Improved Voting System using two factor Biometric Authentication

Prerana Deokar[1], Samruddhi Dhake[2], Reena Kharat[3], P. Sanyasi Naidu[4], Bramhanand Chukalwad[5], Jayesh Amodkar[6]
[1,2,3]Computer Engineering Department Pimpri Chinchwad college of Engineering, Pune
[4,5,6]CSE Department, GITAM Institute of Technology, GITAM deemed to be University
reenakharat@gmail.com

Abstract— **The advancement in the mobile devices, wireless and web technologies has given rise to the new application that will make the voting process very easy and efficient. The E-voting promises the possibility of convenient, easy and safe way to capture and count the votes in an election. The abundance of security threats in e-voting systems and their increasing popularity makes a strong case for the need to propose new designs, protocols, techniques and tools for their design, development as well as their security assessment-voting minimizes the risk of ambiguities as the voter makes his choice by touching the screen. E-voting could also minimize the need for re-counts as everything is tabulated by the computer. In our proposed system we design website for E-voting (electronic voting). In order to prevent fraudulent voting the concept of Biometric Authentication (Face and Fingerprint) is used. Biometric is used to secure the voting system.**

In this paper, we will focus on biometric authentication techniques like fingerprint.

Keywords—***Biometrics, identification, verification, fingerprint, face .***

I. INTRODUCTION

An authentication strategy mistreats life science which will replace typical authorization mechanisms, especially passwords and private identification numbers (PINs), for higher security applications. The most risk of ancient authorization strategies is that passwords and Pins are unit sensitive to be purloined, guessed or retrieved by someone. Moreover, considering the number of net applications a client uses that need a countersign, it's tough for him/her to possess rely multiple and tough to be guessed passwords. On the opposite hand, life science utilizes intrinsic characteristics of someone and don't seem to be prone to fraud. Another advantage of biometric strategies over the normal ones is that the authentication isn't restricted to a binary call, therefore multiple levels of security is expose. Every biometric authentication has two phases: identification and verification. It can also be stated as feature extraction and feature matching.

II. FINGERPRINT

Fingerprint recognition refer to the automatic method of verifying a similarity between two human fingerprints Attributes such as size, cost, operating environment, reliability, accuracy and speed help determine the suitability for many applications.

Without testing each of these biometric recognition methods, a case can be made that fingerprint recognition has the broadest applicable for most systems and is the best place to begin a search for an appropriate biometric. The use of fingerprint recognition has existed as a means of identification for many years. Not only fingerprints are more usable, but also fingerprint recognition systems generally have low costs, fast speed, and maximum reliability compare to other biometric recognition methods Fingerprints are commonly classified as 5 different types such as: whorl, left loop, right loop, arch, and tented arch. Minutia detection algorithm, Coherence method of detection and many more methods, each algorithm is having the different advantages and disadvantages over one another.

A fingerprint is a flowing pattern on the fingertip of a person consisting of ridges and valleys. Ridges are black lines. Valleys are white space between ridges.Fig.1 shows the image for thumb print which is used in the process of recognition.

1. Approach and methods*:*

Generally fingerprint identification and recognition system consist of 8 main parts: Fingerprint Image Acquisition (Collecting fingerprints)

- Fingerprint feature Extraction

Histogram Equalization, Enhancement Using FFT, Binarization, Minutia Marking.

- Align And Match Template, Save Template

2. Fingerprint Image Acquisition:

In this stage, fingerprints samples are taken manually, as there is no fingerprint detector or scanner available. A small daub of ink is placed on the inking slab and thoroughly rolled until a thin and even film of pigment men the entire surface of the inking slab. Then the bulb of the finger is placed at the right angle to the surface of the inking slab and rolled until the bulb of the finger is evenly inked. The inked finger is impressed on a piece of white paper until satisfactory fingerprint is obtained. Various fingerprint samples are taken from different individuals in order to create a collection of fingerprints patterns available.

