Smart Voting System with Biometric Authentication using Raspberry pi

Vegesna Ananda Sita Raghu Rama Teja
M.Tech, Department of Computer Science and Engineering
B CH S N L S Sai Baba
Assistant Professor, Department of Computer Science and Engineering
Email: raghuvegesna22@gmail.com

ABSTRACT: Democracy is the political system in which voters vote for their leaders. The nation risks falling into the wrong hands if illegal operations are not disrupted. The government has taken many steps to guarantee a risk-free voting procedure. However, the process of verification remains unguarded. Time-consuming tabulation, unreliable proxy voting, and a lack of safeguards are all problems that have been addressed in this project. Using RFID cards and biometric technologies like fingerprint and face identification provides three separate levels of security. The fingerprint samples are collected from the system once the RFID card has been validated. Facial recognition technology, which uses photographs of voters to verify their identities, increases security. Voter fraud, including proxy voting and influence from rival parties, may be prevented on Election Day by using this secure verification mechanism.
RFID Cards, Biometric Identification

1. INTRODUCTION

Voting is a means through which voters pick their government and political representatives and make their opinions known on a wide range of issues, legislation, citizen initiatives, constitutional changes, and recalls. There is a growing use of technology to aid voters. Voter identification is required both when registering to vote and while casting a ballot. This is done to confirm that voters are who they say they are (authentication). There have been several current and ancient fingerprint discoveries on artifacts. This finding has contributed significantly to the development of fingerprinting and identifying methods. In 1788, the underlying anatomy of fingerprints was first described. In the early nineteenth century, Sir Francis Galton developed analytical processes for comparing fingerprints, and by the early twentieth century, fingerprints had been classified into nine unique categories. The need to identify criminals by a unique physical trait arose as the criminal justice system got more intricate. In 1901, Richard Edward Henry of Scotland Yard was the first to use fingerprinting, and its success led to its widespread use. A rapidly expanding field, biometrics was formerly limited to only one kind of bodily identification but has now expanded to include a wide variety of methods. Even Nevertheless, fingerprints are still the biometric technique of choice for law enforcement and are utilized in numerous contexts for identification purposes. Fingerprint scanners have been developed in response to these theories of human identification in order to efficiently and immediately verify an individual's identity before granting them any desired privileges. The basic idea behind these technologies is the same as that of fingerprint scanners; it uses a database of fingerprints to identify a person.

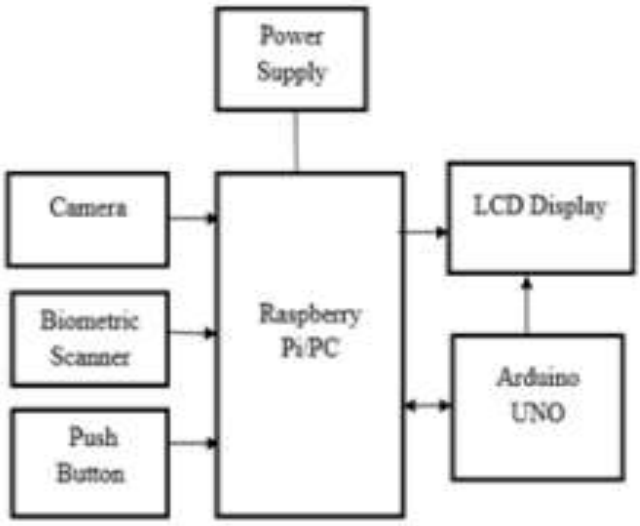

Fig.1: Example figure

A Voting Protocol that prevents voter fraud and privacy invasion is crucial to the success of any electronic voting system. Soon to be developed and implemented, the e-VOTE system's voting protocol will combine the finest parts of current voting processes with new ideas and innovations meant to address their main flaws. The e-VOTE system will fully support the following features, and it will be tested and verified to ensure that it meets all of the requirements. The study found that if an electronic voting system met these requirements, it would have a good chance of earning the trust of both voters and process organizers.

