Remote Voting System with On-line Biometric Authentication

PRATISH CHOUDHARY[1], SHRIPAD V. DESHPANDE[1]
[1]Electronics and Telecommunication Engg Department, Symbiosis Institute of Technology,
Symbiosis International (Deemed) University, Pune

Abstract — **Free and Fair election forms foundation of any healthy democracy. Voting by large percentage of genuine citizens of the country is the basis for this to happen. We propose a system by which a genuine voter will be able to vote in the election irrespective of his/her current location. This system employs biometric identifiers for ensuring authenticity of the voter. Pre-collected biometric details of all the voters in the country are maintained in a central database by the government. At the time of voting, the biometric data collected from the voter is on-line validated in real time with the central database to ensure the identity of voter. Usage of Raspberry-Pi for web casting of the complete voting process and periodic display of detailed polling statistics tremendously improves the credibility of the process. Transparency and minimum usage of personnel is achieved with reduced cost and simpler process.**

***Keywords*— Fingerprint detection/ recognition system, *Face detection/Recognition* MySQL, Database, Server.**

I. INTRODUCTION

Elections are a transformative tool for democratic governance. They are the means through which people voice their preferences and choose their representatives. Elections are unique. They change the fate of nations, influence participation and activism in politics, and deeply affect the lives and attitudes of citizens. Society deems the voting process so important that it must be 100 percent reliable.

Each vote is part of a larger process that stretches before, during and after an election: The Electoral Cycle. At present in most of the countries, election processes comprise of paper ballot system/ digital recording electronic systems/even online voting system

Nowadays, election process plays a very important role in democratic country. The election is a process for selection of a perfect candidate who will lead the nation. In a democracy, people choose their leader by giving their vote. Recently in India, electronic voting system is used. In this system, voter is able to cast his/her vote only in the city where the voter is registered. Due to some reasons on the day of voting if the person is away from his/her native place then he/she is deprived of voting. This is major drawback of electronic voting system. An online voting system is the solution as voter can vote from anywhere.

To improve the efficiency and accuracy of voting process, we can use this online voting system. With this system the direct visible benefit is increase in voting percentage. The system uses internet to cast the vote and transmit it.

To design a system, which will provide smart way of voting and will prevent proxy votes, some important objectives are set as follows –

1. To improve polling percentage.
2. To minimize the human resources and hence help reducing malpractices in the process
3. To recognize fake voter and stop him/her from casting vote.
4. To make it possible for a voter to vote from anywhere in the country.
5. To make more efficient voting systemby making the process fast and transparent.

II. SYSTEM DESCRIPTION

The block diagram of the system is shown in the Fig. 1.

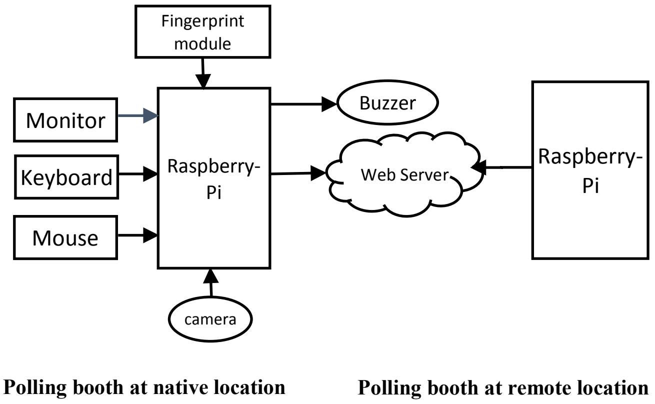


Fig. 1. Block Diagram

The Fingerprint module, a Camera, Monitor, Keypad, Mouse and Buzzer, are interfaced to the Raspberry-Pi.

One of the most important part of the voting process is biometric authentication of voter before voter casts his/her vote. The process starts with face authentication. When the voter enters the polling booth his/her photograph is captured on camera and sent to the central government database. If the face is validated, then he/she will be asked for biometric authentication in the form of fingerprint. Immediately after taking the fingerprint scan from the voter using fingerprint scanning machine, it is processed and sent to the central database that is maintained by government.

The database maintained by government comprises of list of voters, corresponding voter details regarding the native where their voting rights are registered and their fingerprint data. All the data in this database is confidential hence for security reasons, this database is not distributed and maintained at central location. The system checks for a match with fingerprint information in this database and if match is not found it may be because of some error, so the voter will be provided an alternative method of authentication. If a match is found, the database returns a unique ID of the voter corresponding to that fingerprint.

