An Automated Secure Voting System for Digital India

M.P.Swetha[1] N.Sharmila[2] M.K.Sandhya[3#]
[1&2]*Final Year UG Student* [3]*Associate Professor*
Department of Computer Science and Engineering, Meenakshi Sundararajan Engineering College
Chennai, India

Abstract

Digital India aims at empowering our country digitally in the field of technology. In the era of secured transactions from banking to smart ration cards, it is time to use technology for voting system to make it automated and secured. In this paper, an automated secure voting system using biometrics is proposed. This system is used to authenticate the voter and prevent fake votes. The iris and fingerprint data are used to authenticate the voter using image processing techniques. The ultrasonic sensors are used for fingerprint recognition. The contact details like mobile number and mail id of the voter are verified.The automated voting system ensures authentication of the voter and confidentiality of the vote casted using Advanced Encryption Standard. The authentication technique will help the migrants also to vote. Vote revocation can also be done in case of any discrepancy.

Keywords - *Automated Voting System, Biometrics, Ultrasonic sensors, Image processing, Advanced Encryption Standard*

I.INTRODUCTION

Elections in the Indian constitution comprises of elections for the Parliament, RajyaSabha, LokSabha, the Legislative Assemblies, and numerous other Councils and local bodies.The Election Commission of India is an autonomous entity prescribed in the Constitution of India[1]. It is the federal authority responsible for administering all the electoral processes of India and ensuring that the election processes are conducted in a free and fair mannerThe Electronic Voting Machines (EVM) are presently used for the elections in India. The paper ballot vote was replaced by EVM from 1999 in some part of elections and completely after 2014 in all general state elections in India [2]. Figure 1 presents the Electronic voting machine.

In this paper, an automated secure voting system using biometrics is proposed. This system is used to authenticate the voter and ensure valid votes. The iris and fingerprint data are used to authenticate the voter using image processing techniques. The automated voting system ensures authentication of the voter and confidentiality of the vote casted using Advanced Encryption Standard.

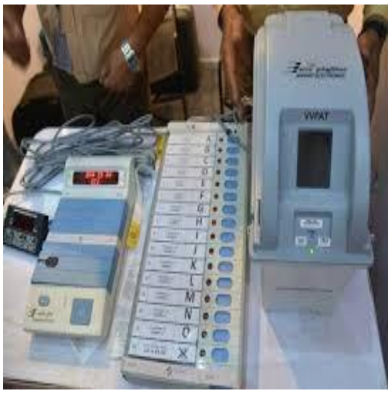

Figure 1. Electronic Voting Machine
(Source: www.indiatvnews.com)

The rest of the paper is organized as follows. Section II describes with the existing EVM system. Section III presents the related technologies to be applied in the proposed automated secure voting system. Section IV presents the working of the proposed automated secure voting system. Section V presents the concluding remarks and the future enhancements.

II.EXISTING EVM SYSTEM

An EVM comprises of a control unit, and the balloting unit. The five meter cable is used to join the two units of electronic voting machine. The voting counts and the results are displayed on 7th segment LED displays. The controller used in EVMs has its functioning program etched eternally in silicon at the time of manufacturing by the manufacturer. No one (including the producer) can change the program once the controller is factory-made [2].
An EVM will record a majority of 3840 votes and might cater to sixty four candidates. There is provision for sixteen candidates in a very single choice unit and up to four units are often connected in parallel. The conventional ballot paper/box methodology of polling is employedif the number of candidates exceeds sixty four. The EVMs ensures the principle of *'one person, one vote'*[2].

The Voting Unit is placed within the selection compartment and the management unit is with the leader or a polling officer. The balloting unit presents horizontally labeled with corresponding party image and candidate names with blue buttons (momentary switch) .The administration unit, on the other hand, provides the officer-in-charge with a ‘Ballot’ distinct button to continue to the next voter, as opposed to issuing a ballot paper to them. This activates the ballot unit for one vote from ensuing citizen within the queue. The voter has to cast his vote by once pressing the blue button on the voting unit against the candidate and image of his selection.

When the last elector has voted, the Polling Officer-in-charge of the management unit can press the 'Close' Button. Thereafter, the EVM will not accept any votes. When vote count has to be declared, the results are displayed by pressing the 'Result' button. There are two methods to prevent the 'Result' button from being pressed before the counting of votes officially begins. This button cannot be pressed until the 'Close' button is pressedat the end of the voting process in the polling booth by the Polling Officer-in-charge. Further, this button is hidden and sealed and this can be broken only at the counting center in the presence of designated officers [2].

