SMART ELECTRONIC VOTING MACHINE USING RASPBERRY PI

[1]Mrs. Spoorthi S P, [2]Mr. Abdul Azeem, [3]Mr Arjun HN, [4]Mr. Gowrish R, [5]Mr. Karthik L

[1]Assistant Professor, [2,3,4,5]UG Students
Department of ECE
Atria Institute of Technology
Bengaluru – Karnataka, India.

Abstract: **The main aspect of democracy of a nation is the VOTE by which people elect their favorite candidate to rule the nation. Intervention of illegal practices will lead the nation to wrong hands. There are several methods adopted by the government to avoid crimes during voting. But the untouched area without proper security is the verification process. All the problem like time delay for vote counting, security, proxy voting can be overcome through this project. The main idea behind this is to provide three levels of security using RFID card and biometric techniques such as Fingerprint face recognition.The fingerprint samples are extracted from stored database after the verification of RFID card. For giving additional security face recognition technique is added which captures an image of the voter and matches with the stored in the database. This secured verification process prevents proxies, political party intervention and other crime activities during the Election Day.**

Keywords: **Raspberry pi, RFID, Fingerprint module,Open CV Algorithm**

1. INTRODUCTION

The democracy of any nation lies in VOTE the people cast to elect their leaders. But this system despite high security is still suffering from various issues mainly during verification process and the manpower requirement during that process is large. There are chances of intervention of political parties and human errors in this process but yet there are no best solutions to overcome this problem. If this problem is not overcome then it might lead the nation into wrong hands. The security and manpower requirement during the verification process can be overcome by the method used in this paper.Throughout the history different methods and techniques of voting have been adopted. The design parameters of voting system should be chosen in such a way that all concerned parties acting as candidates as well as voters that are polling the votes must be satisfied with the announcement of results after elections have been conducted. Environment of voting and conducting elections basically depends upon the cultural values as well as political policies.

2. Literature review

A. Iris Detection in Voting System The image of eyes are captured and further the Iris is detected by using the image processing technique and compared with the stored images. Once it matches, the system confirms the voter to be the eligible individual to vote by checking his/her Aadhar details. Once confirmed the voter will be allowed to cast the vote. As the existing Aadhar database contains all the information about voter's Iris, fingerprints and other details like address, blood-group voter can be easily tracked and checked. This approach requires less manpower and highly secure,

B. Voting System using Fingerprint Recognition .Fingerprint is Recognition using sensor and save in database .Once the biometric image is read and the information will be sent to the web application through the microcontroller's serial port. Input image is compared with the existing image in the database or server sends the message and displays it on the LCD confirming the voter's identity. If not Matching, it displays the same as not eligible through LCD.

C. Smart Voting Information of individuals above age 18 will be taken from the Aadhar database. In the first phase, the voters will be given an Id and password through the registered email Id before the voting process. The second phase is validating the voter using fingerprints data and once confirmed voter will be allowed to cast the vote. After casting, as a part of the third phase, the voter id will be deleted leaving no second chance to vote again. Aadhar details that were used by the voter will be locked to track the voter for further access. The count will be updated parallel.

D. Blockchain Based Secure Voting System using lot. The voting process is record in client and it is stored in the Server. Registered the name and address of voter in the Website and Lot is given to voter at the time of voting process. Fingerprint image is taken by using sensor and fingerprint image is compared with database images. When it match with input voter will allow to vote. Block chain means blocks of voting recorded for each voter and stored in the server.

E. Multimodal Biometrics based on CNN the Multimodal Biometrics recent method having the secure of face, iris and palmprint images. The features extraction of images done using Convolutional Neural Networks. The multimodal Biometrics is old method using CNN. The input image is compared with images in database using CNN .The matching of fingerprint images are also done by CNN. Two layer fusions is used in the recent CNN.

