Smart India Cloud base Online Booth Polling System using Adhar Card

Dheivani P,
B.E. (Computer Science and Engineering),
Government College of Engineering,
Thanjavur, India

Vinitha D,
B.E. (Computer Science and Engineering),
Government College of Engineering,
Thanjavur, India

Yuvaraj D, B.E. (Computer Science and Engineering),
Government College of Engineering,
Thanjavur, India

Gayathridevi M, Assistant Professor (TF),
Government College of Engineering,
Thanjavu r, India

***Abstract*— The way of e-Governance in India from 2006[National e-Governance Plan (NeGP)] has planned to transform India into a digitally empowered society and knowledge economy. The paper will give an overview of Online Booth Polling System which will access the data stored in the database of Adhar card, a government id card for each citizen in India, while casting their votes. While issuing the Adhar card a citizen of India needs to give his/her unique biometric data. In this concept, the voter can vote from anywhere in booth and no need to be in native. In order to provide authentication, the voter's biometric details are matched and verified. This proposed system can eradicate duplicate voting in several elections in India, and to get transparent election in future.**

Keywords- e-Governance, Booth Polling System, biometric data, digitally empowered society

I. INTRODUCTION

Election is a basic idea for selecting the leaders among the parties of people as the representative of the country. Based on the democracy, selecting leader is independent for every individual citizen of the country but is major and difficult task.

Voting is a right for every citizen and it is not a new process. In traditional system, Kings and other Ministers are selected by the people by using the method "KUDAYOZHAI"system, where the people select their representative independently [1].

In 1947, the leaders are selected on the basis of democracy. It is termed as "for the people, of the people and by the people". During this period, election was carried out with "ballot paper with rubber stamp" where the people elect their votes in polling stations.

In 1998, the constitution of India developed the "electronic voting machine" instead of ballot boxes. Critics of electronic voting argue about the security issue, the unequal access and vulnerable to security.

In India All six municipal corporations of Gujarat: Ahmadabad, Vadodara, Surat, Rajkot, Bhavnagar and Jamnagar offering online voting started online voting To avail the online voting, firstly voters register through website[2]. Citizen ID's and Password will be provided by council of election commission only, means no sign up link on the website. A citizen can change his password. Main drawback of the system is to use same device for voting means lacking the facility voter can cast from anywhere.

To get rid of these serious problems, Online Booth Polling System can be used for any election procedure which will achieve and attain the highest possible privacy and security while casting the vote by a voter. The description of paper is following as 2.Online booth polling system, 3.Biometric detection, 4.Authentication of polling system and 5.Conclusion

II. ONLINE BOOTH POLLING SYSTEM

Every single person in the world has unique fingerprint, iris, and facial dimension. In order to provide authentication, the OBPS allow the voter to scan his/her biometrics (fingerprint, iris, facial dimension) .The scanned biometric details are verified with the biometric details which is already stored in the database called Adhar database[Fig 1]. Then the authorized user is allowed to vote. When the voting process is over, the machine can automatically stores the vote in the separate database i.e. polling database, so the counting of votes will be made easy. After polling of vote, the particular details of the voter will be hiding temporarily to avoid polling of duplicate voting.

A. Modes of Polling System

The proposed system mainly works in online mode and has two modes namely as follows [3]