The value will be returned to the database that is maintained in local polling booth. This database which is stored in Raspberry Pi device consists of two tables, one with electoral list named as ELECTORAL DATABASE and the other with the list of names who already casted their votes named as CASTED DATABASE. Raspberry Pi itself after taking the value from the central database will search for the unique ID in the electoral database. Search will tell whether the ID is found in the electoral database or not.

If found in database, the voter's name with details will be displayed on the monitor and he/she will be allowed to cast the vote.

This will complete the voting process. There can be two cases when the match is not found. One may be due to voter already voted and other may be due to the voter belonging to other polling station. Considering the situation, the casted table is searched for the voter's ID. And if the ID is found in the casted table, it implies that the voter had already casted his/her vote. So, he/she should not be allowed to cast the vote again.

If the voter's ID is not found in any of the tables i.e. in electoral table and casted table, then a request to find the identification of the voter will be sent to district database, which will return the details of the polling station where he/she has voting right. This completes the voting process of a single person. If it could not return any match, it indicates that the particular voter is not eligible to vote, and controller will not allow him/her to cast vote. Same process is applicable to all other voters who are willing to cast their vote. After voting process voting data will be saved on a web server as well as at the Remote location. The voting details of Native location will be displayed appropriately on the monitor.

Database Management:

Database is for storing critical identification related data of voters. "Central database" maintains details of all the voters residing in the country. The data comprises of particular voter's unique ID to identify, personal details, photographs and most importantly biometric details of the voter. These details are in general not shared with any other organization and so these are maintained on additional servers with stringent security. This data is used for matching of the voters' details at the time of verification process. Apart from this database, at each polling station and district or zone level, a "local database" is maintained which gives the voter's unique ID and personal details only for reference.

This local database need not contain any confidential information like biometrics. These are the two main databases from which we collect information and the prime authentication factor to decide whether the voter is eligible to vote or not.

For reference, the local database is divided into two tables **1. Electoral table 2. Casted table**.

After each ballot, these tables are updated so that voted person details are moved from electoral table to casted table. This table is maintained by Raspberry Pi I. At Raspberry Pi II which is used at RVM, a **Ballot table** is maintained to count and update the casted votes for the respective candidates.

ALGORITHM

A: Algorithm for Verification of Voter in RVS

1. The process of voting starts with face authentication. When the voter enters the polling booth he/she will be asked for face authentication. After taking the image of face, immediately Raspberry-Pi will check whether the person is authorized or not with Image processing.
2. If the face is of authorized person, then raspberry-Pi will check biometric authentication which is a fingerprint scan. In case face doesn't match, then the Raspberry-Pi display a string "Unauthorized person".
3. Immediately after taking the template fingerprint from the voter using fingerprint machine, it is processed and sent to a database that is maintained by government.
4. The database maintained by government comprises of list of voters, corresponding voter details regarding polling and their fingerprint data. For the sake of security, this database is not distributed and kept very confidential.
5. There it checks for a match and if the fingerprint match is not found in the database that may be because of any error, the voter will be provided with an alternative method. If the match is found, the database returns a unique ID of the voter corresponding to that fingerprint.
6. The value will be returned to the database that is maintained in local polling booth. This database, which is stored in Raspberry Pi device, consists two tables, one with electoral list named as ELECTORAL DATABASE and the other with the list of names who already casted their votes named as CASTED DATABASE.
7. Raspberry Pi itself after taking the value from the central database will search for the unique ID in the electoral database. Search will tell whether the ID is found in the electoral database or not.
8. If found in database, the voter name with their details will be displayed on the monitor and he/she will be allowed to cast their vote. This will complete the voting process.
9. There can be two occasions when the match is not found. One may be due to voter already voted and

other may be due to the voter belonging to other polling station.

10. Considering the situation, the casted table is searched for the voter's ID. And if the ID is found in the casted table, it implies that the voter had already casted his/her vote. The voter is a fraud.

The voter's ID if not found in any of the tables i.e. in electoral table and casted table, then a request to find the identification of the voter will be sent to district database.

Finally, it will return the details of the voter to which polling station he/she belongs to. This completes the voting process of a single person.

If it could not return any match, it indicates that the particular voter is not eligible to vote, and controller refuses his identity.

Same process is applicable to all other voters who are willing to cast their vote.

