Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 3955 - 3965
Received 15 April 2021; Accepted 05 May 2021.

A Secure Biometric Voting System Linked with Fingerprint Database

B.Nataraj, K.R.Prabha, R.S.Mukesh, R.G.Nitin Sarvesh, R.Vineeth and G.Vishnu Deva
Department of Electronics and Communication Engineering, Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu, India
nataraj.b@srec.ac.in

ABSTRACT

The Embedded Systems and Internet of Things (IoT) has contributed for major advancement in interconnecting electronic devices and other appliances without any human intervention and also transferring of data is done at ease. One of the major problems faced in dense populated countries which are not given much consideration is the voting method. The current problem faced in the electronic voting system is that they do not have any electronically voter verification method to cast their respective votes. This may lead to casting of fake votes which will cause unnecessary problems in the elections. Thus the proposed system is implemented with the help of fingerprint verification of the voter. The voter has to verify his identity by placing his finger in the fingerprint sensor. The fingerprint data is verified with the help of the data stored in Aadhaar database. Only if the fingerprint matches the voting machine is enabled and allowed to cast his vote. The voters who are allowed to vote is also stored in a database which can be later verified while counting the votes to remove the fake votes casted. If the fingerprint does not match, a buzzer alert is given and also the identity of the person is verified physically by checking the Aadhaar and other identity details to confirm his identity, if the person also fails in this process thy person is not allowed to vote thereby reducing the chance of casting fake votes. A LCD is also interfaced to display the necessary commands and the data. Thus the proposed system offers maximum security and efficiency.

Keywords
SQL Database, Raspberry Pi, Biometrics, Fingerprint Verification

Introduction

The constitution of every country is decided by the vote of every individual who are associated with the country. The process of selecting the party to rule is done in the method called voting. This process plays a very important role in deciding the situation of the country until the ruling party comes to an end. The current voting system is done with the help of Electronic Voting Machine (EVM). This microcontroller device is used to cast and count the votes during the elections. This voting system comprises of punched card, optical scan voting scheme and a designed voting kiosk. The voter comes to the respected polling booth and the identity of the voter is checked and thy allowed to cast their vote. But this system has a major problem that is process of verifying the voter is not done electronically. Thus, the data of verifying the voters can be changed according to their favorable circumstances in order to cast fake votes and thus damaging the constitutional right of every individual. This major error can be minimized by the help of verifying the biometrics of the voter when they come to cast their votes. Biometrics is defined as the process of identifying an individual with the help of their biological traits. The biometric traits in humans are classified of four types, Fingerprints, Facial geometry, Retinal Patterns and voice recognition. In the proposed method fingerprints are used to identify the voter identity with help of biometrics stored in Aadhar database. Thus, the verification is done electronically and only if matched the fingerprint stored the voter is allowed to cast the vote. The verification data is also stored in a database. Even-though if any fake vote is casted, it can be easily identified by checking the database of the voters allowed and those votes which are casted other than the allowed votes can be removed while counting and as all the data are stored electronically it cannot be altered. Thus the major problems in elections can be minimized.

Literature Review

Several steps are taken by the election commission in order to reduce the amount of fake votes casted during elections and other possible errors which can happen. But in the proposed method we have

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 3955 - 3965
Received 15 April 2021; Accepted 05 May 2021.