Fingerprint image acquisition for database:
In this section, only the useful area of the digitized fingerprint image (PEG format) acquired in the earlier section would be selected and edited to the size of 256 x 256. The flowchart of this process and its implementation results are shown in Figure 2

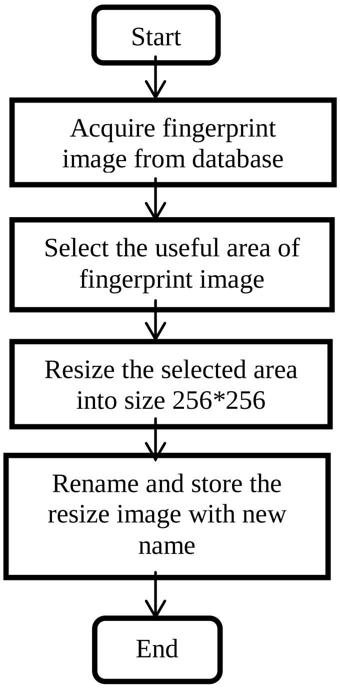

Start
Acquire fingerprint image from database
Select the useful area of fingerprint image
Resize the selected area into size 256*256
Rename and store the resize image with new name
End

Fig.2 Fingerprint Flowchart

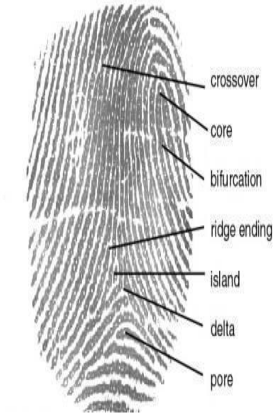
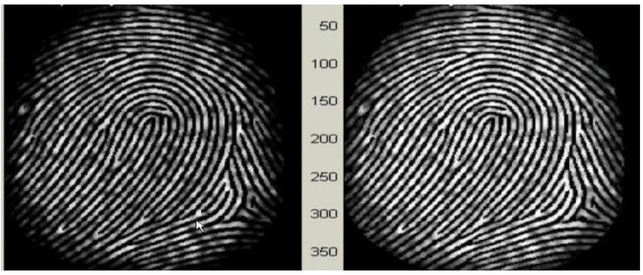


Fig.1 Minutia Markings

2.1 Histogram Equalization:

Histogram equalization is mainly used to increase the pixel value of an image so that the perception information also increases. It is shown in figure 3. Histogram represents the relative frequency of various types of grey levels in an image. By using this method we can improve the contrast of an image and it is one of the most important techniques in image enhancement.



(1) **(2)**

Fig.3 (1) Original Image
(2)Enhanced Image after Histogram Equalization

2.2 Enhancement Using FFT

Here first of all we divide the **images** into different small processing blocks those are of 32 by 32 pixels then use the Fourier transform according to formulae:

Enhancement by Fourier transformation:

The image enhancement by FFT is done by the following formulae $(x, y) = F^{-1}\{F(u, v)\times F(u, v)^{k}\}$

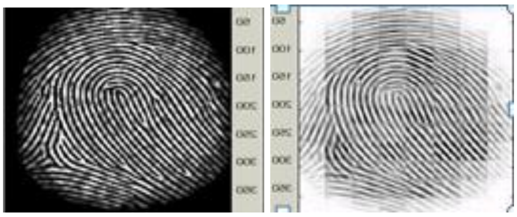


Fig 4. Enhanced Image using FFT

Fig.4 shows the Enhancement of the image using FFT. To enhance those small processing blocks through its dominant frequencies, we multiplied the FFT of the block with its magnitude a set of times.

1.1 Binarization:

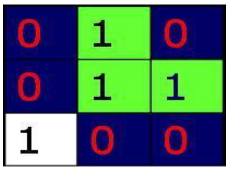
Image Binarization is the method is basically use to lighten or increase the sharpness of the given image. In case of image Binarization we initially binarize the image by extracting the lightness of the image that is here we extracts the brightness and densities of the images as a feature amount from the

images. When we select a pixel in an image, a sensitivity is added to it and it is subtracted from the value of Y the selected pixel because here we have to set the range of threshold value.