1. User Mode

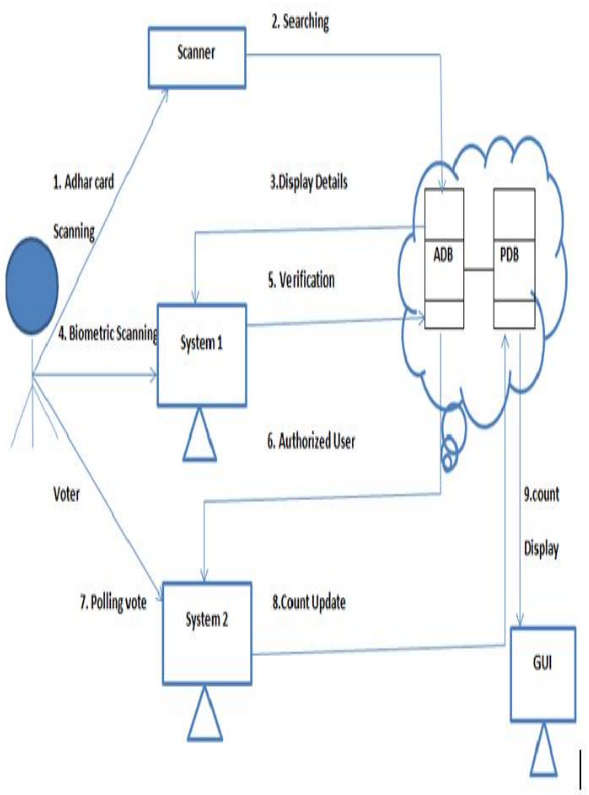
This mode is for general voters. At first, the voter's need to scan the adhar card. If the age of the voter is below 18, the system displays the particular voter's details along with the message "you are not eligible to vote". If the age of the voter is equal to or greater than 18, the system displays the particular voter's details and proceeds by scanning of fingerprint, iris and facial dimension.

If the current biometric details are matched correctly with their biometric details stored in the adhar database, then the voter can vote in the system which is designed by "Graphical User Interface". After polling of vote, the particular voter's details will be hidden from the Adhar database so as to avoid duplicate voting.

Among the three biometric details, if any one of the biometric either fingerprint or iris or facial dimension is not matched, then the voter cannot be able to vote.

Thereby the voting count will be stored automatically in the polling database separately which makes easy of vote counting and avoids retraceability of votes.

Fig 1. Architecture of online booth polling system



2. Admin Mode

In this proposed system the officials of Election Commission of India play the role of admin of the system. For the authenticity of the admin, the system will seek the fingerprint, iris, facial dimension after scanning of the adhar card. Only admin should maintain both the databases i.e. “Adhar database”, where the biometric details and their personal details are stored and “Polling database” where the polled votes are stored.

The Admin of the system can

A. View the Result

The system gives the facility to the admin to view the result of the election by fetching the vote result from the “Polling database”.

B. Check the Non Polling Voters

The admin can see the adhar number of the people who have not casted their votes. After casting of vote, the system can hide the voter’s particular details from the adhar database. So, those persons who have not casted their votes, their details will not be hidden from the adhar database. The system searches for these persons and show their name and adhar card details to the admin.

C. Delete the vote related data

The admin can delete the previous election data in the “polling database” from the system. This is needed to clean up the databases and to make the system ready for next election. The admin can delete the previous election data in the “polling database” from the system. This is needed to clean up the databases and to make the system ready for next election.

D. Insert people data

In every year, huge amount of people are issuing adhar card. To include their details in the adhar database, this system provide another facility to the admin.The officers of the Election Commission can insert the details of the new adhar card issuers directly into the Adhar database. The system will seek all the personal details along with their biometric details [fingerprint, iris, facial] of the adhar card issuer. Then it will process the data and store it into Adhar database

The scanning of biometric details is explained as follows:

III. BIOMERIC DETECTION

A. Fingerprint recognition

Fingerprint recognition has been widely used in both forensic and civilian application [4]. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip. The endpoints and crossing points of ridges called minutiae. It is widely accepted that minutiae pattern of each finger is unique and does not change during one’s life. When human fingerprint experts determine if the two fingerprints are from the same finger, the matching degree between two minutiae pattern is one of the most important factors[5]. The algorithm used in this paper belong to the minutiae based matching method

1) Minutiae Based Matching:

Let T and Q be the feature vectors, representing minutiae points, form the template and query fingerprint. Each element of these feature vectors is a minutiae point, which may be described by different attributes such as location, orientation, type, quality of the neighborhood region etc[Fig 2].The most common representation of a minutiae is the triplet x, y, Ө where x,y is the minutiae location and Ө is the minutiae angle [6]. Let the number of minutiae in T and Q is m and n

$T=m_{1,}$ $m_2,$ m_3………………………..m_m
$m_i=x_i,y_i,\Theta_i$,i=1, 2, 3,…………………..m
$Q=m'_{1,}$ $m'_2,$ m'_3………………………..m'_m
$m_j=x'_i,y'_i,\Theta'_i$,j=1,2,3,…………………..n