reduced the major errors during elections with the help of biometric traits of the voters. Fingerprint is used as the biometric factor for verification as it is easily detectable and already available in the database.
P.M.Benson Mansingh et al. [1], proposed a method uses RFID tags to identify the voter and the verification is done using fingerprint sensor. The fingerprint database and verification is done with the help of Aadhaar database. Hemalatha.S [2] proposed method helps in the process of recognizing the fingerprint with the help of interfacing an fingerprint sensor and the what model of Fingerprint sensor must be used to carry out the processes on Fingerprints. Tarang Chugh[3] proposed in explaining the method to recognize the fingerprint with the help of an algorithm called Minutiae Algorithm. The Minutiae algorithm works by checking the five major points in a fingerprint which are called as Ridge Points, Valley Points, Arch Points, Loop Points and Whorl Points. These points are verified to finalize whether the fingerprint is unique or not. Kai Cao and Anil K Jain[4] helps in increasing the speed of fingerprint recognition by using the minutiae algorithm and to recognize just the needed points to mark the fingerprint as an unique one. Thus this study explains that just 20 points are required to identify the fingerprint if it's an unique one or not. Ali, M. M. H.[5]helps in identifying the types of biometric traits of human body is categorized and the purpose of selecting the fingerprint among them is explained. This study concluded that the fingerprint recognition is fast and cost effective than other methods of recognizing human identity. Muzhir Shaban Al- Ani[6]explained the types of fingerprint recognition algorithm in carrying out the process. This study concluded that the minutiae algorithm is majorly used algorithm for fingerprint recognition process.

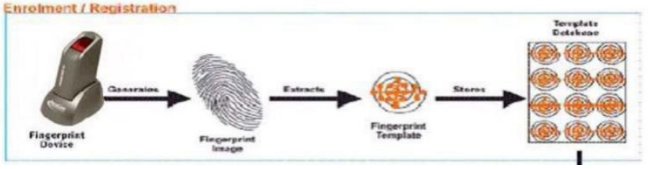
Methodology

A. Fingerprint Database

The fingerprint of the voter is already available in the Aadhaar database of the UIDAI. But in the proposed method we have created a database to store the fingerprints of the voters for verification.

Fig.1.Finger is placed to get stored in Database

Once the fingerprint is placed and recorded it gets stored with the respective name of the voter. Then the fingerprint is available at the database for verification.



Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 3955 - 3965
Received 15 April 2021; Accepted 05 May 2021.

Fig.2. Steps in Finger Enrollment in the Database

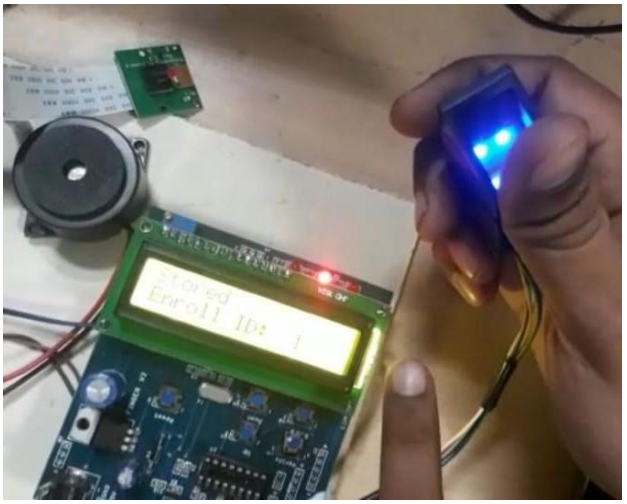


Fig.3. Fingerprint is stored in Database

B. Fingerprint Verification

After storing the fingerprint in the database the next in the proposed method is the verification of the fingerprint of the voter. The identity of the voter is checked and is allowed to place the finger in the fingerprint sensor for verification. If the fingerprint matches with the stored fingerprint then the EVM machine is enabled and the respective voter is allowed to cast his vote. If the fingerprint does not match a small buzzer alert is given and the Aadhaar and other respective identity proofs are verified manually by the booth agent to confirm his identity. If the voter fails to satisfy these conditions he/she is not allowed to cast thy vote.

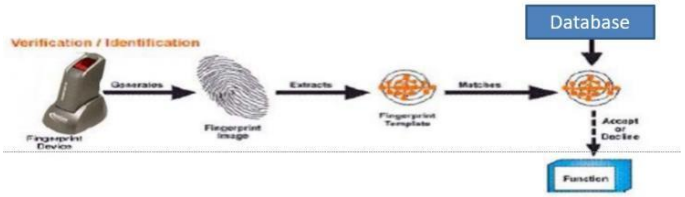


Fig.4. Steps in Fingerprint Verification

C. Algorithm Used

In order to verify the fingerprint an algorithm Minutiae Algorithm is used in the proposed method. It is the process of identifying a fingerprint with the help of five points in a fingerprint which are as follows, Valley Points, Ridge Points, Arch Points, Loop Points and Whorl Points.

