Smart Voting System with GSM module

Asritha Reddy[1], Hema Chowdary[2], Thaanvi Sudarsan Meda[3], *Malathi P.[4]
[1]Deptartment of Computer Science and Engineering
Amrita School of Engineering, Coimbatore

Amrita Vishwa Vidyapeetham, India.

[1]cb.en.u4cse18061@cb.student.amrita.edu,
[2]cb.en.u4cse18224@cb.student.amrita.edu,
[3]cb.en.u4cse18261@cb.student.amrita.edu,
[4]*p_malathy@cb.amrita.edu

Abstract. India is the one among the largest democratic country where in the voting process is considered very crucial and essential. India is the second most populated country which brings in the requirement of an effective voting system to avoid any kind of impersonation and negligence during this process. The researches conducted in the year 2014 show that not more than 66.4% of the citizens cast their votes. In certain regions there is still the practice of using the traditional EVM(elctronic voting machine) which are considered not so efficient and can lead to various types of fraud. Biometrics verification is the process that validate each of the vvoter to proceed with the voting process. Further, a methodology is explained which verifies every voter with their respective IDs and the existing database using biometrics and provide the voters with their voting status through an SMS to the registered number.

Keywords: Minutiae, biometric, verification.

1 Introduction

The proposed system is aimed at evaluating the fingerprints of every voter of the country as to avoid the impersonation during the voting process. This system comprises the biometric technology to identify and authenticate the voters based on their unique characteristics (i-e minutiae of the fingerprint). For the validation of each voter, respective fingerprints are compared with the database. This ensures the elimination of multiple enrollments on the voters list during the voting process. The voter can proceed after validating his / her identification. The voter receives an SMS regarding the status of the validation station if he/she is a valid voter or not. An alarm buzzes displaying the validity of the voter. Depending on the status, the voter can proceed with the vote casting process. The voter then receives an SMS about the status of the casted vote.

2 Literature survey:

The authors have proposed a Real time sytem. New voters must complete a registration form and enroll their fingerprint using a user id and password. The database server will double-check this information. Sweat pores on fingerprints have proven to be useful features for personal identification. The interface allows to vote and displays confirmation message. With the use of fingerprint scanners, this research provided an overview of the voting process. They went over the fingerprint identification and authentication stages in detail, as well as the flow of the election process using this new technology. They also discussed the step of fingerprint gathering and data comparison.stage and matching stage for the aim of recognition in depth with some earlier work.Furthermore, they have introduced various fingerprint authentication approaches that could be useful in voter identification. Finally, there's the Using this cutting-edge technology, the voting procedure is carried out. In this paper they failed to show the verification of the user [1]. The idea is to provide security while also overcoming the constraints of traditional voting.In comparison to the traditional paper-based vote-casting technique, this system is simple to use, convenient, and cost-effective. It could be used instead of a ballot system because the proposed machine provides additional security. The fundamental advantage of this technique is that because everyone's fingerprints are unique, duplication of votes can be eliminated. Further development of the prototype gadget could be done in the future by using numerous fingerprint modules for each party, making it more secure Voter is asked to place their finger on the existing module of the polling booth,allowing an impression of the voter's finger to be taken and used as identity. The impression is then sent to the controlling