3. EXISTING SYSTEM

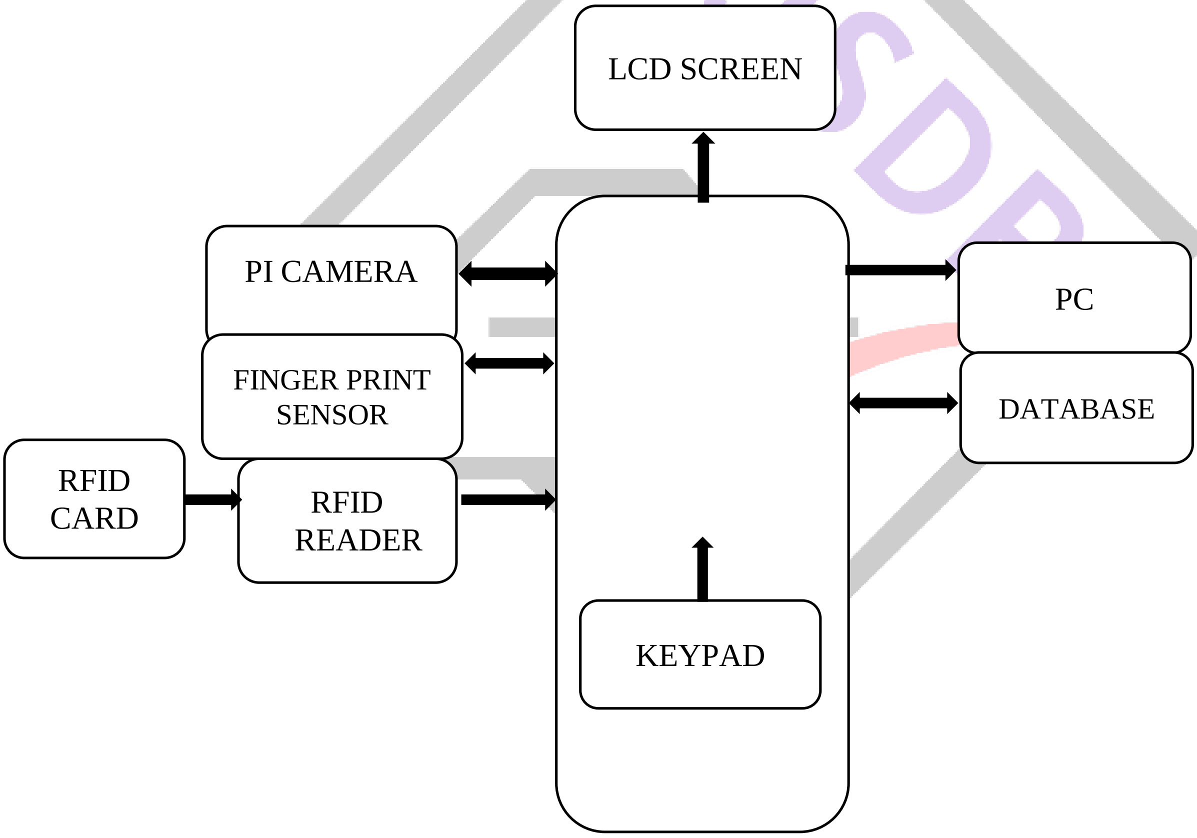
There are several methods available to carry out verification process. Out of several processes biometric verification is the most secured process. But in the existing systems only either of the biometrics are used. The security cannot be ensured in these processes. Also these methods have not been implemented successfully.

4. PROPOSED SYSTEM

The voter ID card is replaced with a RFID card which serves as an access to the individual on the day of voting. During the day of voting the voter undergoes a three step verification process. The first step is one in wherein the voter has to show his RFID card and it is read by a RFID reader module. The reader module senses the card and displays the details of the individual on the LCD screen. Once after the details are displayed the voter is asked to place his/her registered finger on the fingerprint sensor. The sensor module verifies the fingerprint with the existing database and permits the user to next level of verification process if the details matches else the LCD displays “wrong user”. Once after the fingerprint matches, the camera turns on for the face recognition and captures the image of the person and matches it with the existing database. If the images also matches then the door of ballot booth opens for the voter to cast his vote and the votes are simultaneously on the monitor. Thus this process provides a much secured three level verification process and the illegal practices during the day of voting are also avoided.

5. METHODOLOGY

The proposed system is based on electronic voting machine with different levels of security. In first level the system is able to identify each voter by their RFID cards. Secondly it uses biometric fingerprint, whenever the system receives a fingerprint, it will match the fingerprint from the database. After the verification of fingerprint, it will go to third level of authentication by using face recognition. If the image of the voter is matched with the stored database it will allow the voter to vote. We have also given option for voter to select their constituency and vote to their respective candidates. Touchscreens will be used instead of push buttons in voting machines but for demo purpose we use PC to cast the vote. Figure shows the block diagram of our proposed block diagram.