It is defined as the point where a ridge forks or diverges into branch ridges. Most of the fingerprint extraction and matching techniques are done using minutiae algorithm. The similarity of two fingerprints is determined by the distance between two minutiae sets.

Fig.5. Minutiae Algorithm Working Principle

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 3955 - 3965
Received 15 April 2021; Accepted 05 May 2021.

- Ridges points:
  - In this method an associate table is introduced to describe the relation of a ridge with its neighbor ridges
  - Thus the whole ridge pattern can be easily handed.
- Valley points
  - It is the most evident structural characteristic of a fingerprint pattern of interleaved images
  - These are also called as ridge lines which is dark.

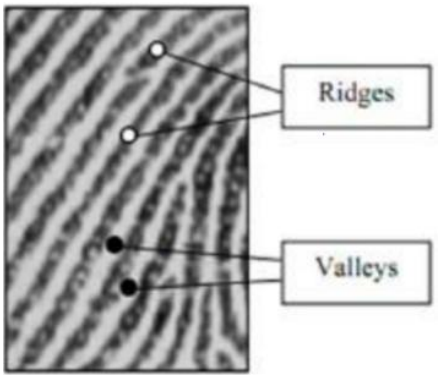


Fig.6. Ridge and Valley Points

- Arch, Loop and whorl Points:
  - Arch points creates a wave like pattern and include plain arches and tented arches. Tented arches rise to a sharper point than plain arches
  - Loop points print that recurve back on themselves to form a loop shapedivided into radial loops and ulnar loops
  - Whorl points form circular or spiral patterns like tiny whirlpools. It makes up about 35% of pattern type.

Fig.7. Arch, Loop and Whorl Points

Results

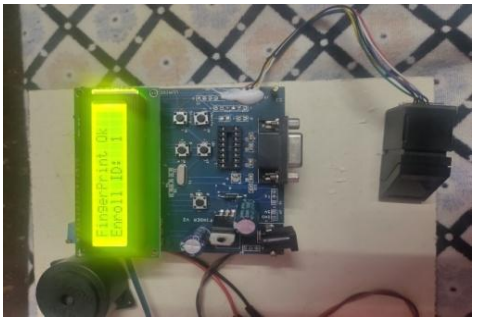
Thus for creating a database first the names of the voters is fetched with the help of their identity card.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 3955 - 3965
Received 15 April 2021; Accepted 05 May 2021.

SNO	VoterName
1	Nitin
2	Mukesh
3	Vineeth
4	Ramesh
5	Rajkumar
6	Saravana
7	Venkatesh
8	Raghul
9	Pradeep
10	Rahul
11	Ram
12	Arjun
13	Vijay
14	Surya
15	Vishnu
16	Vicky
17	Harish
18	Bala
19	Ravi
20	Vimal
NULL	NULL

Table.1. Database of Name of the Voters

Now the fingerprints are stored in the database and available to the polling booth officers to check their biometric identity to cast the votes.



Fig,8. Storage Space for the name

Now an Enroll ID for the voter is created and the voter is allowed to keep his fingerprint to store in the database with respective to their name.

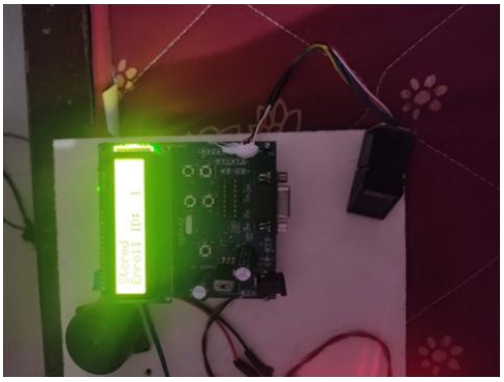


Fig.9. Fingerprint is stored

Thus the fingerprint is stored in the respective name of the user in the database. Likewise for reference the image of five fingerprint storage by creating an enroll id is shown below.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 3955 - 3965
Received 15 April 2021; Accepted 05 May 2021.