unit to be verified.The information is stored in the EEPROM microcontroller of the database which is connected to aurdino board. But EEPROM microcontroller is not producing exact results and verification [2]. BalaMurali et.al has proposed system using IOT Mysql, cloud based databases. Every candidate after casting their respective votes would receive a message to their cell phones.Using IOT makes sure that the votes that are casted is been sent to the server of the database. This system focuses on the confirmation of casted vote by the voters There is not much information provided about the protection of the data of the voters[3]. 3 stages of security in the voting procedure. The initial level is the authentication of Aadhar number, second stage is the authentication of Voter ID and third stage is facing matching.The proposed approach has the potential to eliminate the flaws and shortcomings of the current system, resulting in a reduction in fake and false voting. Because the face cannot be easily altered in a live session, even this would be a difficult effort for hackers, ensuring a secure and enjoyable voting environment free of annoyance. People can easily vote using this method from their local polling booths or even from their homes if they understand how the technology works and are familiar with the system's basic functions.Using LBPH (Linear Binary Pattern Histograms) algorithm. The primary level is the authentication of Aadhar number, second stage is the authentication of Voter ID and third stage is facial matching. Authenticate the facial image of the voters from the database and face is matched with the given data and faces, it gives a message “Face Detected” then it directly redirects to the voting page.Users can cast their vote and Submit. Once the vote is submitted it shows “You have voted successfully”. If the user tries to vote again, then it shows “Fraud Detected” [4]. They propose a method that allows voters to vote from anywhere in India, eliminating the requirement for voters to travel to their constituencies on election day. We use the Aadhar database to store information such as a person's name, age, address, biometric identity, iris information, and phone numbers. We use biometric authentication at the beginning of the voting process for security reasons, and we also verify the voter's age. The voter's vote will be recorded in the voter constituency database, allowing us to easily announce the results without the risk of human error.Using RFID, Microcontroller and GSM technology.We can have chance to avoid electoral frauds and get secured and safety votes by using Biometric verification. So that there is no chance of manual errors during the process of counting the casted votes. Once the registration process is over, during the voting day the voter will login by the given credentials and only on the given day the credentials are valid . It will cross check the image with existing image of the database and sends the OTP to the voter, if the image matches with the existing image. OTP is verified to check for the valid voter[5]. There are two types of voting systems in use in India right now. Ballet paper and Electronic Voting Machines (EVM) are the two methods, but each has its own set of limitations and drawbacks.The existing voting mechanism is not only insecure, but also time-consuming. As a result, under this notion, we must propose a voting system or method that is very effective in voting. The system will be made up of two parts . The first one is “before the election day” and “on the election day”.On the Day of Election another independent Android application is used for voting operations.The

voter is verified using face recognition technology. This system consumes more time [6]. This System has prposed by using Raspberry pi, fingerprint sensor, LCD display, such that safe voting happens without impersonation. No single person can vote multiple times and impersonation of the absentee voters can be avoided. It is easy to use and is also cost efficient with minimal human resources. No knowledge of other official Ids is used in this system to verify every voter.Voter does not receive any information after casting his/her vote about the validity of the same[7]. They propose a blockchain-based e-voting scheme that fits all of the e-voting process's requirements. Block by block, all votes on the blockchain are cryptographically linked. When two blocks with the same timestamp have the same signature value, the block with the higher signature value is chosen. The voter can vote in line with the list of candidate or vote for any other persons he/her wants. In most cases, the vote is open to the public, therefore the information about the vote is not encrypted. The blockchain-based e-voting system can be used in a number of voting situations as well as for other purposes. Despite being a secure technology, blockchain employs ECC public key encryption, which is vulnerable to quantum computer assaults.Paper has been proposed by using blockchain in P2P network technology. A design of synchronized model of voting records based on distributed ledger technology (DLT) to avoid forgery of votes. The system involves electronic voting theory, cryptography, and software engineering theory[8]. By using Arduino-based Smart E-Voting system with fingerprint authentication. Different algorithms are employed in some other studies and different methodologies are presented in some other works that are based on multimodal biometric identification.In this study, they have introduced the idea of obtaining a voter's fingerprint impression, which would then be submitted as data into the system. The data was then compared to what was available in the database. Access to cast a vote is allowed if the specific data matches anyone on the accessible record[9]. Elections in India will no longer be a time-consuming task. The purpose of this paper is to provide an overview of the biometric voting system.Fingerprint technology improves security by preventing tampering, forgery, and repetitive voting. This has the potential to result in by holding free and fair elections in India, India has made a fundamental change in electoral procedure. Illegal practises such as rigging will be eliminated as a result of this.As a result, voters can exercise their democratic right to choose their leaders and political parties. The same procedure was used can be implemented in other nations, and the political process can be substantially altered as a result of this technology.There is a comparison of fingerprints so as to avoid multiple votes by a single voter.The binary pattern is used by an image processing technique to scan the fingerprints of a voter. The system is highly reliable and has a low maintenance cost. Requires more human resources for the verification process during the election process This system does not provide any information to the voters about their respective vote.Every voter is not assured whether his/her vote is valid or invalid[10].

3 Architecture :

In this proposed system we first begin by obtaining a clear image of the fingerprint of the voter using the ultrasonic fingerprint scanner. Then, we enhance the obtained image to improve the clarity of ridge and furrows of the minutiae. We process the fingerprint image to enhance the unique features and compare the results with the fingerprints of the database. This validates the voter and displays the outcome of the verification process. The voter can cast their votes depending on the confirmation displayed of the verification process and an SMS is sent to their registered mobile numbers.

