

VOTING SYSTEM BASED ON FINGERPRINT RECOGNITION USING MINUTIAE MATCHING

Flavius Arockia Milan.L¹, Mohamed Bazeer.H², Dhinesh.S³, Prakash.M⁴, Rengaraj @Muralidharan.R⁵

Dept of IT, Saranathan college of Engineering, Trichy, Tamilnadu ^{1,2,3,4}

Assistant Professor, Dept. of IT, Saranathan college of Engineering, Trichy, Tamilnadu ⁵

Abstract— Voting system nowadays involves more fraudulent activities which leads to incorrect voting process and it also decreases the security of the voting process. Biometric authentication will provide unique authenticity to every voter. There are various types of applications for Fingerprint recognition which is used for different purposes. Fingerprint is one of the challenging pattern recognition system. The Fingerprint recognition system is divided into four stages which were explained in this paper. We have proposed an Online Voting System which uses Fingerprint recognition and verification as the security measure, thereby providing solution for several security issues. In order to make the system more efficient, we also proposed a online process using OneTimePassword(OTP) which allows people to vote in their comfortable place. This will result in a secure online voting system thereby increasing voting percentage.

IndexTerms—biometric, fingerprint, matching, minutiae, voting.

I. INTRODUCTION

Biometric authentication is a security process that depends on the unique biological characteristics of an individual to verify that he is the person. Biometric authentication systems compare a biometric data acquired with stored authentic data in a database. If both samples of the biometric data match, authentication is confirmed. Biometric authentication is used to allow authenticity for an individual to physical and digital resources such as buildings, rooms and computing devices. Biometric authentication is becoming

relatively common everywhere. In addition to the security provided by hard-to-fake individual biological traits, the acceptance of biometric verification has also been driven by convenience: An Individual can't easily forget or lose his biometrics. The oldest form of biometric verification is fingerprinting.

A fingerprint is an impression left by the friction ridges and endings of a human finger. Fingerprints are easily deposited on suitable surfaces (such as glass or metal or polished stone) by the natural secretions of sweat from the eccrine glands that are present in epidermal ridges. These are sometimes referred to as "Chanced Impressions"[15]. Human fingerprints are detailed, unique because ridge characteristics differs for every human. Fingerprints are difficult to change, and durable over the life of a person. Fingerprint identification is based primarily on the minutiae, or the location and direction of the ridge endings and bifurcations (splits) along a ridge path. There are a variety of sensor types such as optical, capacitive, ultrasound, and thermal which are used for collecting the digital image of a fingerprint surface. Optical sensors take an image of the fingerprint by making use of Light Emitting Diode(LED), and are the most common sensor today.

The two main classification of fingerprint verification techniques are minutiae-based matching and pattern matching[15]. Pattern matching compares two images to see how similar they are. Pattern matching technique classifies the images based on the types of fingerprint. Pattern matching is usually implemented in fingerprint systems to detect

duplicates. The most widely used fingerprint recognition technique, is minutiae-based matching in which minutiae points are extracted from the image acquired using various techniques. The next section elaborates the survey done on fingerprint recognition techniques and applications.

II . LITERATURE SURVEY

1. FINGERPRINT RECOGNITION

1.1. Biometric Security Using Finger Print Recognition

A Fingerprint Recognition for digital handheld devices had been proposed by Mazumdar et.al[6]. They are using a device that scans the finger print and gives out a high quality image. The output is an image that has been stored and processed to extract the critical pixel information (minutiae). A secure process is then forked based on the authorization. The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutiae points, which are unique features found within the patterns. They used the *libfprint* open source fingerprint recognition library to handle image capture, enrollment, verification and identification. The current system of *libfprint library* is that a fingerprint is scanned using a scanner (storing its minutiae data), and at the time of verification, the pre-stored (enrolled) minutiae data is compared to a *live scan*. A parameter known as match score is returned which specifies the similarity between two fingerprints. *libfprint* provides enrollment, verification and identification API. Enrollment is a process in which a user's fingerprint is scanned using a fingerprint scanner, processed and stored for matching purpose. *libfprint* extracts the minutiae information from the image and if quality of detected minutiae is above a threshold it declares it as a successfully enrollment. Verification is a process in which user provides one's identity and the system compares the scanned fingerprint against stored fingerprint data for that user identity and declares a match or no match. In Identification, a user provides one's fingerprint scan which is compared against all previously enrolled fingerprint data to find the identity. This system gives high quality image of fingerprints, highly precise and accurate image but less compatible.