For the system to be considered "democratic," it must ensure that only qualified voters may cast votes and that each voter casts a single ballot (un-reusability). The voting method should make it hard for anybody participating in the process (election officials, party members, other voters, etc.) to link a particular ballot with a specific voter, or for a voter to establish that he or she voted a certain way, in order to safeguard voters' privacy (Un traceability).

No one's vote should be able to be tampered with or duplicated under any circumstances, thus it's important to take steps to prevent these issues (unchangeability). By design, the system will prevent anybody from manipulating the final total by erasing a legal vote or adding an illegitimate one. The system should allow for and promote checks to ensure the accuracy of the final tally of votes. The voting process should be quick and easy enough that voters may complete their votes in one sitting without needing any extra training or equipment.

2. LITERATURE REVIEW

Biometrics Based Secured Remote Electronic Voting System:

The people of India have the power to elect their own government officials, which is fundamental to the concept of democracy itself. However, several issues, such as booth capture, rigging, fraudulent voting, interference with the Electronic Voting Machines (EVMs), etc., have arisen in recent years that threaten the integrity of the electoral process. We have an obligation to society as responsible engineers to take action to stop this threat. Electronic voting machines

(EVMs) are becoming popular because they allow voters to cast their ballots without the need for time-consuming and sometimes inaccurate paper ballots. Authenticity of the voter is a major issue nowadays, and it must be prevented that the same person votes again. Biometric voting systems, which use factors such as a voter's fingerprints to verify their identity, are one solution to this problem. Therefore, the rule will be that each legitimate voter shall have one vote. The current endeavor involves the development of a prototype biometric voting system that uses fingerprint scanning technology. It is recommended that the Unique Identification Authority of India (UIDAI), Government of India (GoI), New Delhi's Aadhaar database be integrated. This will make it possible for all eligible voters to enroll in the system without any human intervention, and for their biometric data to be automatically sorted into regional and parliamentary constituency categories. The technology created in this study may then be used in elections all around the country, expanding its scope to the national level. This will ultimately make a major improvement to the democratic process in India.

A Safe Biometric Voting System Based on Radio Frequency Identification Data Backed by the Aadhar Registry:

The Internet of Things (IoT) is a relatively new technology that allows for the seamless movement of data between computers, smartphones, and other electronic devices, software, sensors, cars, and household appliances. Due to the lack of up-to-date security measures, phony voters may cast multiple duplicate or fake votes in the current system, which is a major concern with electronic voting machines. Therefore, RFID and IoT (Internet of Things) are included into the system's implementation to enhance the safety measures. Here, an active RFID tag is substituted for voter id; the system scans the tag and compares the data to fingerprints stored in the Aadhar database. After scanning the RFID tag, the voter must verify their identity by providing a fingerprint scan. This voting system utilizes a finger print scanner and an active reading device (reader) to read information from RFID tags. Votes are counted only if the fingerprints submitted match those in the database; otherwise, an alert is triggered to prevent votes from being counted again. Since no two people have the same fingerprints, using an LCD to show the voter's matching data from the database helps prevent fraudulent voting and impersonation. By integrating the voting procedure with the Aadhar database, the technology provides the highest levels of safety and efficiency. Also, the voter database's registered phone numbers get the preset data.

Biometric facial and fingerprint detection image processing for online smart voting:

Despite being a democratic nation, India still uses expensive and time-consuming voting machines to conduct its elections. Because the voting mechanism is hosted online, voters may participate from any location. The Indian government has blocked access to the website at a certain IP address for voting purposes. People should fill out a website registration form with their name and address. Voters' fingerprints and facial images will be collected by the election commission. The pictures will be saved on the server or database. On Election Day, when photos are collected, they will be matched to a database, ensuring safe and secure voting. Voting machines will soon be able to be unlocked using a combination of your face and fingerprint, much like a modern smartphone. Many voters find it bothersome that they must be present at the polls in order to cast their ballots. Time savings are another benefit of this method. The number

of fraudulent votes may be lowered by the use of face and fingerprint image detection. It is a security feature that the space between the eyes and eyebrows does not change with aging. In order to accurately identify a voter's name, this study uses a dataset of 10 print images.

