-time monitoring impede transparency and efficiency. As populations expand and elections become more complicated, these limitations need to be tackled with creativity. This project addresses

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI: 10.15680/IJIRCCE.2025.1305019

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

these challenges using facial recognition technology for real- time secure voter identification, hence enhancing election security, transparency, and trust.

IV. METHODOLOGY

A. Open CV

OpenCV-Python open-source library, which issued for computer vision in Artificial intelligence, Machine Learning, finger recognition, etc.

Object Detection using Haar feature-based cascade classifiers is an effective object detection method. It is a machine learning based approach where a cascade function trained from a lot of positive and negative images. It is then used to detect objects in other images. Each feature isa single value obtained by subtracting sum of pixels under the white rectangle from sum of pixels under the black rectangle.

1. Architecture

The architecture of the Smart Voting System using Finger Recognition is designed to ensure security, efficiency, and accuracy after, where voters can log in and take a selfie. They will be able to view the status at all times. A facial recognition module takes a photo of the real-time facial feature of the voter through a webcam. It establishes a comparative modeling of the Voter's portrait on the basis of a number of parameters extracted through deep learning algorithms with respect to this model and referenced against an encrypted face template stored in the voter's database. The authentication server verifies the voter ID and eligibility on the basis of comparing the facial portrait of the voter with the database. Once found, the voter will be given access to the memory module, wherein he will vote securely. This backend system will do all processing of data, the feature matching, and communication between the modules. This design of architecture ensures a diffusion and tamper-proof voting process with effective technology adopted to include security in polling.

A flow chart indicating a safe and precise way through the voting system based on face recognition. The process starts with the user activating at the registration stage. Such new users supply basic personal information and face data, which is then safely recorded in the database for future reference or authentication by other users.Voting requires the user to log in with a User ID (UID), which he provide to the system for validation against the database. If UID is valid, then the user is subjected to face identification, which acts as a second measure to confirm his identity.

If face verification fails, the system ,
denies access, ensuring only authorized users can proceed further.Having verified the identity, they go to the next phase, which is voting-the process of choosing the desired candidate. The information about the candidate who will be voted for is quietly recorded and stored in the database for integrity's sake. After voting, the user can log off.It also encompasses an admin login option for the concerned authorized administrator to access the database to obtain and display results. This guarantees an efficient result management and transparency.The database is a fundamental part of the system that ensures secured storage and of the user details, face data, and voting records. The other advanced technologies implanted include face recognition. This provides strongholds for security, keeping unauthorized sources at bay and reducing fraudulent acts for the voting process, respectively.

2. Implementation

A Smart Voting System with Finger Recognition involves developing multiple modules in tackling various tasks, such as user registration, finger recognition, vote casting, and result generation. Below is an overview of the key components and their implementation details.

- OpenCV: For image capture, finger detection, and preprocessing.
- TensorFlow/Keras: For facial recognition model training and inference.
- MySQL/PostgreSQL: For storing user, candidate, and vote data.
- Flask/Django: For the backend of the web interface.
- HTML/CSS/JavaScript: For building the frontend interface.
- Python Libraries: NumPy, Pandas, and Matplotlib for data handling and visualization.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI: 10.15680/IJIRCCE.2025.1305019