B: Algorithm for RVS Working

1. After successful biometric authentication, valid voter comes to cast his vote in RVM. Now, Control Manager gives initialization signal by pressing the control switch of RVM. Control switch should be in adequate distance from RVM to ensure privacy of voter while voting.
2. On Initialization of RVM, GPIO pins of Raspberry Pi [17], [18] gets activated to input mode.
3. In RVM, all the GPIO pins are connected to buttons present in line with all the contestants. In input mode, GPIO pins wait for any button to be pressed to receive input.
4. Voter casts his vote in RVM by pressing the button corresponding to the contestant name of his choice.
5. As soon as the voter presses any button, vote count of that contestant should be increased and updated in the database.

This process can be explained as a separate sub process as follows:

(1) In input mode, GPIO pins are all set to low level logic (0 Volts).

(2) When voter presses any button, GPIO pin connected to

(3) Corresponding button will be raised to high level logic (5 Volts) due to switching action of button.

(4) Now, only one GPIO pin is in high level logic. Rest of the pins are in low level logic.

(5) GPIO pin giving the value '1' (high level logic) is determined by Raspberry Pi with the help of coding.

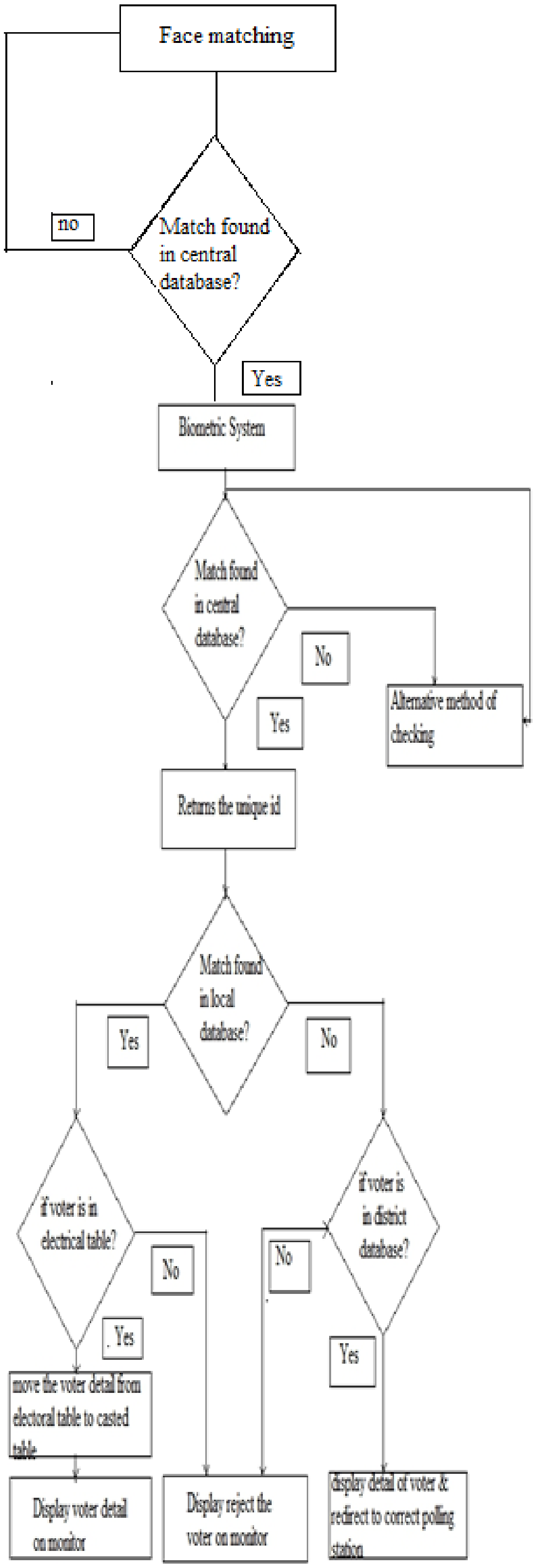
(6) Corresponding contestant name is also identified by using this pin number, using input dictionary which consists of matching pin number with contestant name.

(7) After a voter casts his vote once, GPIO pins are deactivated. Even if voter tries to cast another vote, it won't be valid.