Next, when a new pixel is selected again a new threshold value range is set which contains the calculation result and the previous threshold value. Then the pixels are extracted up to the same brightness whatever the selected pixel and the extraction results is displayed on to the screen. Fingerprint Image Binarization is used to transform the 8-bit Grey fingerprint image to a 1- bit image and here the value for the ridges is 0 where as it is 1 for the furrows. After this operation, the various ridges in the fingerprint will be highlighted with black color while furrows will be color with white.

2.4 Minutia Marking

After completion of fingerprint Binarization process, a minutia marking is performed by using 3 x3 pixel window as follows. In case of minutia marking the concept of Crossing Number (CN) is generally and widely used.



0	1	0
0	1	1
1	0	0

Fig.5 Minutiae Branching

2.5 Align and Match Template

After testing the various types of minutia set of points of two finger print image we perform Minutiae Matching operation to check whether they belong to the same person or not. It includes two consecutive stages such as: Alignment stage, Match stage

2.5.1 Minutiae alignment

Alignment stage can be done by :

I1={m1,m2,..mM}
where mi =(xi,yi,)
I2={m'1,m'2,..,m'N}
where m'i=(x'i,y'i)

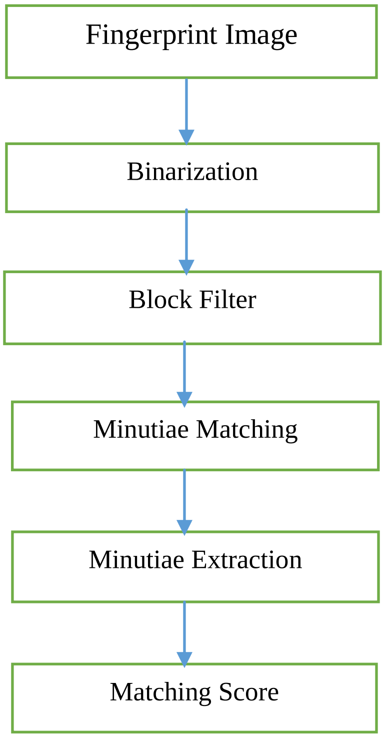
$$S=\frac{\sum i=0xiXi}{\sqrt{\sum i=0xiXi}}$$

2.5.2 Match stage

$$\text{Match Score}=\frac{\text{Number of total matched minutiae pair}}{\text{Number of minutiae of fingerprint}}$$

If the matched score is greater than a threshold value which is prespecified, then the two fingerprints taken are from the same finger.

The following model is used to match the test fingerprint with the template database using Minutiae matching score.



Fingerprint Image*:* The input fingerprint image is the gray scale image of a person, which has intensity values ranging from 0 to 255. Minutiae points are the locations where a ridge becomes discontinuous. A ridge can either come to an end, which is called as termination or it can split into two ridges, which is called as bifurcation.

Binarization: The pre-processing of FRMSM uses Binarization to convert gray scale image into binary image by fixing the threshold value. The pixel values above and below the threshold are set to '1' and '0' respectively.

Block Filter: The binarized image is thinned using Block Filter to reduce the thickness of all ridge lines to a single pixel width to extract minutiae points effectively. Thinning preserves outermost pixels by placing white pixels at the boundary of the image, as a result first five and last five rows, first five and last five columns are assigned value of one.

Minutiae Extraction: The minutiae location and the minutiae angles are derived after minutiae extraction. The terminations which lie at the outer boundaries are not considered as minutiae points, and Crossing Number is used to locate the minutiae points in fingerprint image.

Minutiae Matching: To compare the input fingerprint data with the template data Minutiae matching is used. For efficient matching process, the extracted data is stored in the matrix format.

Algorithm:
1. Pre-processing the test Fingerprint.
2. Extract the minutiae points.
3. Matching test Fingerprint with the database.