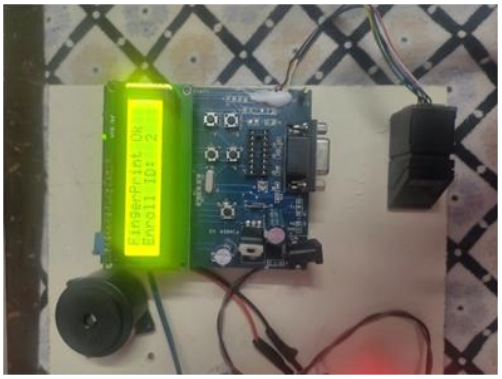


Fig.10. Enroll ID for User 2

Fig.11. Fingerprint is stored for User 2

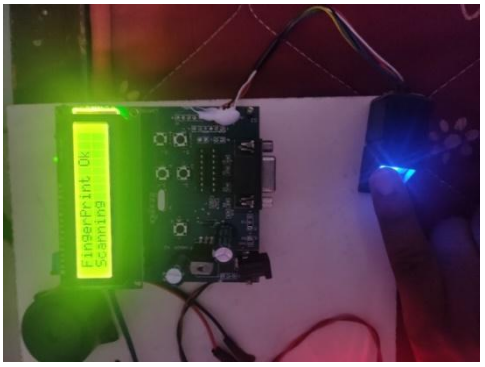


Fig.12. Enroll ID for User 3

Fig.14. Fingerprint stored for User3

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 3955 - 3965
Received 15 April 2021; Accepted 05 May 2021.

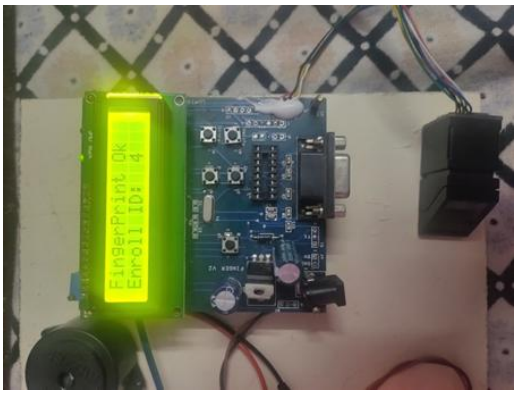


Fig.15. Enroll ID for User 4

Fig.16. Fingerprint stored for User 4

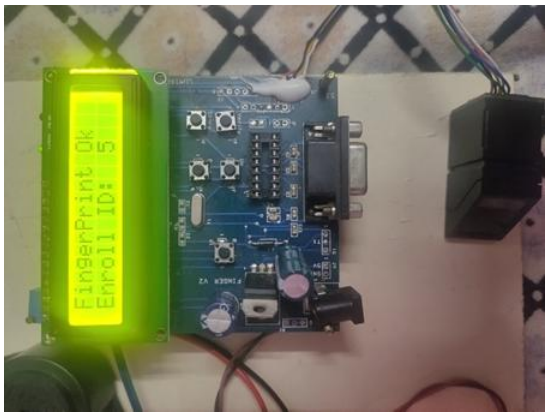


Fig.17. Enroll ID for User 5

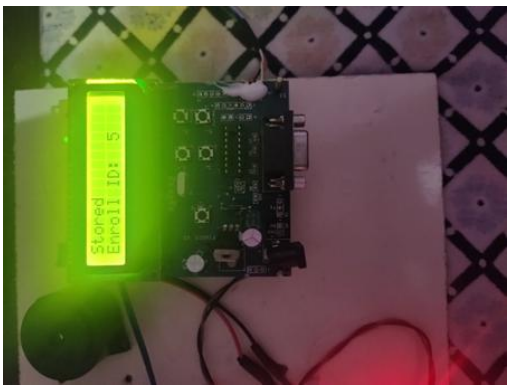


Fig.18. Fingerprint Stored for User 5

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 3955 - 3965
Received 15 April 2021; Accepted 05 May 2021.