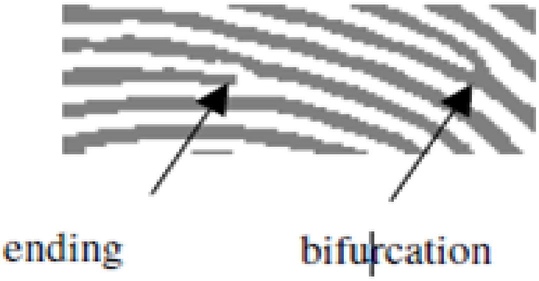
A minute m_i in T and m'_j in Q are considered matching,

$$\mathbf{sd\ (m'_j,m_i)} = \sqrt{(x'i - xi)^2 + (y'j - yi)^2} \ \ <= \mathbf{r_0}$$

$$\mathbf{dd\ (m'_j,m_i) = min\ (|\Theta'_j - \Theta_i|, 360-|\ \Theta'_j - \Theta_i|) <= \Theta_0}$$

Here r_0 and Θ_0 are the parameters of the tolerance window which is required to compensate for errors in feature extraction and distortions caused due to skin plasticity. The number of “matching “minutiae points can be maximized, if a proper alignment between query and template fingerprints can be found. Correctly aligning two fingerprints require finding complex geometrical transformation function (map ()), that maps the two minutiae set (Q and T) the desirable characteristics of Map () functions are: It should be tolerant distortion [7]; It should recover rotation, translation and scale parameter correctly.

Fig 2. Minutiae based matching



B. Face Recognition

The technique used for face recognition is feature based technique. This technique can extract the facial features and use them to classify faces. The recognition system should be robust enough to classify the face. The front view and side view are two important aspects of face [8].

The front view should provide feature such as the distance between the left and the right iris centers, the two inner eye points, the two outer eye points, the eye center and the nose tip, the iris center and the eye brow for both the eyes, and the face width. The side view of the face can also be taken. The feature can be extracted are nose point, chin point, forehead point, bridge point, brow point and the distance between the lip bottoms to the lip curve. The distance feature such as face to forehead, nose to bridge,nosetip to nose bottom, brow to chin, brow to bridge and nose to chin can be deduced from the face.

Once the features are extracted, a feature table can be constructed. The Bayesian classifier can then be used for classification.

1. Bayesian Classifier

It is based on the Bayesian theorem It is particularly suited when the dimensionality of the inputs is high [9].

a. Bayes Theorem

Bayesian reasoning is applied to decision making and inferential statistics that deals with probability inference [11].

Algorithm for Bayes Theorem

Step 1 It is loaded the image which will be classified as being ONE, TWO or THREE

Step 2 There are loaded the images found in the folder images. The name of the files belonging to class ONE are: “image1_*.jpg”, the ones belonging to class TWO are: “image2_*.jpg” and the ones for class THREE are: “image3_*.jpg”.

Step 3 It is determined the a priori probability for each class:
P(UNU)=NrTemplateInClassONE/NumberTotalTemplates
P(DOI)=NrTemplateInClassTWO / NumberTotalTemplate

P(TREI)=NrTemplateInClassTHREE/NumberTotalTemplate

Step 4 It is determined the probability that the image from the Step 1 to be in class ONE, TWO or THREE. Let (i,j) be the position of a white pixel in the image. It is calculated the probability that the pixel having the coordinates (i, j) to be white for the class ONE, TWO and THREE.

```
count1i, j = 0
for k = 1, n; n – the number of images in class ONE
if image1_k (i,j) = 255 then
count1i,j = count1i,j + 1
probability1 (i,j) =count1i,j / NrTemplateInClassONE
count2i, j = 0
for k = 1,n ; n- the number of images in class TWO
if image2_k (i,j) = 255 then
count2i,j = count2i,j + 1
probability2 (i,j) =count2i,j / NrTemplateInClassTWO
count3i,j = 0
for k = 1, n; n- the number of images in class THREE
if image3_k(i,j) = 255 then
count3i,j = count3i,j + 1
probability 3(i,j) =count3i,j / NrTemplateInClassTHREE
```