5.1 Raspberry Pi 3

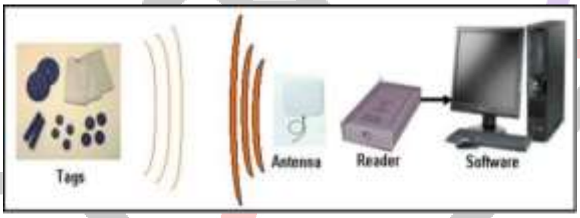
Raspberry pi 3 model B is the earliest model of third- generation raspberry pi. It is a 1.2GHZ Broadcom BCM2837 64 bit CPU. It has four USB 2 ports and CSI camera port for connecting a raspberry pi camera. A micro SD port is available for loading OS and for storing data. These features make this pi 3 to be one of the efficient controllers. The image processing is done with the help of this controller as image has to be in a high clarity. The ATMEGA 329p is also interfaced to this processor. Also pi enables the capturing and verifying the captured image very quickly than other processors. Pi has the ability to work as normal computer. The language which is used in Pi is python.

5.2 Finger print sensor

The Fingerprint scanner module used in this project is R305. The device is able to capture fingerprint, save it and match fingerprint with the database. The module has 4 external wires, two of them which communicate with the Raspberry pi. Other two wires are biasing voltage and ground. We use fingerprint sensor as the second level of authentication. Only after the verification of fingerprint, the third authentication method i.e face recognition is carried out.

5.3 RFID Card and Reader

Radio Frequency Identification (RFID) is a wireless identification technology that uses electromagnetic fields of radio frequency range to identify RFID tags. It is used for identification of people, object etc. The RFID tag contains a radio antenna mounted on a substrate which carries 12 bytes unique identification number. The reader module is used to read unique ID from tags. Whenever the RFID tags comes into range, the reader reads its unique ID and transmits it serially to the microcontroller. Data can be read or write from the cards because they consists of EEPROM. In the same way in this system the voter ID card which is modified as RFID card is contains personal details of the individual stored in it. Once the reader reads the tags, the details are displayed on the LCD.



5.3 LCD

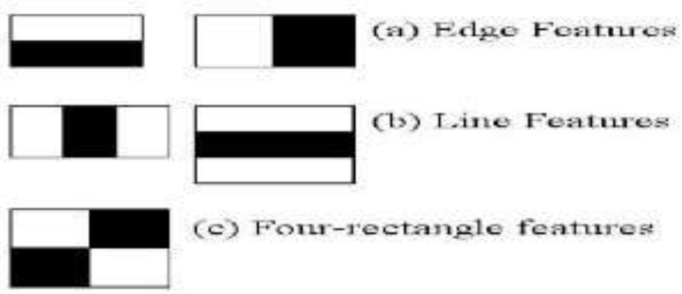
A liquid crystal display is a flat panel display or other electronically modulated optical device that uses the light modulating properties of liquid crystals combined with polarizers Liquid Crystal Display technology works by blocking of light. They do not emit light directly but instead uses a backlight or reflector to produce images in a monocular. This project uses the LCD display to establish the details of an individual and producing a confirmation message.