1.2. Fingerprint Recognition System using Minutiae Estimation

Manu Garg et.al[8] focused on developing a system for recognizing two fingerprints using minutiae matching. They utilized a combination of image processing and frequency domain processing to build a minutiae extractor and a minutiae matcher. The several other steps in fingerprint recognition process also includes image segmentation using Morphological operations, improved thinning, false minutiae removal methods and minutiae marking. The final results are obtained in percentage of matching minutiae. The first step is the process in which the two fingerprint images have to be matched are read and then image enhancement is applied on the two images. For enhancing the fingerprint images, histogram equalization is used. It is a technique of improving the global contrast of an image by adjusting the intensity distribution on a histogram. The second step is to take the Fast Fourier Transform(FFT) of the input images. The FFT provides the improvements on the enhanced image such as some false broken points on ridges get connected and some spurious connections between ridges get removed. Converting the enhanced images to their binary version is the next step. Binarization is a process which transforms the 8-bit Gray image to a 1-bit image with 0-value for ridges and 1-value for valleys. After the operation, ridges in the fingerprint are highlighted with black color while valleys are white. Computing Region of Interest using Image Segmentation. To extract the ROI, a two-step method is used. The first step is block direction estimation, while the second is computing ROI using the Morphological methods. Initially, 16x16 pixels is estimated in the block direction for each block of the fingerprint image in block direction estimation. The last step is minutiae marking and extraction. This system clearly explains the algorithm for Minutiae Extraction and Matching. Fingerprint results are more Accurate but it contains complex calculations and too many steps to achieve accuracy.

1.3. An approach for Minutia Extraction in Latent Fingerprint Matching

Ajay Kumar Singh[10] proposed a system where the minutiae extraction method was improved by combining it with image enhancement that includes noise reduction, smoothing, contrast stretching, histogram equalization, Fourier transform and edge enhancement. For the image preprocessing steps, they have used histogram equalization followed by Fast Fourier Transform to do the image enhancement and then image binarization is done by locally adaptive threshold

method. This method presented a satisfactorily performance. Some of the methods are :Fingerprint image enhancement is to prepare the image to be better to ease further operations. The fingerprint images were first enhanced by using Histogram Equalization. Histogram is a process that attempts to spread out the gray levels in an image so that they are evenly distributed across their range . Fingerprint image binarization is done to transform a 8-bit gray image to a 1-bit binarized image where 0-value holds for ridges and 1-value for furrows. Region of interest is the useful part where the image area without effective furrows and ridges will be first discarded from the image since it has only background information. To get the ROI(Region of Interest) ,they used a two-step method. The first step constitutes “block direction estimation” and “direction variety check”[10], whereas the second step is done using some morphological operations. Thinning is the process of reducing binary objects or shapes to strokes whose width is one pixel wide . The minutiae details of two fingerprints are obtained using the above procedures and they are matched using the minutiae match algorithm. Alignment based match algorithm is used in our project. It comprises of two stages:

- i. Alignment Stage.
- ii. Match Stage.

To align one set of minutiae with respect to another an iterative ridge alignment algorithm is used and to count the number of matching minutiae pairs an elastic match algorithm is used.This paper gives brief explanation of minutiae extraction method and gives result with highly reduced noise but separate algorithms were used for alignment and counting minutiae pairs.

2. ONLINE VOTING SYSTEM

2.1 An Efficient Online Voting System

Ankit et.al[12] proposed a system to design, build and test a online voting system that facilitates user (the person who is eligible for voting), candidate (Candidate are the users who are going to stand in elections for their respective party), Election Commission Officer (Election Commission Officer who will verify whether registered user and candidates are authentic or not) to participate in online voting. The proposed system is developed to work on Ethernet and supports online voting. The system creates an environment that enables the user to login to the system using their username and password and click on his favorable candidates to register vote thereby increasing the voting percentage in India. By applying high security it will reduce false votes. The voting system had evolved from counting hands, ballot voting, punch card, mechanical lever and optical-scan machines. But it also provides the advantages of the traditional voting system such

as accuracy, convenience, flexibility, privacy, verifiability and Mobility. The system has many advantages even though it suffers from various drawbacks such as Time consuming , consumes large volume of pare work ,no direct role for the higher officials, damage of machines due to lack of attention, Mass update doesn't allows users to update and edit many item simultaneously. They provide a detailed description of the functional and performance characteristics of online voting system. The voters can cast their vote irrespective of their location i.e., from anywhere in the world without visiting the voting booths, in highly secured way. That makes voting a fearless of violence and that increases the percentage of voting.