Contactless Fingerprint Minutiae Extraction and Pose-Invariant Matching: Towards Improved Accuracy

There has been a rise in interest in contactless fingerprint identification installations because of the benefits it provides to users in terms of ease and cleanliness. However, it is difficult to maintain a consistent position when presenting fingers to the contactless fingerprint sensors, which may dramatically reduce the accuracy of fingerprint matching. This research presents a more accurate method of minutiae extraction and pose-compensation to overcome these issues and increase the quality of fingerprint matching. Instead of using picture augmentation, which may introduce artifacts, our deep neural network–based solution is resistant to misleading details. Our network's extracted details are put through a three-stage pose compensation framework consisting of: a) view angle estimation based on the location of core point; b) ellipsoid model formulation which simulates and compensates finger pose; and c) intersection area estimation and alignment between different view angles. For use with 2D contactless fingerprint images, the authors offer an ellipsoid model that can adjust to the shape of the fingerprint's outline and the user's predicted viewing angle. To align two contactless fingerprints for high-quality matching, this model may be used to hypothetically estimate the area corresponding to the varied view angles. This research presents replicable experimental findings utilizing public datasets and a database gathered for this work that demonstrate the superiority of the proposed framework over both commercial software and previous methodologies.

Liveness Detection of Fingerprints using an Enhanced Convolutional Neural Network and Image Scale Equalization:

Fingerprint identification methods are often susceptible to fakes because of the absence of pre-judgment of fingerprints. It is possible for anonymous individuals to impersonate authorized users in order to accomplish different authentication activities, which may cause serious disruptions to daily operations and significant economic losses for a community. Therefore, fingerprint liveness detection (FLD) has been used as a potential anti-spoofing solution to guarantee that legitimate users' fingerprint data is not misused. The deep convolutional neural network (DCNN) can learn the high-level semantic information automatically using a supervised learning algorithm with little to no human intervention or expertise, making it a superior alternative to hand-crafted feature approaches. One drawback of most CNNs models is the need for input pictures to have a fixed scale (e.g., 227 x 227). Cropping and scaling processes, which turn an image of any size into a fixed scale, solve the scale issue, but they often result in the loss of important textural information and a drop in picture quality, which reduces the classifier's ability to generalize. In this work, we present a unique FLD technique, an enhanced deep convolutional neural network with image scale equalization, to keep texture details and original resolution when scaling images. Moreover, this work employs an approach that allows for a variable learning rate. The confusion matrix is introduced as a new performance metric for use in FLD assessment. The detection performance of our technique is better than other methods, as

shown by the quantities of the experimental findings based on the LivDet 2011 and LivDet 2013 data sets.

3. METHODOLOGY

We still use picture IDs given by the government as our primary means of voter verification in India, but the poll worker manning each location has the final say on whether or not a voter is allowed to cast a ballot. This leaves the door open for imposters to cast votes. Since 70-80% of voting booths in an Indian election use moderate balloting, this scheme's major drawback is that voters who aren't in their home cities may be unable to cast ballots.

There are several approaches to the verification process. Biometric authentication provides the utmost security when compared to other techniques. However, none of these biometrics are used in active systems at the moment. This method cannot provide security. Also, these tactics have not been implemented adequately.

Limitations of the Current Method:
Why One candidate may illegally cast the votes of all or a large number of voters on the electoral list, which is a major problem with the existing system.

There will be no way for anybody, not even the government, to identify who voted for whom.

The EVM's factory-installed programs are upgradable (security problems).

• There is also the problem of accessibility. If the poll is available to all voters from the start to the finish, the system will operate as designed.