III. FACE

Face Recognition System can act as the other form of authentication system. So we propose the Face Recognition System (FRS) to avoid such kind of problems in the real life and to provide the security to system at greater level. FRS doesn't require remembering the password as face is always carried by user and every person is having unique face.

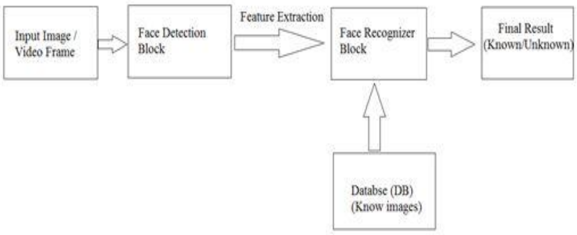

Input Image / Video Frame
Face Detection Block
Feature Extraction
Face Recognizer Block
Final Result (Known/Unknown)
Databse (DB) (Know images)

Fig.6 Face Recognition System

1. **Image frame**-Input given to system.
2. **Face Detection**-This block is used to detect the faces in a given image by using the Haar cascade Feature based identifier. Haar cascade feature based identifier is the best technique used to detect the object in a image, and commonly used today

Face recognizer:-This block is used to identify the face which is detected in the previous stage. This block uses the PCA algorithm to recognize the face. Features extracted from the given image by PCA algorithm are compared with those of known images stored in the database.

4. **Database**-This is the Database having the known images.

5. **Result block**-This is the final stage in face recognition whether to give access or not to a user is decided by this block.

Fig 7: Eigen face database

A. Procedural approach

Step 1: Get data

Here data provided to the system is the image captures from the video frame, these images are converted into the gray scale images and different operations are performed on these image vectors to show what the PCA analysis is doing at each step. We are working with the gray scale image rather than the directly working with color image so memory requirement for storing the images in database is also reduced at some extent. And the speed of processing becomes faster.

Step 2: Normalization

Here the mean image is calculated and from each image mean is subtracted in order to obtain the unique feature from each image. Due to normalization best unique features database is created. Which is further used in the process of face recognition?

Step 3: Calculate the covariance matrix

Suppose the image is of size N*N, then convert the image into one column called image vector of size N^2*1 that means image vector is having N square rows and one column.

Converted image vector space N^2*1 is used for the calculating the covariance matrix. Suppose A is set of all unique features .i.e. image vectors A = $\{\Phi 1, \Phi 2, \Phi 3 \ldots \Phi M\}$

Then Covariance can be calculated as, Covariance = $A.A^T$.

So size of Covariance matrix would be
$(N^2*1) * (1* N^2) = N^2 * N^2$

Step 4: Calculate the eigenvectors and Eigen values of the covariance
Matrix

If we see the size of the covariance matrix ($N^2 * N^2$) which will be very large for images and becomes the huddle for processing. So dimensional reduction technique is used to improve the performance of the system ex. Memory requirement will be less when dimensional reduction technique is done. Since the covariance matrix is square, we can calculate the eigenvectors and Eigen values for this matrix. These are rather important, as they tell us useful information about our data. Eigen values calculated by taking the common multiplier of the image vector and final obtained image vector is the Eigen vector which is having the unique feature.

$$A= \begin{bmatrix}2\\8\\4\\6\end{bmatrix}$$ A is image vector having size N^2*1

Then, by taking the common multiplier

$$A= 2 \begin{bmatrix}1\\4\\2\\3\end{bmatrix}$$

This is how the size is reduced for all the image vectors, as this is the small matrix but in case of images having large matrix this will definitely help.

Step 5: Weight vector

Consider one person is having the at least 10 images with the variations in the expression, position etc. The for each image

Eigen values and Eigen vectors are calculated and finally the weight vector of the Eigen values of all the images are formed .This weight matrix is used for the comparison. Some threshold value is calculated and stored into the database.