5.5 FACE DETECTION USING HAAR CASCADE

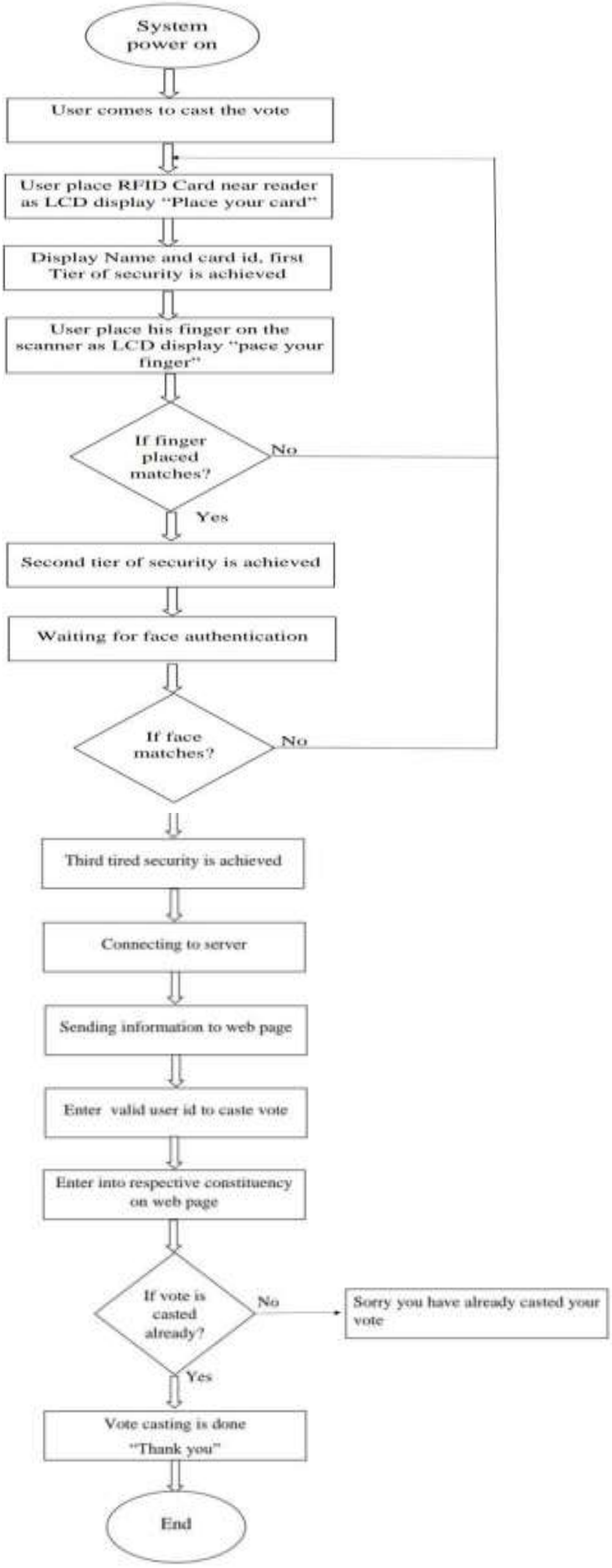
Face detection, object detection algorithm used to identify objects in an image or video. The algorithm is trained to detect a face by Haar features-sequence of square-shaped functions. Then it uses classifiers to detect the face and not a face . This face detection happens in four stages. The first being, detection of Haar features, using integral images, third stage is Adaboost and fourth is the cascade of classifiers.

Haar Cascade detection in Open CV:

Open CV comes with a trainer as well as a detector. It contains many pre trained classifiers for eyes, face, smileetc. First we need to load the required XML classifiers and then load our input image in grayscale mode. If the faces are found it returns the position of detected faces as rectangle. Once we get the location we can create a ROI for face and eye detection. There are three different processes carried out during face recognition. First the image of the person is captured which uses a dataset program running at the background. Once the program is executed the camera captures image of a person in all possible directions by creating a rectangular block around the face. The captured images are used to train the classifier for face recognition process to be completed. During face recognition phase the, a separate program runs to compare the original face in the classifier and the captured face. The use age of cascade classifier enables to produce effective face recognition and detection.



6. FLOW CHART


System power on
User comes to cast the vote
User place RFID Card near reader as LCD display "Place your card"
Display Name and card id, first Tier of security is achieved
User place his finger on the scanner as LCD display "pace your finger"
If finger placed matches?
No
Yes
Second tier of security is achieved
Waiting for face authentication
If face matches?
No
Third tired security is achieved
Connecting to server
Sending information to web page
Enter valid user id to caste vote
Enter into respective constituency on web page
If vote is casted already?
No
Sorry you have already casted your vote
Yes
Vote casting is done "Thank you"
End

shows the detailed flowchart of our project, below is the brief procedure of the voting process. Voter place the RFID card on the reader, If it is valid card the voters information like Name and ID are displayed in LCD else it will display a message telling that card is not valid. For 2nd level of authentication the voters fingerprint are scanned and is matched with the stored database. Then for the third level of security the voters face is recognized using Open CV algorithm. After completion of three levels of security the voter is allowed to cast his vote through a website which appears on the screen. Finally the voter can cast his vote to their respective constituencies If a person tries to vote for the second time an error message will be displayed on the screen telling that the voter has already registered his voter.

7. Conclusions

The proposed method is to develop a secure voting system based on biometrics which tried to overcome all the drawback occurs in traditional or current voting system. The proposed system has many strong features like correctness, verifiability, convenience etc. For this system no requirement of an election officer, paper ballot or any electronic voting machine only the internet connection and Face scanners are required one can vote from anywhere securely. In this system no voter can vote twice because the voters Facial pattern will be linked to their Card. If any user tries to vote twice with some other person's RFID card, it will lead to a mismatch in the respective facial and finger Patterns stored in database storage which results in an error. This model satisfies the democracy, anonymity (privacy), reliability, accuracy and usability criterion. This model shows potential to re- engage all demographic age groups to participate in elections and cast their votes.

8. Future Work

The performance of EVM can be increased by using Iris recognition. Confirmation messages can be sent to respective voter after casting their vote.

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.