Thus the fingerprints are stored of the respective voters in the database with respect to their Enroll ID.

SNO	VoterName	fingerprint_Storage
1	Nitin	Stored
2	Mukesh	Stored
3	Vineeth	Stored
4	Ramesh	Stored
5	Rajkumar	Stored
6	Saravana	Stored
7	Venkatesh	Stored
8	Raghul	Stored
9	Pradeep	Stored
10	Rahul	Stored
11	Ram	Stored
12	Arjun	Stored
13	Vijay	Stored
14	Surya	Stored
15	Vishnu	Stored
16	Vicky	Stored
17	Harish	Stored
18	Bala	Stored
19	Ravi	Stored
20	Vimal	Stored
NULL	NULL	NULL

Table.2. Database of the Stored Fingerprints

Now the fingerprints are stored and the verification process is done in the next step. If the fingerprint matches the voter is allowed to cast his vote if not the voter is not allowed to cast his vote.For instance, three conditions on matching condition and two conditions on non-matching conditions are shown below.

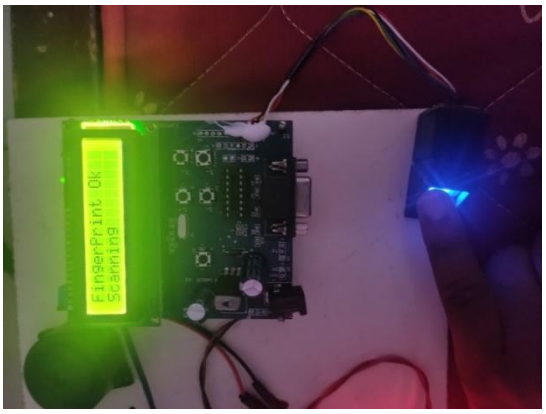


Fig.19. Fingerprint is placed for Verification

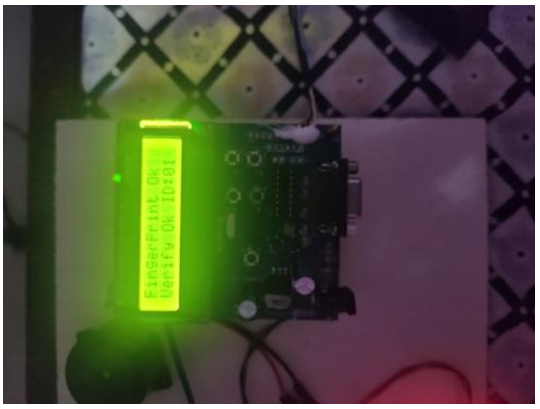


Fig.20. Fingerprint is verified and the saved ID is displayed

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 3955 - 3965
Received 15 April 2021; Accepted 05 May 2021.