Step 5 The posteriori probability that the image in Step 1 to be in class ONE is:
P (T|ONE) = average (probabilitate1 (i,j)); (i, j) – the position of the white pixels in the image from Step1

Step 6 The posteriori probability that the image in Step 1 to be in class TWO is:
P (T|TWO) = average (probabilitate1 (i,j)); (i, j) – the position of the white pixels in the image from Step1

Step 7 The posteriori probability that the image in Step 1 to be in class THREE is:
P (T|THREE) = average (probabilitate1 (i,j)); (i,j) – the position of the white pixels in the image from Step1

Step 8 It is determined the probability P for each image class and it is assigned the image from Step1 to the class of images that has the greatest probability.
P (ONE|T) = P (T| ONE)*P (ONE)
P (TWO|T) = P (T| TWO)*P (TWO)
P(THREE|T) = P (T| THREE)*P (THREE)

It is used the knowledge of prior events to predict future events.

P (h/D) = P (D/h) P (h)/ P (D)
P (h): Prior probability of hypothesis h
P (D): Prior probability of training data D
P (h/D): Probability of h given D

P (D/h): Probability of Ds given h

C. *Iris Recognition*

The colored ring surrounding the pupil in the human eye is called iris. The iris is unique between the left and the right eye of the same person [10]. Therefore iris recognition can be a powerful technique for identification purpose. The relative advantage of iris recognition systems is its low false positives, relative fastness in recognition and the ease of use.

The steps of recognition process are

1. Image acquisition
2. Iris localization
3. Pattern recognition

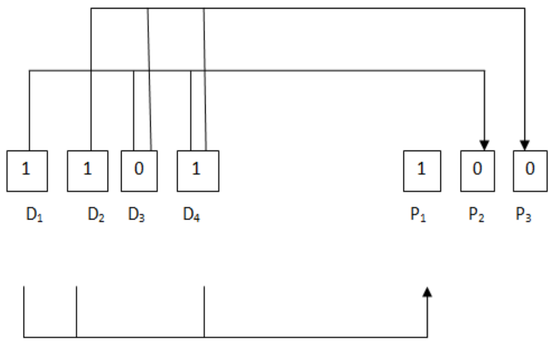
The first step involves the use of iris scanner for capturing the image of the retina. In the second stage, active contour models are used to segment the iris. In the localization process, the surrounding eyelashes are removed using histogram analysis and statistical inference[11].

Iris recognition is used in 1: M identification mode. In the third stage, the test iris is validated with the library of the stored patterns by the matching process. The iris matching process involves the hamming code distance and the result is normalized to prevent false positives.

1) Hamming Code Distance

The Hamming code is used to produce parity check data as the authentication message [12]. The Hamming code is a kind of forward error correction (FEC). That means the receiver has ability to correct a transmission error according to the code itself. Therefore, it comes in quite handy when there are data to be transmitted in a noisy environment. To have this ability, some bits must be appended to the original data [13]. The appended bits are called parity check bits. Generally speaking, the Hamming code has the ability to correct single-bit errors and detect two-bit errors [Fig 3]. The basic idea of the Hamming code is the concept of parity check.

Fig 3.Data bits and Parity check bits



The Error Detection and Correction Rules:

i. If a code can detect‘t’ number of errors, then its minimum hamming distance must be t+1.

ii. If a code can correct‘t’ number of errors, then its minimum hamming distance must be 2t+1

In order to correct the corrupted bits at the receiver, the following two variables must be known at the receiver.

1. Position of the bits corrupted.
2. The original value of the bits.

IV. AUTHENTICATION OF POLLING SYSTEM

This paper considers a Public Key encryption method using RSA algorithm that will convert the information to a form not understandable by the intruder his paper considers a Public Key encryption method using RSA algorithm that will convert the information to a form not understandable by the intruder . This paper considers a Public Key encryption method using RSA algorithm that will convert the information to a form not understandable by the intruder his paper considers a Public Key encryption method using RSA algorithm that will convert the information to a form not understandable by the intruder .

The RSA Algorithm for Creating RSA Public and Private Key Pair:

The RSA algorithm can be used for both key exchange and digital signatures. Although employed with numbers using hundreds of digits, the mathematics behind RSA is relatively straight-forward.