Internal Rigging removal is a primary goal of the proposed project.

This setup uses a Raspberry Pi for its biometric fingerprint verification. Here, we employ fingerprint scanning to check an individual's voting history before letting them cast a ballot.

in support of the Proposed Strategy
Nothing Can Be Rigged Internally
The potential applicants will be unveiled after a biometric check.

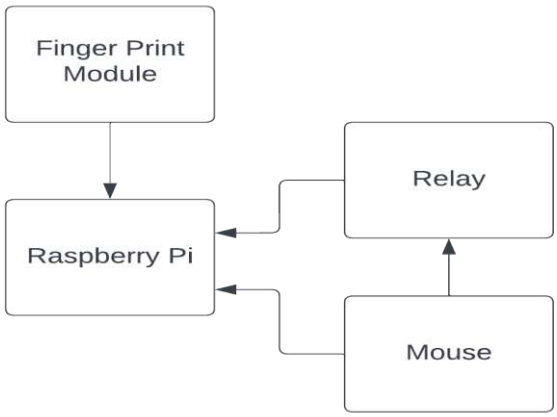

Fig.2: Block diagram

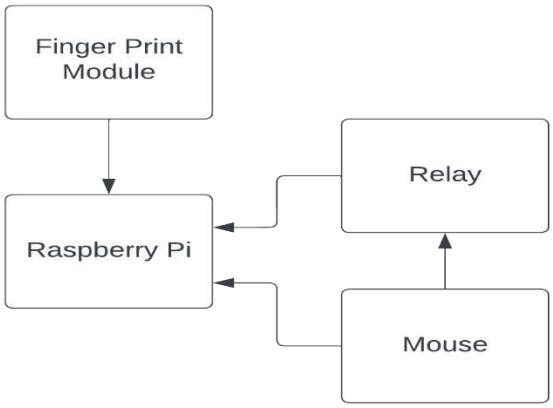

Fig.3: Circuit diagram

4. IMPLEMENTATION

Biometric authentication has quickly become the preferred method of verification for users who are unable to or do not choose to use a traditional password for various reasons. The goal of this project is to increase voter turnout by making election procedures faster and more secure. This project uses an RFID reader, an LCD, and an Arduino to implement a biometric voting system, with the former two components serving to prevent voter fraud by ensuring that only those whose fingerprints match those on file are permitted to cast ballots. A person's face print may be captured by the system when they stand near the Pi camera, and the information can then be checked against a database. Voting is denied to anybody whose information is not found in the voter rolls. The company often makes a decision in less than 5 seconds.

A vote is a way for voters to have their voices heard and make a choice or show support for a certain candidate. The administrative authorities used to utilize voting machines to decrease the possibility of mistakes or manipulations and to keep the administrative expenses of elections under control. The new feature of this gadget is biometric protection to be done to be discovered by the fingerprints of the voters, and this is decided by the digital voting tool that is used in this

project. One of the least expensive ways to establish one's notoriety is via one's fingerprints, thus it seems sense that this biometric would be ideal for developers to exploit. The government has also taken important initiatives, such issuing the Aadhaar card, to help make this a reality. For this project, we're building on a digital voting system that already exists to eliminate voter fraud in public elections by using two forms of ID. Biometric methods of identification, such as fingerprint scanning and face recognition Both fingerprint- and face-based authentication are completed by feature extraction based on a definitive machine learning set of criteria.

5. EXPERIMENTAL RESULTS

Despite the fact that most fingerprint recognition scanners are based on the same hardware standards, other components and software can play a significant role in determining how fast and how accurately they can identify fingerprints. Specifically, different manufacturers use different algorithms to discover key fingerprint traits. Comparison of the minutiae minimizes the amount of processing power needed to find the fingerprint, helps to prevent forgeries in cases when the scanned fingerprint is dirty, and even enables the finger to be positioned off center without invalidating the scan.

Fig.4: Fingerprint

There are two primary phases to the process.