III.RELATED TECHNOLOGIES

Biometrics involves the measurement of physical and biological features distinctive to each individual for the purpose of personal proof of identity. It is critical in many security-related situations. These include limited access to areas, data, objects, and in some cases, medical crises. Direct measurement can be more expedient, user-friendly and secure compared to some form of ID, key or password consigned to the person.A 3D imaging technique of fingerprints through an ultrasonic sensor, assures to take the security to another level [3-5]. Fingerprint sensor technology currently used yields a two-dimensional image of a finger’s surface, which can be hoaxed effortlessly with a printed image of the fingerprint. The ultrasonic sensor eradicates that risk by imaging the ridges and valleys of the fingerprint’s surface, and the tissue underneath, in three-dimension.

The process of recognizing people based on distinctive patterns within the ring-shaped region near the pupil of the eye is called iris recognition. The iris commonly has a brown, blue, gray, or greenish color, with composite patterns that are noticeable upon close examination. Since it makes use of a biological characteristic, iris recognition is reflected as a form of biometric authentication [6].Iris recognition systems take high resolution images of the iris of a person’s eye and then apply pattern recognition for reading and matching iris patterns against the patterns stored in the biometric database.

IV. AUTOMATED SECURE VOTING SYSTEM

The proposed automated secure voting system provides voter verification using the biometrics like iris and fingerprint. Each voter’s iris and fingerprint is used to authenticate the user. The one time password is sent to the email and mobile number of the voter. This ensures valid votes and no manual verification of voter is required. The vote details are encrypted using Advanced Encryption Standard (AES) to ensure the privacy of the voters

The fingerprint is unique for each individual even for twins. The most widely used scanners for fingerprint recognition[5] are optical scanners and capacitive scanners. These scanners can be easily forged by the high quality images and also it does not correctly recognize the ridges and whorls of the edge in the fingerprint. The ultrasonic fingerprint scanner is used takes 3D capture of all the ridges and valleysin the fingerprint, compared to a photo captured by an optical scanner which is a 2D image. Ultrasonic fingerprint scanners are more precise than their optical equivalents and more protected because of the 3D impression that the scanner generates of your finger. Ultrasonicwave penetrate through glass up to 800 µm or microns thick and metal up to 400 µm. Figure 2 presents Ultrasonic Fingerprint Imaging and Figure 3 presents a 3D Fingerprint image.

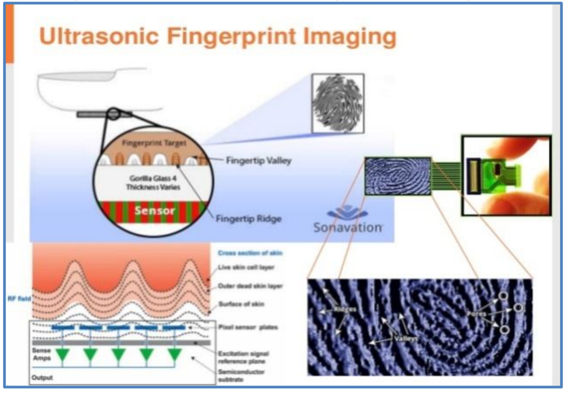

Figure 2. Ultrasonic Fingerprint Imaging

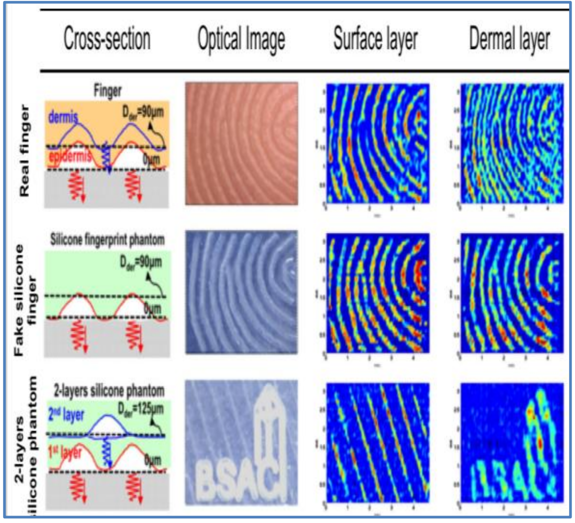

Figure 3. 3D Fingerprint Image

The iris data is unique for each individual hence it provides proper authentication of the voter. The first step is image acquisition in which the beam of optical wave is passed to detect the eye structure and the iris and pupil details are stored in the database. The second step is called segmentation process which isolates the iris in the image captured. In Segmentation process the edge map is formed by the intensity values from the digital image. The next step is to use Daugman's Rubber sheet model for normalization. The normalization procedure will produce iris regions, which have the same perpetual measurements, so that two prints of the same iris under altered situations will have characteristic features at the same three-dimensional location [6]. The iris is matched with iris details stored in the database and if the matching is correct then the voter is allowed to vote.Figure 4 represents the block diagram for Iris recognition.