Step 6: Face recognition decision

Whenever there is image for face recognition, corresponding weight vector is calculated if the value is above the threshold value then face recognized and corresponding information about that face is display. And if the value is less than threshold value then face is not recognized, may be the person is new .These six major steps have to follow in order to recognize the face using principal component analysis

IV. PROPOSED SYSTEM

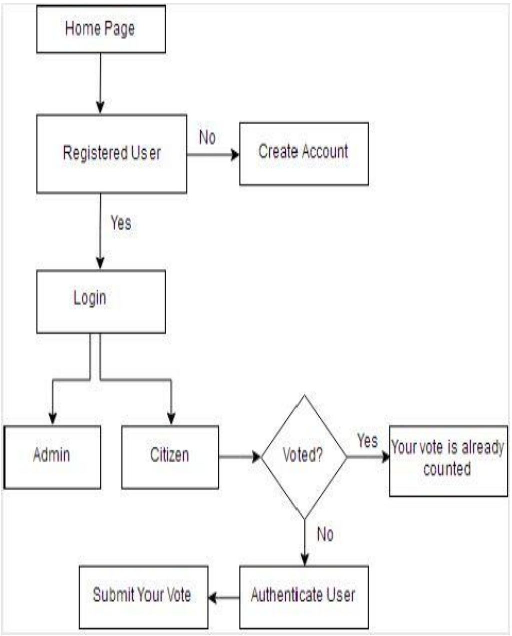


Fig 8.Proposed System

In “Online Voting System Using Biometric Security” architecture of the system is based on functionality provided to different users by the system. The three users of system and their task are:

1) Citizen

- **Registration of voting card**

General public can request for access voting rights. Citizen will be able to apply for voting card by submitting his details online or at the electoral office. In order to get registered in the voting list, he will have to enroll his finger print image at the electoral office along with his documents.

- **Online voting**

He can vote to desired candidate and see the result online, in case he has access to internet and a biometric device.

- **Citizen's Forum**

He can get information regarding the electoral process, his rights and duties and interact with the leader parties through a forum.

2) Admin

Add registered & unregistered users after verifying the documents and scanning the finger print image.

Statistical analysis of registered citizens and number of votes and result declaration. In order to use the system every user must have to register first and so they have a unique username and password, which enable different users to use the functionality provided to them by the system.

V. CONCLUSION

After implementation of this project we can change face of today's traditional voting system making it more secure and corruption less. It will give a fare chance to every leader to win on the basis of his/her capability and not on the basis of strength of money and power. The scope of the project to raise to the society, institutional or nations level by using a more secure and efficient database management system that could handle hundreds, thousands or billions of users.

VI. REFERENCES

[1] Ravi. J, k. B. Raja, Venugopal. K. R, "Fingerprint recognition using Minutia score matching", International Journal of Engineering Science and Technology Vol.1 (2), 2009, 35-42.

[2] Trupti Umakant Pavshere, S.V.More, "Secured E-Voting System Using Bio-metric", ISSN: 2350-0328 International Journal of Advanced Research in Science, Engineering and Technology Vol. 3, Issue 3, March 2016.

[3] Alaguvel.R 1, Gnanavel.G2, Jagadhambal.K, "Biometrics using Electronic Voting System with Embedded Security."

ISSN: 2278 1323 International Journal of Advanced Research in Computer Engineering Technology (IJARCET) Volume 2, Issue 3, March 2013.

[4] Kevin Daimi and Katherine Snyder, Robert James, "Requirements Engineering for E-Voting Systems", University of Detroit Mercy, St 600 Detroit, Michigan 48219, USA.

[5] Anshul Gupta, Nileshkumar Patel, Shabana Khan," Automatic Speech Recognition Technique for Voice Command", IEEE-32331.

[6] Alaguvel.R 1, Gnanavel. G 2, Jagadhambal.K, " Biometrics using Electronic Voting System with Embedded Security", ISSN: 2278 1323 International Journal of Advanced Research in Computer Engineering Technology (IJARCET) Volume 2, Issue 3, March 2013

[7] Srivatsan Sridharan," Implementation of Authenticated and Secure Online Voting System", IEEE - 31661Pimpri Chinchwad.