.

To create an RSA public and private key pair, the following steps can be used:

Step 1 Choose two prime numbers, p and q. From these numbers you can calculate the modulus, **n=pq**

Step 2 Select a third number, e, that is relatively prime to (i.e.it does not divide evenly into) the product (p-1) (q-1), the number e is the public exponent.

Step 3 Calculate an integer d from the quotient **(ed-1)/ (p-1) (q-1).** The number d is the private exponent.

Step 4 The public key is the number pair (n, e). Although these values are publicly known, it is computationally infeasible to determine d from n and e if p and q are large enough.

Step 5 To encrypt a message, M, with the public key, creates the cipher-text, C, using the equation:
C=M ^{e} Mod n.

Step 6 The receiver then decrypts the cipher-text with the private key using the equation:
M=C ^{d} Mod n.

V. CONCLUSION

This paper is the maiden overview of the Online Booth Polling system will pave the way towards smart India and to achieve hundred percent votes. Duplicate of voting will be eradicate and make vote easy. Single window voting system can also be implemented .The future work can also continue by enhancing more advance security algorithm and techniques.

.

REFERENCES

[1] Tadayoshi Kohno,Avan Studblefield,Aviel D.Rubin,Dan S.Wallach, "Analysis of an Electronic Voting System," IEEE Symposium on Security Privacy 2004,IEEE computer Society Press, May 2004,Feb 27 2004.

[2] Anooja A, Internet Voting System and Digital India. International Journal Of Emerging Trends and Technology in Computer Science, Volume 5, Issue1,January-February2016

[3] Soumyajit Chakra borty, Siddhartha Mukherjee, Bhaswati Sadhukhan, Kazi Tanvi Yasmin ,Biometric Voting System using Adhar card in India, International Journal of Innovative Research in Computer and Communication Engineering ,Volume 4,Issue 4,April 2016.

[4] Sangran Bana and Dr.Davindran Kaur, "Fingerprint Recognition using Image segmentation," International Journal of Advanced Engineering Science and Technologies (IJAEST), Volume 5, Issue No 1,012-023.

[5] Iwasokun Gavriel Bavatunde, "Fingerprint Matching using Minutiae – Singular points Network,", Internaional Journal Of Signal Processing, Image Processing and Pattern Recognition, Volume 8 ,No 2(2015,PP.375-388)

[6] Weiping Chen and Yongsheng GAO"A Minutiae based Fingerprint matching algorithm using phase Correlation", Digital Image Computing Techniques and Application.

[7] Deepika Sahu, Rashmi Shrivas, "Minutiae based Fingerprint Matching For Identification And Verification", Internaional Journal Of Science And Research (IJSR) ISSN(Online):2319-7064.

[8] Faizan Ahmad,Aaima Najan and Zeeshan Ahmed, "Image Based face Detection and Recognition," IJCSI International Journal of Computer Science Issues, Volume 9,Issue 6,No 1,Nov 2012,ISSN(Online):1694-0814.

[9] Mohamed Hechama,Agnes Desolneux and Frederic J.P.Richard, "A Bayesian Technique for Image Classifying Registration", IEEE Transaction On ImageProcessing, TIP-08569-2012.R1, May 2012.

[10] Gao Xiaoxing,Feng Sumin,Cui Han, "Enhanced Iris Recognition Based On Image Match And Hamming Distance," International Journal on smart Sensing And intelligent Systems,Vol 8,No 2,June 2015.

[11] Khattab M.Ali Alheeti, "Biometric Iris Recognition based on Hybrid Technique," International Journal on Soft Computing (IJSC), Volume 2, No 4, Nov 2011.

[12] Jerome Landre, Frederic Truchetet, "Image Retrieval with Binary Hamming Distance.

[13] Chi Shiang Chun,Chin Chen Chung, "An Efficient Image Authentication Method Based On Hamming Code," Journal of the Pattern Recognition Society.

[14] Nentawe Y.Goshwe, "Data Encryption and Decryption using RSA Algorithm in a Network Environment," IJCSNS International Journal of Computer Science and Network Security, Volume 13, No 7, July 2013.