Online voting system contains:

- a) Voter's information in database.
- b) Voter's Names with ID and password.
- c) Voter's vote in a database.

2.2 NEW APPLIED E-VOTING SYSTEM

An electronic voting system has been developed by Feras et.al[13] that have security context is known as e-trusted voting system. This system was developed mainly to provide trusted framework for electronic voting. The voter can use the system using the username and password provided to them. The process involves in which that the voter can enter the system and votes on the existing e-ballot on the election date and the voter can see the result immediately after the end of election date. In order to test whether the system had been fully functioning and meets the user's requirement, we have to apply the system to a sample of 20 persons and check whether the system provides authenticity to those attempting to vote. Recent democratic elections using voting machines have shown that the winning margins could be less than the error margins of the voting systems themselves, making election an error prone task. The traditional voting system has some disadvantages which can be overcome using the Electronic voting system. Formerly when elections were made traditionally, organizers determine who is eligible to vote. This may involve a formal registration period or an announcement that anyone who is a member of a certain group as of a certain time may vote. Once the voter begins to vote, administrators may verify the details of those attempting to vote. This way could involve asking voters for identification cards or passwords. Generally, this procedure also involves keeping track of who has already voted so that eligible voters may vote only once. Moreover, the traditional way of voting generates mores constraints such as election fraud that can be prevented by using physical security measure, audit trails, and observers representing of all parties involved. But the prevention of election fraud is made more difficult by the frequent requirement that votes remain private.

III. MINUTIAE EXTRACTION TECHNIQUE

Most of the fingerprint verification technologies are based on Minutiae. Minutiae-based techniques represent the fingerprint by its local ridge patterns, like terminations and bifurcations[17]. The first step to do fingerprint recognition is enrollment which is the process to register the biometric data to database as a template then fingerprint recognition undergo either Verification process or Identification process which is depending on the purpose of study. In the verification process the person's fingerprint is verified from the database by using matching algorithms. Also it is called (1:1) Matching. It is the comparison of a claimant fingerprint against enrolled fingerprint. Initially the person stores his/her fingerprint into verification system using a scanner, and the result will show whether the fingerprint taken from the user during a live scan is matching with the fingerprint stored as a template in database or not. Fig 1 shows the sequence of steps used in minutiae extraction algorithm. There are 3 stages :

1. Pre-processing stage.
2. Minutiae Extraction stage.
3. Post-processing stage.

Each stage contains series of steps which are used to extract the minutiae and for matching purposes. Compared to other fingerprint features, the minutia point features having corresponding orientation maps are distinct enough to distinguish between fingerprints robustly. Fingerprint representation using minutiae feature reduces the complex issue of fingerprint recognition to an issue of point pattern matching. However, the primary challenge lies in extracting the minutiae from a poor quality image.

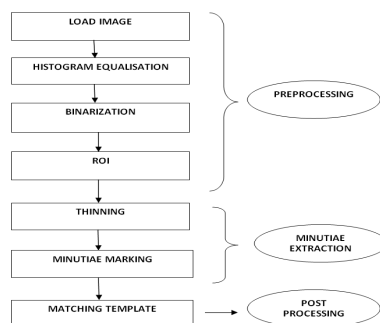


Fig 1: Stages and steps in minutiae extraction technique

The Stages are discussed as follows:

A. PRE-PROCESSING STAGE :

The Pre-processing stage is the process of removing unwanted data in fingerprint image such as noise , reflection ,etc. It is used to increase the clarity of ridge structure. The main steps in Pre-processing stage are :

1.Acquiring fingerprint images from the user:The **First step** is to acquire the fingerprint image by using a fingerprint scanner.It is the process to obtain image by different ways such as Online and Offline .There are number of methods are used .In online method the optical fingerprint reader is used to capture the image of fingerprint . In offline method the fingerprint image is obtained by ink in the area of finger and then put a sheet of white Paper on fingerprint and scan it to get a digital image.