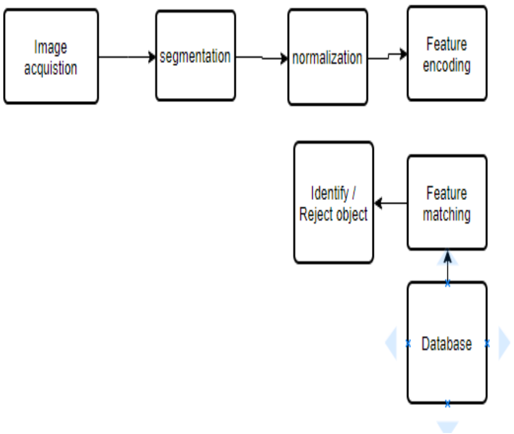

Figure 4. Block diagram for Iris recognition.

The candidate details according to the constituencies are stored in the database.The voter's fingerprint is checked using ultrasonic sensor and if this validation is successful, the next step is to scan the iris and it is validated.Once these two steps of authentication are passed the unique number for the voter is generated and the key along with location details are sent to voter's email and phone number. The fake votes are not possible since the authentication process is two levelusing biometrics .

Based on the address details stored in the database the voter's constituency is displayed and once the voter casts the vote, the vote details are sent to voter's phone number to ensure what the voter has voted is only saved not the modified vote. Previously there are different techniques for provideing security in voting system [7]. In this system, the vote details are encrypted using the unique key generated by AES for the voter and the vote is stored in the database.The AES encryption algorithm contains of four stages that make up a round which is iterated 14 times for a 256-bit key.The first stage is Substitute Bytestransformation which is a non-linear byte substitution for each byte of the block.The second stage is shiftrows transformation which cyclically shifts the bytes within the block.The third stage is each column of four bytes is converted using a special function. It takes as input the four bytes of one column and outputs four completely new bytes, which replaces the original column and the result is another new matrix consisting of 16 new bytes.The last stage is add round key conversion which adds the round key with the block of data.Once the voting time is over the election commisioner can able to generate the results and the non-voters will get the message to confirm they didn't cast the vote. Figure 5 presents the block diagram for automated secure voting system.

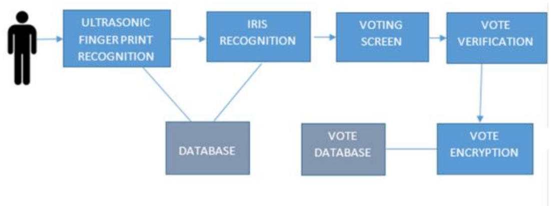

Figure 5. Block diagram for automated secure voting system

Domestic migrants can also cast their votes in this system.Thus the automated voting system enable the voters to cast the vote from any election booth to any constituency irrespective of the location. In case of discrepancy, revocation of vote is also possible.

V.CONCLUSION

The proposed automated secure voting system ensures authentication of the voter using biometrics and the verification of vote by the voter. Moreover, the privacy of the voter is also ensured. The automated voting system will decrease the cost for conducting the election and it will increase the voting percentage. The smartphones with ultrasonic fingerprint scanner and iris recognition features are available in the market. Hence the voting system can be made online so that people can vote from anywhere and it is not necessary to come to polling booth or to wait in the queue. The cost of these smartphones is high.The mobile application which can use the ultrasonic scanning technique and iris recognition in built in the smartphones can be developed at lower cost.

REFERENCES

[1] https://en.wikipedia.org/wiki/Elections_in_India

[2] https://en.wikipedia.org/wiki/Electronic_voting_in_India

[3] Viswanadha Raju, S., Vidyasree, P., Gudavalli, M, "Reinforcing the Security in India's Voting Process through Biometrics", Proceedings of International conference on Advanced computer science and information technology, Chennai September, 2014.

[4] P. Vidyasree, S. V. Raju and G. Madhavi, "Desisting the Fraud in India's Voting Process through Multi Modal biometrics", IEEE 6thInternational Conference on Advanced Computing (IACC), Bhimavaram, 2016, pp. 488-491.

[5] Tang HY, Lu Y, Assaderagh F, Daneman M, Jiang X, Lim M, Li X, Ng E,Singhal U, Tsai JM, Horsley DA,"11.2 3D ultrasonic fingerprint sensor-on-a-chip", In proceedings of IEEE International Solid-State Circuits Conference (ISSCC) Jan 31, 2016 pp. 202-203.

[6] Alhamrouni, M., "Iris Recognition By Using Image Processing Techniques", Atilim University, 2017.

[7] X. Yang, X. Yi, S. Nepal, A. Kelarev and F. Han, "A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic Encryption", IEEE Access, vol. 6, pp. 20506-20519, 2018.