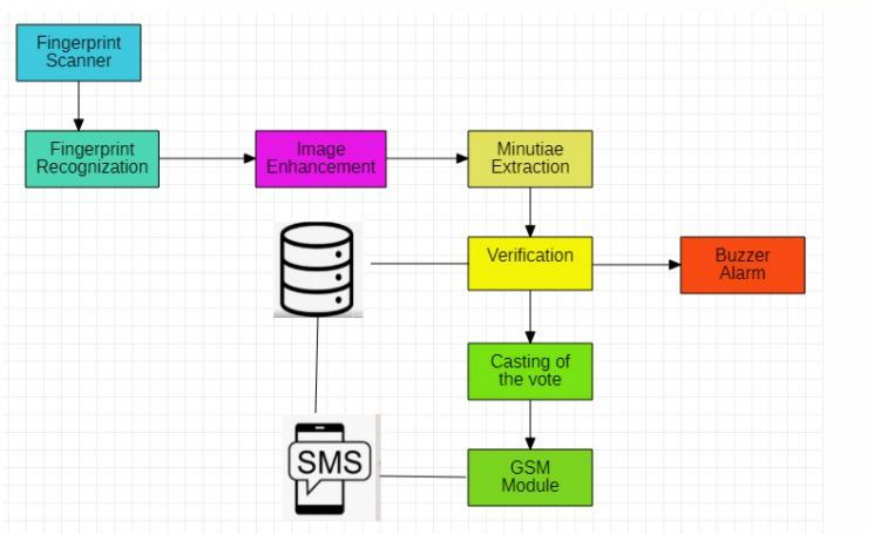

Fig. 1. Architecture diagram

4 Methodology :

4.1 Image enhancement:

The Image Enhancement process removes various kinds of noise such as creases, smudges and holes. It is to reconstruct the true ridge/valley structures in the regions of the fingerprint. This provides us with the required characteristics of the fingerprint or the minutiae. All the below mentioned functions combine in an effective image enhancement.

4.1.1 Image segmentation:

This technique creates pixel-wise mask for each object in the image (i-e dividing it into a multiple segments).Pixels with intensity [Grey level value]:

- ⇨ Greater than the threshold: Considered
- ⇨ Lesser than the threshold: Removed

4.1.2 Image normalization:

Each of the pixels of the fingerprint image has varied mean-variance which makes it necessary to normalize the image. To obtain the required uniform pattern, the pixels are normalized in the range of grey values.

4.1.3 Image orientation:

The image is formed based on the ridge orientation.

- ⇨ Orientation = average of vectors orthogonal to gradient of each pixels at x and y direction.

4.1.4 Image filtering:

The appearance of an image is altered by changing the colors of the pixels.The contrast is increased by using Gabor filter or a Butterworth filter.

4.2 Minutiae extraction:

Further, we proceed with image binarization and image thinning for the precise location of ridge endings and false minutiae is filtered out. We qualify minutiae by

type and quality to make the search quicker and easier. The user is then verified using biometrics and the SMS is sent to their registered mobile numbers.

4.2.1 Image binarization:

Image is converted to a binary image.
Based on the global threshold ; pixel value
greater than the threshold = 1
less than the threshold = 0

4.2.2 Image thinning:

This is used to eliminate selected background pixels from the binary image.
This preserves the necessary details and connectivities of the ridges.

Fig. 2. (a) binarized image (b) thinned image

4.2.3 Harris corner detector:

Harris Corner Detector is an operator that is commonly used to extract corners and infer features of an image. This has been proved to be more accurate in distinguishing between edges and corners.

Corners - A corner is a point whose local neighborhood stands in two dominant and different edge directions.

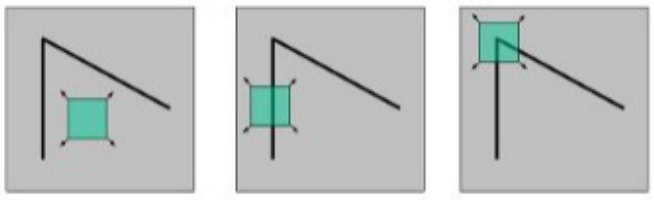

Fig. 3. Flat region Edge Corner

This detector identifies the corners of the images from each of the pixel of the processed image. The corners are detected as the regions where there exists variations in large intensity of gradients when traversed in all directions of the image. A window like figure is considered around the pixel and identify such windows which are unique. This can be measured by moving the window at a very small distance in different directions and calculating the amount of changes that occured in each of the pixel values.