2. Enhancing the acquired fingerprint image:The **Second step** is to enhance the acquired image using Histogram equalisation.It is a method that improves the contrast in the image acquired, in order to increase the intensity range.To make it clearer, from the Fig 2, you can see that the pixels seem clustered around the middle of the available range of intensities. What Histogram Equalization does is to stretch the range of pixels. Take a look at the figure below: After applying the equalization, we get an histogram like the figure in the center. The resulting image is shown in the picture at right.

The result of enhancement is shown in the Fig 2.

Histogram Equalization



Fig 2:Enhanced image using histogram equalisation

3. Binarization :The **Third step** is image binarization in which a threshold value is chosen and all pixels having values above the threshold are classified as white while all other pixels are classified as black. A correct threshold is selected by using adaptive image binarization method where an optimal threshold is chosen for each image. As the run-length representation reduces memory space and also speeds up

processing time, it is considered very efficient for binary or labelled images. The binarization of fingerprint image is a process to transform the image from 256 levels to two levels (0,1) refers to (black and white) respectively. The result of binarization is shown in Fig.3. In this paper we used locally adaptive binarization method which is summarized in this steps below:

1. The image is divided into blocks with size 16x16.
2. mean intensity value for each block is Calculated.

Generally, Adaptive binarization method is used for local binarization. In this a window of NxN blocks slide over the entire image and threshold value is computed for each local area under the window for binarization. The adaptive method give more accurate result as compared to global binarization in such conditions where the image effected from bad shading, blurring, low resolution and non uniform illumination.

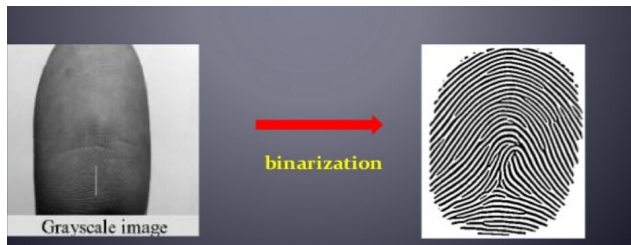


Fig 3: Binarized image

4. Region of Interest: The last step (ROI) is a segmentation technique. The main motive of the segmentation is to make the image simpler which can be representing very easily and to make image meaningful that will be easy to analyze. Generally ROI (Region of Interest) is very useful for analyzing a fingerprint image. It is a subset of an image or a dataset analyze for a particular purpose. When the image area has ineffective ridges and furrows so firstly it made wider and larger in all directions. Extraction of the ROI is performed in two steps: First, block direction estimation and direction variety check; Second, using some Morphological methods. Two types of morphological methods are available i.e. OPEN and CLOSE. The OPEN operation can enlarge the images and eliminate background noise and CLOSE operation can shrink images and eliminate small cavities. In other words, Region of Interest where the interested region i.e: the region where we want to focus on the fingerprint to get a better quality and to reduce the time in matching the fingerprint image. It is done by cutting the image and focusing on the region. For eg ,centre of fingerprint will show you the type of fingerprint. Fig 4 shows the region of interest:

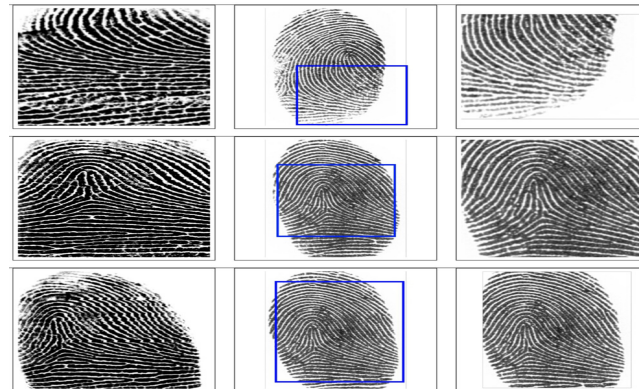


Fig 4 : Images showing particular region

B. MINUTIAE EXTRACTION STAGE:

The extraction stage is used to extract the features (minutiae) that are used to match, verify or identify the individual. There are two steps involved in this stage:

1. Thinning: Thinning process is the **first step** involved in the minutiae extraction process. After the thinning process is applied, ridges in the fingerprint impression become one pixel wide. The main purpose of the thinning algorithm is to eliminate the redundant pixels in the image. Thinning process can be carried out with the help of parallel thinning algorithm. The redundant pixels are first stored in small image windows (3*3). Then the redundant pixels can be removed after several scans. But the parallel thinning algorithm is not a very efficient algorithm because it takes too much time. The binarization process is applied in the first step in the fingerprint impression because it contains the maximum grey intensity values. The parallel thinning algorithm is complex in nature. Thinning process can be done using the morphological thinning operator. Thinning process works only on black and white images. Thinning step plays a very important role in the minutiae extraction process because it reduces the amount of data to be processed. It also reduces time. It is also helpful for the extraction of the minutiae features. Shape analysis can also be done using the morphological thinning algorithm and minutiae extraction process becomes easy to use when it is applied on line like patterns.

Thinning process which is shown in Fig.5, is also called (skeletonization)[17]. To enhance the binary image the thinning algorithm is used to reduce the ridges of fingerprint images. There are number of thinning methods. The most popular thinning algorithms are medial axis method, contour generation method, local thickness based thinning approach, sequential and parallel thinning. We used

morphological operation on binary image ,the main steps to do thinning is :

1. Clean up the thin image by remove single isolated , removes H-Breaks and removes spikes.
2. Remove the connected region at the boundary.



Fig 5: Thinned image

2. Minutiae marking: Minutiae marking is done in the minutiae extraction process .This step produces a better result when larger number of minutiae are detected. This step is applied after the image pre-processing step. It mainly works on the pixel value (1 or 0). There are two methods involved in the minutiae extraction process. The first method deals with value one and the second method deals with value zero. The binarization process is carried out with the help of mask. Minutiae are points in the fingerprint impression which has one neighbour or more than one neighbor. This stage is a process where the resultant image from thinning stage is taken and minutiae points are marked .This method extracts the minutiae from the thinned image. This method extracts the ridge endings and bifurcations from the thinned image by examining the local neighbourhood of each ridge pixel. Minutiae marking is generally done based on 2 ridge characteristic patterns. They are : Ridge bifurcation and Ridge ending. It would produce a better result when large number of minutiae points are detected and marked.

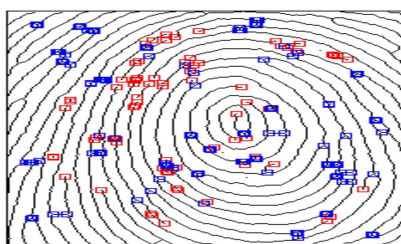


Fig 6: Minutiae marking

C. MATCHING STAGE

The matching stage is a process to compare two fingerprints images (input and template) and compute the similarity degree between them. It checks with the image that has been scanned with the one that has been already stored in the database. The matching algorithm is used to know either the two minutiae set from the same finger or from different finger . Generally, it returns true if the matching score is above the threshold value and false if score is less than the threshold value. Fig 8 shows how the matching stage is done. While enrolling the fingerprint, the features are extracted and are stored in the database. While verification , the fingerprint is scanned using a scanner and features are extracted and then matched with the prestored image database. Minutiae marking is done to match the images . This step produces a better result when larger number of minutiae are detected.

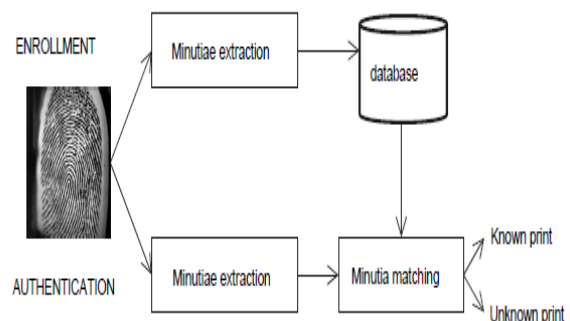


Fig 7: Images matched with Database

After the fingerprint matching stage , according to the result the voter is allowed to vote and the results are stored in the database to view the voted status once the election is over.

IV. OTP GENERATION

A one-time password (OTP) is a secret key or unique authentication key that is valid for only one login session or transaction, on a computer system or other devices. It is generated by Randomly picking characters from our all possibilities and generate a string of the desired length from it or by randomly deriving numbers using many inbuilt functions. OTPs are generally 6-7 characters long and randomness in 6-7 characters almost guarantees a secure way

of logging in. Also there are various ways of generating OTPs such as numbers and strings together or numbers alone.