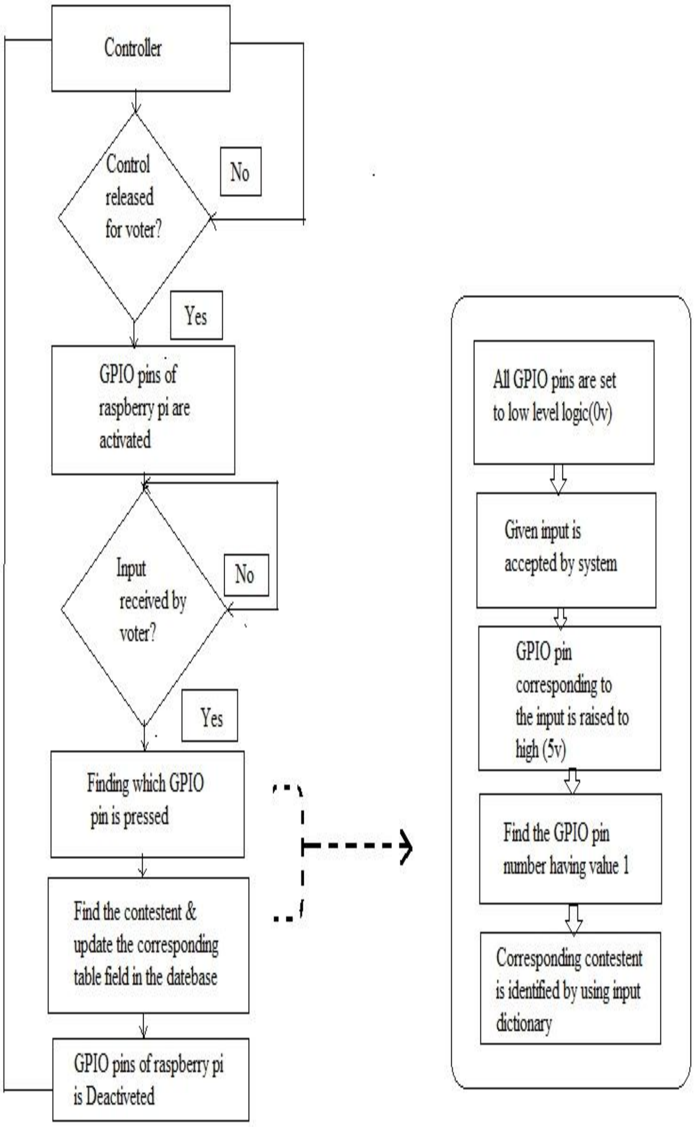
(8) Deactivated GPIO pins are again activated only by initialization of RVM by Control Manager.

(9) Control manager gives initialization when next valid voter comes from biometric check only and this process continues repeatedly till voting process terminates.

III. FLOWCHART


Face matching
no
Match found in central database?
Yes
Biometric System
Match found in central database?
No
Yes
Alternative method of checking
Returns the unique id
Match found in local database?
Yes
No
if voter is in electrical table?
No
Yes
move the voter detail from electoral table to casted table
Display voter detail on monitor
Display reject the voter on monitor
No
if voter is in district database?
Yes
display detail of voter & redirect to correct polling station

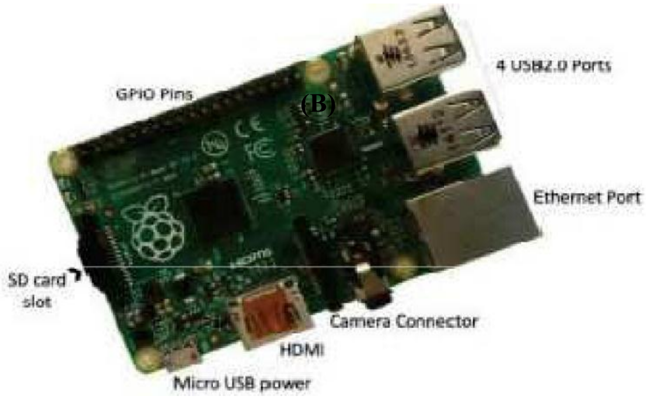
(A)


Controller
Control released for voter?
No
Yes
GPIO pins of raspberry pi are activated
Input received by voter?
No
Yes
Finding which GPIO pin is pressed
Find the contestent & update the corresponding table field in the datebase
GPIO pins of raspberry pi is Deactiveted
All GPIO pins are set to low level logic(0v)
Given input is accepted by system
GPIO pin corresponding to the input is raised to high (5v)
Find the GPIO pin number having value 1
Corresponding contestent is identified by using input dictionary

(B)