$$E(u,v) = \sum_{x,y} \underbrace{w(x,y)}_{\text{window function}} \underbrace{[I(x+u,y+v)}_{\text{shifted intensity}} - \underbrace{I(x,y)}_{\text{intensity}}]^2$$

Fig. 4. Change of intensity for evry shift [u,v]

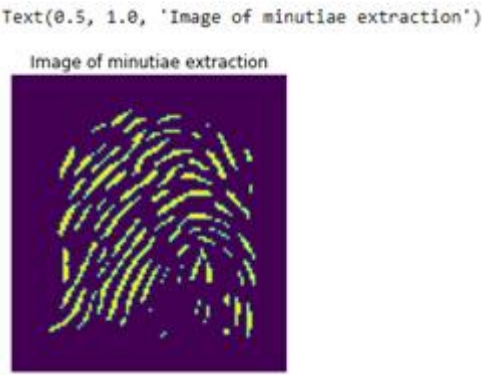

Fig. 5. Minutiae extraction

4.3 Minutiae matching:

The details of the minutiae from the processed image are extracted and are then compared with the already stored image patterns in the database. Hamming Distance –a metric for comparing two binary data strings. The Hamming distance

between two strings, ‘a’ and ‘b’ is denoted as d (a, b). A specific threshold is set to match the minutiae after the score is calculated by summing up the Hamming distance. Two images are taken for the authentication process where the binary points are considered in an array of each of the image. The hamming distacnce between these points is found providing us with n number of sums. All these values are summed up to give the score and is then compared with the threshold value. If the score is greater than the threshold value, it shows that the finger prints match.

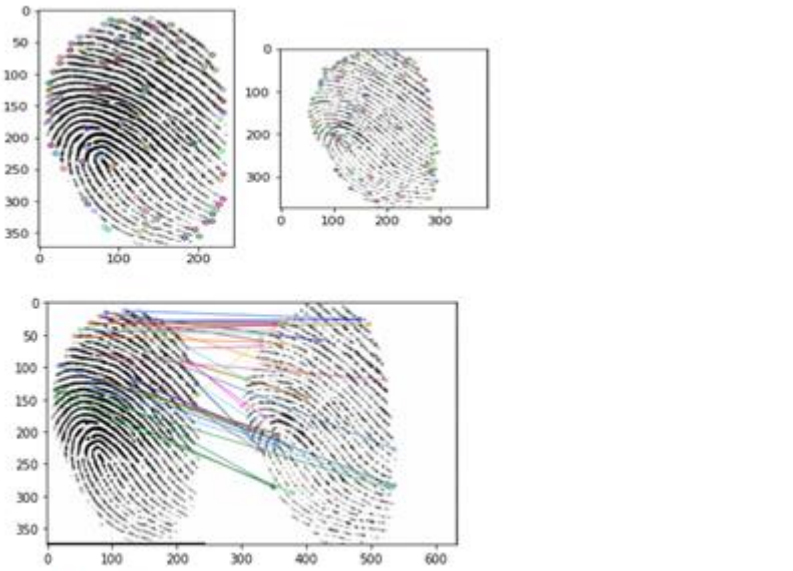

Fig. 6. Fingerprints that matches

4.4 GSM Module:

GSM module is a cellular technolgy that is used for wireless communication using two or more devices. Later with the SMS provision, a user can send a voice message to the receiver that can be transmitted through air. This technology can be included in the voting process to send information to the voter's registered mobile numbers. After the verification of the voter using biometrics, he/she then receives a message stating if he/she is a valid voter or not. The implementation of the GSM module helps the voter to know on their status on the voting process and make amendments if any for future processes (i-e applying for a new ID). This process is implemented using the API by providing the regsistered mobile numbers present in the database of the voter.