Applications

1. Secretkeys are widely used in various websites like- Facebook, Google Sign-in, Account creation sites, Railways Portal Login etc.
2. Even the GeeksforGeeks has a unique string for all the codes compiled through it.

How it gets generated ?

Well it is a great possibility that they use the random function algorithm as an OTP is generated. If by chance (very rare) the secret key generated is already been generated before a while and has connection with a different code then another random string is used.

As per now it is noted that only four numbers are generated randomly for a unique identification of all codes. A time will come when all the possible four number combinations may get exhausted. So yes, even the web-related stuffs also heavily relies on randomness. The following code generates a secret or unique key.

Algorithm:

1. Create an object for Random function.

```
Random r1= new Random();
```

2. Generate Secret Key using inbuilt functions.

```
int ran = r1.nextInt();
```

```
double x = (double)ran/Integer.MAX_VALUE*6999
```

```
int secnum = (int)x + 2001;
```

```
secnum = Math.abs(secnum);
```

In this paper, once the user login to the system, the details of the user are verified and if the details are matched with any of the prestored data an OTP is sent to the user's mailid. Then, the user wants to enter his/her secret key to continue the process of voting. Once the user enters his secret key correctly, he/she will be directed to the voting page and the vote status of the user will be stored in the database.

V. PROPOSED SYSTEM

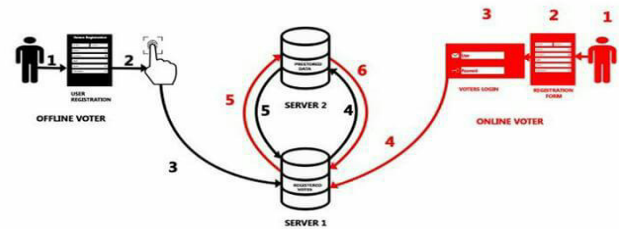


Fig 8: Flow Diagram of proposed system

A.ONLINE MODE

First, the voter must register his details along with his Aadhar number in the registration form. Then, he can vote from his comfort place by logging in through his registered Aadhar number. Once he enters his Aadhar number, the number is checked in the database and if it exists, an OTP (One time Password), a unique key will be sent to the voters registered email id. After entering the OTP, the voter can vote and the voted details are stored in another database. The following are the steps that explain the online voting process in the system architecture.

- ❖ **Step 1: User Registration:** In order to use the system, the voters must register to the system. This explains the registration process. The voter enters the website and a registration form will be opened.
- ❖ **Step 2: The Registration form:** In the registration form, the user enters the details such as name, Aadhar number, and other information. On clicking the submit button, the user will be successfully registered to the system.



Fig 8.1: User Registration

- ❖ **Step 3: User login:** In the login form ,the user must use his registered Aadhar number to login to the system.
- ❖ **Step 4: Cross Verification:** Once the user login, the system will cross verify that the user had already voted or not. The system will move to the server 2 to check whether the user had already registered his vote or not.
- ❖ **Step 5: Validation:** If the user did not registered their vote yet, then the server2 will search for the user's prestored details in the server1 such as the name, aadhar number etc., else an error message will be displayed to the user.This step will allow only the legitimate voter to vote and will not allow any voter to vote twice thereby increasing the security.
- ❖ **Step 6: OTP Generation:** In order to cast the vote the voter had to login to the site using valid credentials. The user have to enter his/her aadhar number to login. The system verifies the user details and will generate an OTP to the user's registered email id.
OTP is generated by using the algorithm that is defined above. It generates a four number combination keys which will be sent to the user's registered mailid. OTPs generally change for every session and it thus provides a better randomness thereby increasing the security measure.

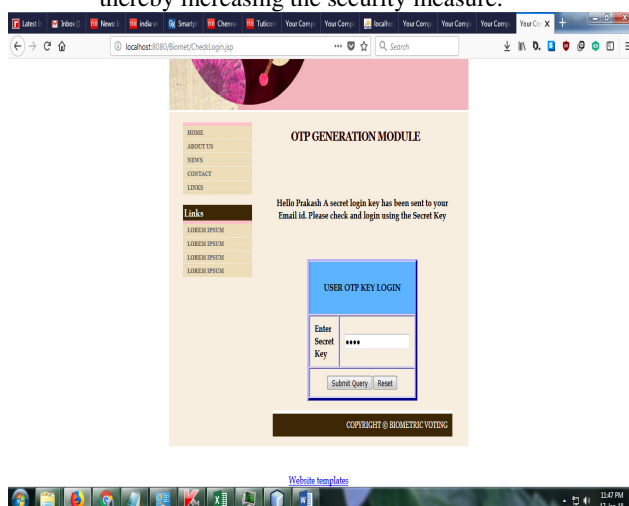


Fig 8.2: OTP Generation

- ❖ **Step 7: Vote Casting:** After the user enters his secret key to the system, the user can cast his/her vote to a candidate of their wish. Then the system will move to step 5.