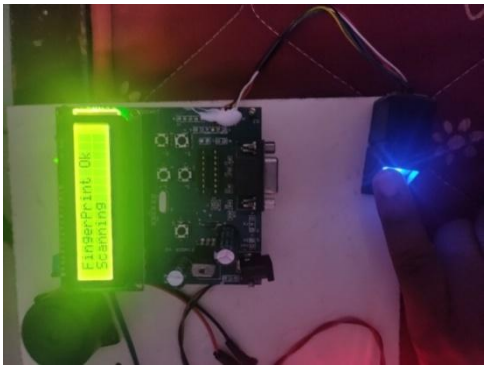


Fig.21. Fingerprint is placed for Verification

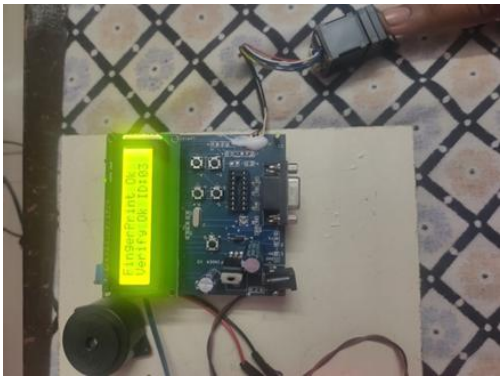


Fig.22. Fingerprint is stored and saved ID is displayed

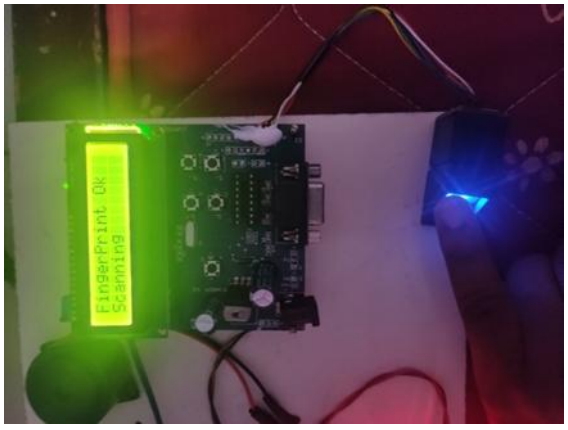


Fig.23. Fingerprint is placed for Verification

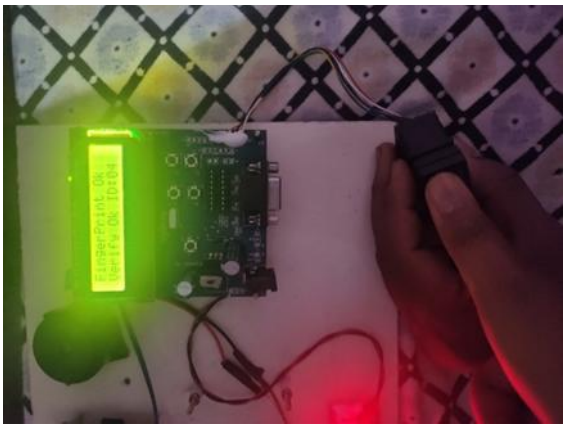


Fig.24. Fingerprint is verified and saved ID is displayed

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 3955 - 3965
Received 15 April 2021; Accepted 05 May 2021.