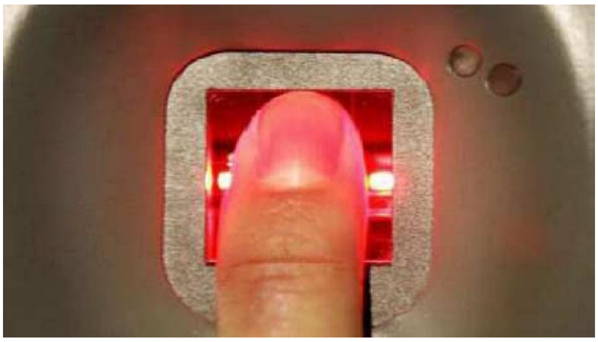
IV. HARDWARE

RASPBERRY PI:



Pi is a credit card sized single board computer. This board is cost effective when compared to an actual computer. This board contains many features like camera connector, Ethernet port, GPIO pins for interfacing sensors and switches, USB ports to connect to external devices (like keyboard, mouse, Wi- Fi adapter etc.,), HDMI port to interface to monitors (like LCD screens, projectors, TVs etc.) and an audio jack also available. limited to single use, it can be of wide use according to the application. Using Raspberry Pi multiple programs can be run at a time. Raspberry Pi board comes in three models A, B, B+. Raspberry Pi B+ model is used in this system. This model supports Linux based operating systems like Raspbian, Pidora, and Raspbmc etc. Latest model Raspberry Pi2 is released with 1GB RAM and it is going to support Windows10 operating system as well.

FINGERPRINT MODULE:



A **fingerprint** is used to narrow sense is an impression left by the friction ridges of a human finger. Optical fingerprint imaging involves capturing a digital image of the print using visible light rays. In this type of sensor is essence in a specialized digital camera. Where top layer of the sensor is used to place the finger, which is known as the touch surface. Down of this layer is a light emitting phosphor layer which illuminates the surface of the finger. Then the light is reflected from the finger passes through the phosphor layer to an array of solid state pixels which captures a visual image of the fingerprint which is used for authentication. But a scratched or dirty touch surface can cause a bad image of the fingerprint.

CAMERA:

Camera is directly connected on Raspberry-Pi board and it is used for taking image of voter and send it for recognition and compare with government Database.

V. ADVANTAGES

- Voters can cast their votes from anywhere
- Improving the polling percentage
- More efficient
- Human Resources are reduced
- Recognize and avoid fake voting

VI. APPLICATIONS

- Electronics voting machine
- Access control
- Attendance system
- Medical Field

VII. FUTURE SCOPE

- We can use IRIS scanner to make more secure
- We can create app for showing a voting percentage to everyone.

VIII. CONCLUSION

The Raspberry Pi Voting System is designed with a motto to improve reliability, efficiency and transparency in election process. Considering the problems of already existing system, this system is developed in such a way to overcome them. With the implementation of this system in election process, surprising results can be obtained. It follows a simple procedure, consumes minimal man power, can save a lot of time, less prone to frauds and manipulations compared to already existing systems. We aimed at extending this system to an advanced model in future in such a way to maximize the polling percentage. The people who work in distant places from home towns are the ones who may not use their right to vote. If these people cast their vote that can drastically change the result. We thought of designing this system so that any voter can utilize his/her vote from any workplace.

IX. REFERENCES

[1] Chaum D., “Secret-ballot receipts: True voter-v erifiable elections”, IEEE Security and Privacy, 2(1):38-47, 2004.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Ashok Kumar D., Ummal Sariba Begum T., “A Novel design of Electronic Voting System Using Fingerprint”, International Journal of Innovative Technology & Creative Engineering (ISSN:2045-8711), Vol.1,No.1. pp: 12 19, January 2011. R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[3] Tigran Antonyan, Seda Davtyan, Sotirios Kentros, Aggelos Kiayias, Laurent Michel, Nicolas Nicolaou, Alexander Russell, and Alexander A. Shvartsman, “State-Wide Elections, Optical Scan Voting Systems, and the Pursuit of Integrity”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Vol.4, NO.4, pp. 597-610, Dec,2009

[4] Ye Wang, Member, IEEE, Shantanu Rane, Member, IEEE, Stark C. Draper, Member, IEEE, and Prakash Ishwar, Senior Member, IEEE, “A Theoretical Analysis of Authentication, Privacy and Reusability Across Secure Biometric Systems”, IEEE Transactions on Information Forensics and Security; Vol 8, No. 6, pp 1825-1840, Dec 2012

[5] J. Bannet, D. W. Price, A. Rudys, J. Singer, and D. S. Wallach, “Hack-avote: Security issues with electron ic voting systems,” IEEE Security Privacy, vol. 2, no. 1, pp. 32–37, Jan./Feb. 2004.