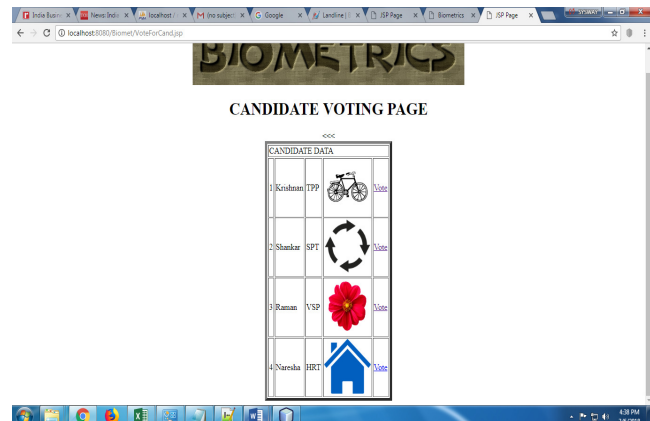


Fig 8.3: Voting Process

- ❖ **Step 8: Vote Counted:** If the system successfully completes the validation process and the given user details are genuine then the vote will be counted to the server1.The system will store the vote status that are registered by voters.

B.OFFLINE MODE

The voter must register his details along with his Aadhar number and Fingerprint in the registration form.In the poll,the voter must register his Fingerprint in a scanner device which is matched in the database to check the authenticity.If exists,the voter is allowed to vote and the voted details is stored in another database. The following are the steps that explains the offline voting process in the system architecture.

- ❖ **Step 1: User Registration:** The voter must register his details and the registered details are stored in the database.
- ❖ **Step 2: User Fingerprint Scanning:** In order to cast vote in offline mode the user have to move to the voting polls. The user have to scan their fingerprints in the biometric device available in the polls, then the system will move to the verification phase. .It is the process to obtain image by different ways such as Online and Offline

There are number of methods are used .In online method the optical fingerprint reader is used to capture the image of fingerprint . In other methods, the fingerprint image is obtained by ink in the area of finger and then put a sheet of white Paper on fingerprint and scan it to get a digital image.

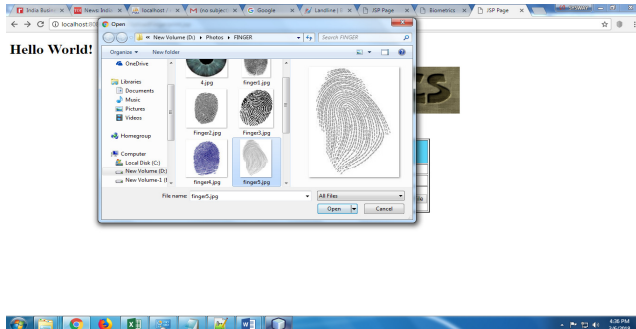


Fig 8.4: Fingerprint Uploading

- ❖ **Step 3: Cross Verification:** When the user scan his fingerprint, the system will cross verify that the user had already voted or not. The system will move to the server2 to check whether the user had already registered his vote or not.
- ❖ **Step 4: Validation:** If the user did not registered their vote yet, then the server2 will search for the user's prestored details such as the aadhar details and the registered fingerprint images in the server1, else an error message will be displayed to the user.

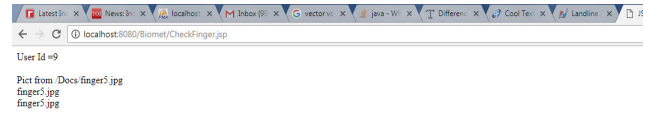


Fingerprint Not Matched You are Not Eligible

Uploaded Fingerprint File Data Details



Fig 8.5 (a) Fingerprint Verification (Not Matched)



Fingerprint Matched You are Eligible To Vote

[Click To Vote](#)

Uploaded Fingerprint File Data Details



Fig 8.5 (b) Fingerprint Verification(Matched)

- ❖ **Step 5: Vote Counted:** If the system successfully completes the validation process and if the scanned fingerprint match with the pre-stored data then the vote will be counted to the server1.