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

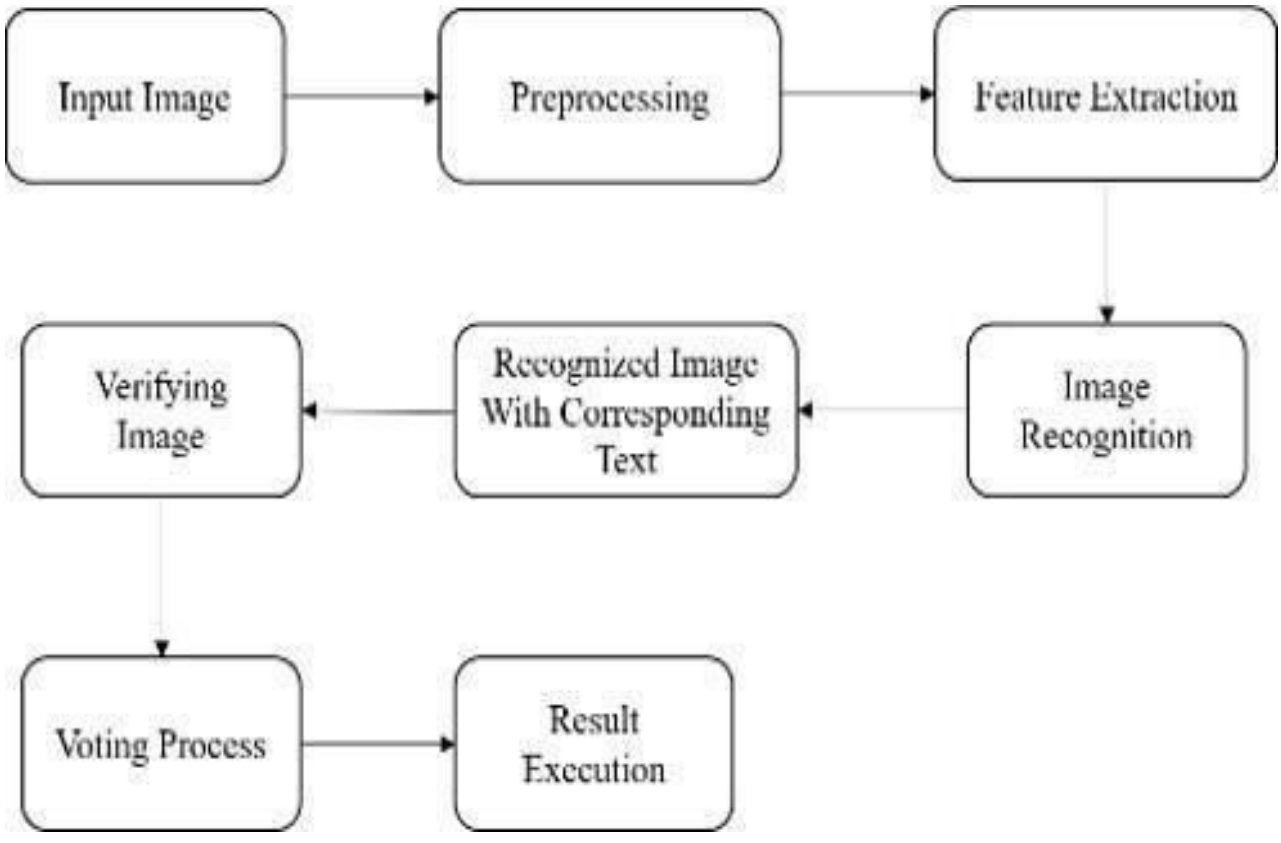
International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

python code

```
 import cv2
import numpy as np
from keras.models import load_model

# Load pre-trained FingerNet model
 model = load_model('facenet_model.h5')

def capture_finger(user_id):
            capture = cv2.VideoCapture(0)
             ret, frame = capture.read()
            # Preprocess the captured frame (resize and normalize)
             finger = preprocess_finger(frame)
               # Extract facial features embedding = model.predict(face)


            # Store face embedding and user info in the database
             store_user_data(user_id, embedding)

              capture. Release ()
```

The implementation of an image recognition-based voting system involves several key steps that ensure both security and efficiency. First, the system captures an input image of the user, typically a face image, using a camera or webcam. The image is then pre-processed to improve quality by removing noise, resizing, or adjusting contrast. Next, feature extraction occurs, where distinct characteristics, such as finger landmarks, are identified using tools like OpenCV or deep learning models like FaceNet. The system then compares the extracted features with stored data in a database to identify the user.



© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI: 10.15680/IJIRCCE.2025.1305019

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. RESULTS

Initially, user needs to register in the system by providing information such as Aadhaar number, Mobile number, City, Age, Password etc. This information is stored in voter dataset. The system takes input image from the user at the time of registration through webcam. This image is stored in face dataset for template matching. Then for casting the vote, user needs to login to the system by entering Aadhaar number and Password. We must have a very good quality camera to get the efficient detection and recognition. It will capture the video. The video into converts the multiple frames. It will helpful for more accurate to produce the results. Facialrecognition is a way of identifying or confirming an individual's identity using their face. Facial recognition systems can be used to identify people in photos, videos, or in real-time. Facial recognition is a category of biometric security.It indicates periods of excessive water usage, which may be a c o n c e r n for efficiency or resource management.