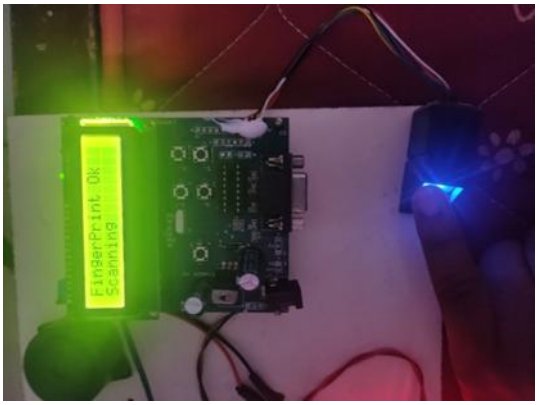


Fig.25. Fingerprint is placed for Verification

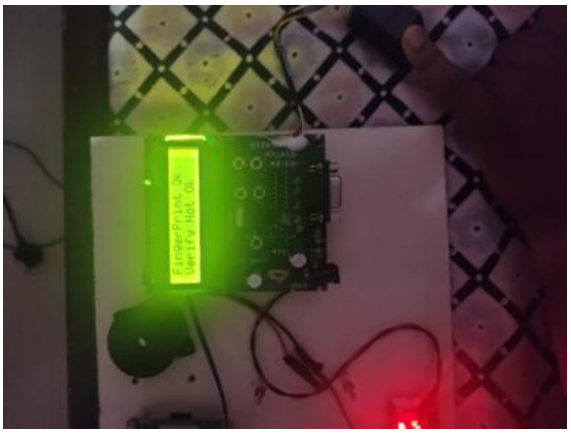


Fig.26. Fingerprint is not matched and the not ok command is displayed

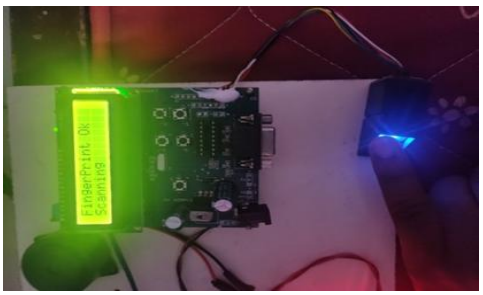


Fig.27. Fingerprint is placed for Verification

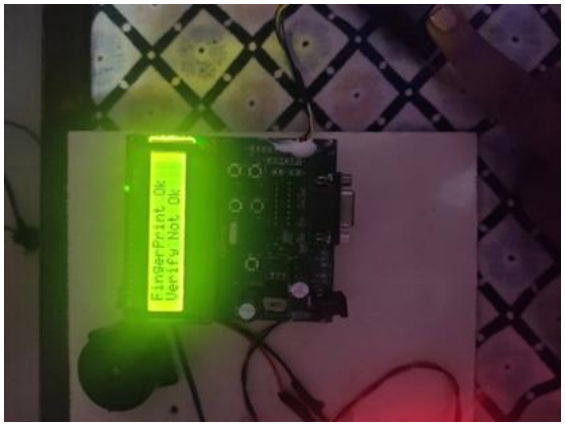


Fig.26. Fingerprint is not matched and the not ok command is displayed

Thus the fingerprint verification for different scenarios is explained. The voting status is also stored in the

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 3955 - 3965
Received 15 April 2021; Accepted 05 May 2021.

separate database, which while considered in counting process the allowed and not allowed voters are separately identified where fake votes can be easily removed.

SNO	VoterName	fingerprint_VotingStatus
1	Nitin	Allowed
2	Mukesh	Not Allowed
3	Vineeth	Allowed
4	Ramesh	Allowed
5	Rajkumar	Not Allowed

Table.3. Database of allowed and not allowed voters

Conclusion

Thus the proposed method has minimized the major errors happening in the elections in dense populated countries. Thus the use of database in storing the fingerprint of the voters and other necessary data electronically the fake voting scam can be minimized at a maximum extent and thus will increase the importance of voting among the general public in a periodically increasing manner in the upcoming days. Thus this methodology will improve the constitutional department of a country for a better and prosperous future.

Future Scope

In the future if we use facial recognition and retinal scanner for the user we can completely stop the fake voting scam in the elections. Although as every biometric data is stored in the Aadhaar database we can use these parameters to verify the voters and the duplication problem can be minimized.

References

[1] P.M.Benson Mansingh, T.Joby Titus and V.S.Sanjana Devi(2020). A Secured Biometric Voting System Using RFID Linked with the Aadhar Database. *6th International Conference on Advanced Computing & Communication Systems (ICACCS).* Vol no.12, pp. 978-1010.

[2] Hemalatha, S (2020), A systematic review on FingerprintbasedBiometric Authentication System.*International Conference on Emerging Trends in Information Technology andEngineering*. Vol.13, (pp. 4142-4341).

[3] Tarang Chugh, Kai Cao and Anil K Jain(2018). Fingerprint Spoof Buster: Use of minutiae-centered patches.*IEEE Transactions on Information Forensics and Security*. Vol.13,(pp. 2190-2202).

[4] Kai Cao and Anil K Jain(2017). Fingerprint indexing and matching: An integratedapproach.*IEEE InternationalJoint Conference on Biometrics (IJCB).*Vol no.12, (pp. 437-445).

[5] Ali, M. M. H., Mahale, V. H., Yannawar, P., & Gaikwad,A.T (2016). Overview of fingerprint recognition system.*International Conference on Electrical, Electronics and Optimization Techniques (ICEEOT).* Vol.3, (pp. 4376-4421).

[6] Muzhir Shaban Al-Ani(2013). A novel thinning algorithm for fingerprintrecognition. *International Journal of Engineering Sciences.*Vol.2, (pp. 43-48).