VI. CONCLUSION AND FUTURE WORK

This paper was an introduction to provide authenticity for the voter using fingerprint minutiae matching. It can be improved with every approach that are presented. The main improvements that can be done are given in the following list:

- Use another algorithm for correspondence based on human strategy when doing this, add more information in the feature vector (orientation for example)
- Use fingerprint classification to speed up the algorithm

To make the system more efficient, we have provided the people to vote from their comfort place using OTP sent to their email. But, Email seems to be time consuming, future work can be done in order to send the OTP to the voters mobile number and also we used ridge endings and bifurcations to match which is also time consuming, future work can be done based on the types of fingerprint which could result in less time consuming.

References

- [1]. J.Ravi,K.B.Raja,K.R.Venugopal,“Fingerprint Recognition Using Minutia Score Matching”,International Journal of Engineering Science and Technology, Vol.1 (2), pp. 35-42, **2009**.
- [2]. H. Costin, I. Ciocoiu, T. Barbu, C. Rotariu, “Through Biometric Card in Romania: Person Identification by Face,Fingerprint and Voice Recognition”, International Journal of Biomedical Sciences, Volume 1, Number 4, pp. 264- 269, **2006**.
- [3]. A.Tudosa,M.Costin,T.Barbu,“Fingerprint Recognition using Gabor filters and Wavelet Features”, Scientific Bulletin of the Politehnic University of Timisoara, Romania,Transactions on Electronics and Communications, Tom (49) 63, Fasc. 1, pp. 328-332,**2004**.
- [4]. <http://bias.csr.unibo.it/fvc2000/>.
- [5]. <http://bias.csr.unibo.it/fvc2002/>.
- [6]. S. Mazumdar, V. Dhulipala, "Biometric Security Using Finger Print Recognition", University of California, San Diego. 7 pages, Retrieved 30 August **2010**.
- [7]. Gabriel I,Oluwole A, Boniface A, Olatubosun O,” Fingerprint image enhancement:segmentation to thinning “, Department of Computer Science. Int J Adv Comp Sci Appl 3(1) **2012** .
- [8]. Manu Garg and Er. Harish Bansal, “Fingerprint Recognition System using Minutiae Estimation”, IJAIEEM, Volume 2, Issue ISSN 2319– 4847, 5 May**2013**.
- [9]. Amandeep Kaur and Ameeta, Babita,” Minutiae Extraction and Variation of Fast Fourier Transform on Fingerprint Recognition”.International Journal of Engineering Research and General Science Volume 2, Issue 6, October-November, **2014**.
- [10].Vaibhav Jain and Ajay Kumar Singh, “An approach for Minutia Extraction in Latent Fingerprint Matching”,International Journal,ISSN:2319–1058, Volume 6, No. 1 , pp. 51-58, October **2015**.
- [11]. Asker M. Bazen,”Fingerprint Identification - Feature Extraction, Matching, and Database Search”, Ph.D thesis from University of Twente, August 19, **2002**.
- [12] Ankit Anand,Pallavi Divya, "An Efficient Online voting system", International Journal of Modern Engineering Research (IJMER)www.ijmer.com Vol.2, Issue.4, July-Aug. 2012 pp-2631-2634ISSN: 2249-6645
- [13] Feras, Mutaz and Khairall, “New Applied E-voting system”, Journal of theoretical and applied Information Technnology 31st March 2011,vol:5 no:2.
- [14] . Chitresh Saraswat, Amit Kumar, “An Efficient Automatic Attendance System using Fingerprint Verification Technique”, International Journal on Computer Science and Engineering(IJCSE), Volume (2) : Issue (2) pp. 264-269, **2010**
- [15]. <https://en.wikipedia.org/wiki/Fingerprint>
- [16].Ajay Singh, “Fingerprint Identification using Real Minutiae Extraction method”
- [17].Ali,Vivek,Pravin,”Fingerprint Recognition for Person Identification and Verification Based on Minutiae Matching”, 2016 IEEE 6th International Conference on Advanced Computing.