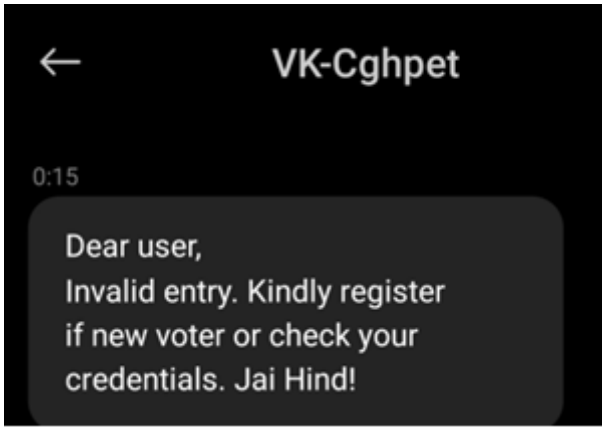

Fig. 7. SMS sent to the respective invalid voter

5. Conclusion:

In this system, the user is verified using biometrics with the database and the present fingerprint of the user obtained by the ultrasonic fingerprint scanner. It begins with

obtaining minutiae characteristics of the user and matching it with the fingerprint of the existing database. An alarm buzzes to indicate the validity of the user and the voter can proceed further. The user then receives a message to his/her registered mobile number if he/she is a valid voter or not and also regarding the validity of the casted vote.

6 References:

1. Charan S, Prasanth, Joseph DA. Smart voting system using Fingerprint Scanner.
2. Kulkarni AV, Ghadge N, Khatave P, Patil S, Sutar U, Tople P. Finger Print Based Voting System Using Arduino. International Journal of Research in Engineering, Science and Management. 2020;3(2):784-6.
3. BalaMurali A, Sravanthi PS, Rupa B. Smart and Secure Voting Machine using Biometrics. In2020 Fourth International Conference on Inventive Systems and Control (ICISC) 2020 Jan 8 (pp. 127-132). IEEE.
4. CH.Chandra Mouli , M. Laasya Priya, J. Uttej, G. Pavan Sri Sai, Dr. R. Vijay Kumar-" Smart Voting system" Using Linear Binary Pattern Histograms,by IJIEMR (2020)
5. GowthamR,HarshaKN,M.Ranjunatha,B Girish H S, Nithya Kumar-" Smart voting system", using RFID, Microcontroller and GSM technology, by IJERT(2019)
6. Mrs. Swetha M S , Mr. Shreejwol Disti , Dr. Thungamani M , Mr. Raman Shah-" Smart voting system support through face recognition",Using Ballet voting System and Electronic Voting Machine,by International Journal for Innovative Research in Science and Technology (2019)
7. G.Rama Lakshmi;CH. Sri Rekha;V.Likhita;T.Alekhya;-K.V. Renuka-" E - Voting System using Biometrics" Using Raspberry Pi scanner and LCD Display Technology, by IEEE (2019)
8. Yi H. Securing e-voting based on blockchain in P2P network. EURASIP Journal on Wireless Communications and Networking. 2019 Dec;2019(1):1-9.
9. Shaikh Rijwana A,Lavhe Bhagyashri B , Wagh Sayali S , Shinde Rekha S, Prof.Bobade Archana M.-" Arduino-based Smart E-Voting system with fingerprint authentication.", by IJERT (2020)
10. Sumanth Kashyap A, Smriti Gururaj-" Smart Voting System to prevent malpractice using fingerprint Technology" Using electronic voter machine , Image Processing using binary patterns, by IJERT (2020)
11. Anand AR, Ramkumar S, Kumar VA, Vinoth K, Aravinth J. Secure Iris Recognition using Negative Database. In2020 International Conference on Communication and Signal Processing (ICCSP) 2020 Jul 28 (pp. 0071-0075). IEEE.
12. Govindraj VJ, Yashwanth PV, Bhat SV, Ramesh TK. Smart Door Using Biometric NFC Band and OTP Based Methods. In2020 International Conference for Emerging Technology (INCET) 2020 Jun 5 (pp. 1-4). IEEE.
13. Prathilothamai M, Nair PS. De-duplication of passports using Aadhaar. In2017 International Conference on Computer Communication and Informatics (ICCCI) 2017 Jan 5 (pp. 1-5). IEEE.
14. Muhammed MA, Aravinth J. CNN based off-the-person ECG biometrics. In2019 International Conference on Wireless Communications Signal Processing and

Networking (WiSPNET) 2019 Mar 21 (pp. 217-221). IEEE.
15. Narayanan A, Varma R, Yashaswi NR, Malladi T, Vasudevan SK, Ramya GR. A Simple, Efficient and Innovative Biometric Human Identification Using Weighted Thresholding and KNN. In2018 15th IEEE India Council International Conference (INDICON) 2018 Dec 16 (pp. 1-6). IEEE.