Checking eligibility and enrolling are two separate processes.

During registration, the user's data may be scanned, processed, and saved in the database in the form of code.

Anyone wishing to enter must first be verified by placing a finger on a fingerprint reader. The scanner picks up the fingerprint and compares it to all of the prints saved in the database during enrollment to determine whether the person is eligible for benefit access. Up to 40,000 fingerprints may be authenticated or disputed each second using these methods.

Operation:

• Voters' fingerprints and photos will be uploaded to a Raspberry Pi. The SD card will be used to record this data.

First, a picture of the individual will be captured using a tiny camera module.
It will have a wire running to the face recognition sensor.
After that, a fingerprint scanner is used to capture the person's fingerprints.
Once that happens, we'll begin the checking process.
If all requirements are met, then the voter is officially registered.

• If he fails any of the exams, he still won't be able to cast a ballot.
• His account will be deactivated when he has cast all of his votes.

He cannot use his ID to cast an unlimited ballot.
Counted votes are added after the voting process has been completed successfully.
• These procedures will be shown on the LED screen linked to the raspberry pi.

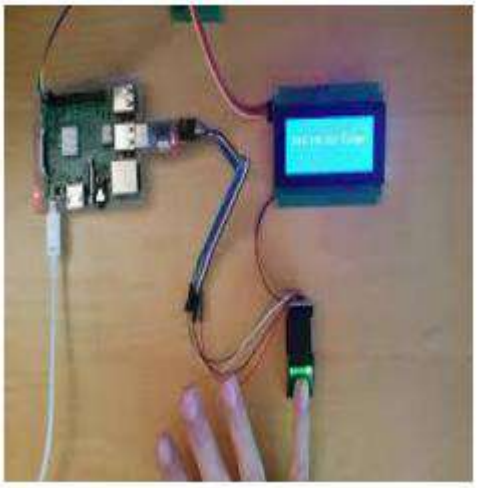

Fig.5: Biometric Authentication using Raspberry pi

6. CONCLUSION

The suggested method involves developing a secure voting system predicated on biometrics in an effort to address all issues with the existing system. There is a multitude of merits to the suggested method that make it sound. With this system, all a voter needs to vote from home is a scanner and access to the internet. In order to prevent voters from casting multiple votes, face patterns will be linked to Voter Cards. If a voter tries to cast a ballot more than once using the same Fp card, the system will reject the latter ballot since it does not match the person's face and fingerprint patterns in the database. This model satisfies all of these requirements: it is democratic, private, reliable, precise, and simple to implement. Taking this tack may help get more individuals of all ages to the polls in the future elections.

REFERENCES

[1] Samarth Agarwal, Afreen Haider, “Biometrics Based Secured Remote Electronic Voting System”. IEEE Conference, Sep 2020.
[2] P.M.Benson Mansingh, T. Joby Titus, “Biometric voting system using RFID Linked with the Aadhar database” IEEE Journal, august 2020.

[3] S Jehovah Jireh Arputhamoni,Gnana Saravanan "Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection Image Processing "IEEE Conference,May 2021.
[4] Suresh Kumar, Tamil Selvan G M, "Block chain Based Secure Voting System Using Lot", IEEE Journal, Jan 2020.
[5] Hanzhuo Tan, Ajay Kumar, "Towards More Accurate Contactless Fingerprint Minutiae Extraction and Pose-Invariant Matching" IEEE Conference 2020.
[6] Chandra KeerthiPothina, AtlaInduReddy"Smart Voting System using Facial Detection"IEEE Journal, April 2020.
[7] Chengsheng, Yuan, Zhihua, Xia, "Fingerprint Liveness Detection using an improved CNN with image Scale Equalization" IEEE Journal 2019.
[8] Anurag Chowdhury, Simon Kirchgasser, Andreas Uhl, Arun Ross "CNN Automatically Learn the Significance Of Minutiae Points for Fingerprint Matching?"IEEE Conference, Mar 2020.