VI. CONCLUSION

Further expanding on the potential of this system, the image recognition-based voting framework is not only atechnological advancement but also a significant step toward improving the inclusivity and accessibility of elections. The application of face recognition through use of a camera is very simple and needs no complicated settings or devices to be brought into use for electoral purposes. This would, in short, fill in the gap where physical voting stations are minimal or arise due to inconveniences, or other technographic hurdles are being encountered.

Other than improving security, the system can also be scripted to provide a legally compliant and regulatory acceptable model guaranteeing it meets all standards in electoral integrity. This facilities its usefulness for other elections, national, local, or organizational, as well as its integration with the well- established digital platforms for a wider audience. Only communication between a user's device and the keystone server, as between each voter, would be.encrypted. Further voter data, protected and in communicator, garners trust in the entire electoral process

Greater scalability is another prime attribute of the model. From the management of a small community election to an immense national referendum, it can match any demands that arise from elections large or small. The extensibility of the platform means that future integration of additional biometric modalities or alternative authentication systems can only serve to strengthen security.

As a contemporary system solution, this solution possesses another crucial benefit: the rapid recognition that cybersecurity and the significance of data protection standards would inspire the adoption of similar systems, thus moving other domains beyond e-voting towards more secured platforms, like online banking, e-commerce, and other governmental service needs. These days, it seems, the digital world is witnessing a gradual change with the elections heading that way; hence, the face recognition basis of this system in itself models for other platforms that reflect security, are smooth, and offer transparency in their operations.

This system brings together biometric security, transparency through real-time data processing, and user compliance into a progressive solution that meets the contemporary challenges in electoral systems while pushing forward the needs of a future restructured alternative in an electronic world.

With the foundation of the highly secure and efficient framework formed, the latest technologies in image recognition of inputs appear set to revolutionize the election by bringing cutting-edge technologies into the time-honoured practice of voting. Face recognition technology forms the basis of the entire system, reducing human error and eliminating the possibility of voter impersonation, providing a foolproof means of verification. With the help of the aforementioned processes of preprocessing and feature extraction, both even of low quality photographic images, the system will contribute to efficient testing in actual operation by granting it various settings capabilities. The database on a central level aids in storing vote records and user profiles. Its retrieval remains highly secure and easy to access.

It further provides a friendly user experience: the voter can cast his ballot without setting up complicated processes. You can conduct quick audits and monitor the status of the election; hence, making things transparent for the election officials and the voters. The results can be evaluated quickly and accurately. Also, there is a facility for management results and real-time vote tallies from an admin interface, causing a significant reduction in time taken to declare results and adding less probability of discrepancies.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The adoption of such technologies not only meets modern-day security measures but also reduces the costs incurred by paper- based voting systems since elections drive their platforms towards further digitization. This face recognition-based voting system would emerge as a notable evolution in electoral technology, ensuring election conduct integrity, improving voter confidence, and providing solid means to live election results.

REFERENCES

1. Research Papers and Articles:
2. Naseer Abdulkarim Jaber Al-Habeeb, Dr. Nicolae Goga,, Haider Abdullah Ali1, Sarmad Monadel Sabree Al-Gayar "A New E-voting System for COVID-19 Special Situation in Iraq", The 8th IEEE International Conference on E-Health and Bioengineering – EHB, 2020.
3. Roopak T M, Dr. R Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology", Proceedings of the Second International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020), pp. 71-75, 2020.
4. Ganesh Prabhu S, et.al., "Smart Online Voting System", 7th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 632-634, 2021.
5. Robert Kofler, Robert Krimmer, Alexander Prosser, "Electronic Voting: Algorithmic and Implementation Issues", Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03), 2003.
6. Books
7. Awsan A. H. Othman, et.al. "Online Voting System Based on IoT and Ethereum Blockchain", International Conference of Technology, Science and Administration (ICTSA), 2021.
8. Frameworks and Libraries:
9. OpenCV – OpenCV Documentation
10. Coding language =Python
11. operating system =window XP

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details