ISSN 2395-1621

A Secure E-Voting System Using Face Recognition and Dactylogram

[#1]Patil Rahul H., [#2]TarteBabita B., [#3]Wadekar Sapana S., [#4]Zurunge Bhakti S.,
[#5]Prof. Phursule Rajesh

[1]rp.patil518@gmail.com
[2]tartebabita@gmail.com
[3]sapana.wadekar@gmail.com
[4]bhaktizurunge@gmail.com

[#1234]Student at JSPM's ICOER,Wagholi, Pune - 412207, India.
[#5]Prof. Phursule Rajesh, Computer ICOER

ABSTRACT

An E-voting system is a selection system in which the election data is recorded, stored and processed primarily as digital information. E-Voting system helps common man to opt for their representatives more firmly and articulate their preferences for how they want to be governed. India is a democratic country which plays a very important role in the development where the populace decides and put back the government by the means of voting. This process is all about needs of man power and resources. Our project implemented a safe and resonance system by using powerful biometric methods such as face recognition and fingerprint. E-Voting is a public voting system that would be deployed to make election process system which will provide secure, speedy, crystal clear and competent. All the questions like time delay for vote counting, security, false and duplicate voting addressed through this project. The main idea behind this project is to provide additional security using different biometric techniques such as face recognition and dactylogram.The fingerprint section was already stored up in the government record. Hence this project provides a best way to avoid the forged voting. The fingerprint scanner is connected to the machine having database of the people who is having eligibility to vote. Once voting is done by voter, status is updated for that particular person. So duplicate voting is avoided. For giving additional security face recognition technique is added which capture image and match with the image stored in the database. So, this project mainly provides extra security to voter.

ARTICLE INFO

Article History

Received :16th April 2016

Received in revised form :

19th April 2016

Accepted : 21st April 2016

Published online :

27th April 2016

Keywords:Election-Voting System, Secure E-Voting, Face Recognition, Dactylogram.

I. INTRODUCTION

Today, the researchers of computer science are focusing on E-Voting system to find out something motivating that will able to make the voting system more secure, speedy and prohibited. E-Voting system helps common man to opt for their representatives more firmly and articulate their preferences for how they want to be governed. India is a democratic country which plays a very important role in the development where the populace decides and put back the government by the means of voting. This process is all about needs of man power and resources. Election provides a opportunity to the citizens to choose leader by recording his or her secret ballot by some electronic means, therefore it must be perfect and transparent.

Problems like unauthorized privilege escalation, incorrect use of cryptography, vulnarabilities to network threats addressed in paper.[1] Also, E-voting system is more susceptible than traditional voting as election data is stored in digital format which can be easily manipulated, hence may result in widespread fraud and corruption [2]. To avoid such types of drawback biometric is integrated with password security to voter accounts [3]. Next to this technique, IRIS recognition is considered to be the most precise and consistent biometric identification system for E-voting [4].

With all the problems Mobile voting technique is proposed focuses on the mobile technology with the use of biometrics encryption for authentication [5]. To make the voting system reliable is very hard just because it requires elevated security necessities, confidentiality and integrity. Also we have to focus Fairness, Eligibility, Uniqueness, Privacy and Accuracy [6]. The issue of duplication casting of votes and capturing the missing voter's vote who cannot cast in their own native has been discussed in [7]. The question related to time and false voting by a false person, addressed in [8].

In this paper, we propose a safe and sound system by using powerful biometric methods such as face recognition and fingerprint. E-Voting is a public voting system that would be deployed to make election process system which will provide secure, speedy, crystal clear and competent. All the questions like time delay for vote counting, security, false and duplicate voting addressed in this paper.

The main concept behind this paper is to provide additional security using different biometric techniques such as face recognition and dactylogram. Technique is to scan the face, and then system will detect the ratios of face of voter stored in database. Then fingerprint of that particular user is getting displayed by matching face ratios. For giving more security, after face recognition, fingerprint is scanned. Voter is allowed to vote if matched, otherwise cancelled. After voting, count is updatedautomatically.

II. METHOD

An electronic voting system is a voting system in which the election data is recorded, stored and processed primarily. The difficulty of false biometric detection can be seen as a two-class classification problem where an input biometric trial has to be allocate to one of two module: real or fake.

Fingerprint Recognition:

Fingerprint recognition or fingerprint verification refers to the computerized method of verifying a match between two Human fingerprints. Fingerprints are one of many forms of biometrics used to spot individuals and verify their uniqueness. A fingerprint looks at the patterns set up on a fingertip. There are a variety of approaches to fingerprint verification. Some emulate the traditional law enforcement method of matching blueprint; others use straight minutiae matching devices and still others are a bit extra unique, including things like more border patterns and ultrasonic. A greater variety of fingerprint devices are available than for any supplementary biometric. Fingerprint authentication may be a good choice for this touch sensing voting systems, where you can give users sufficient explanation and guidance, and where the system operates in a controlled environment. It isnot shocking that the terminal access application area seems to be basedalmost exclusively on fingerprints, due to the moderately low cost, small dimension, and ease of integration of fingerprint authentication devices that will be implemented.

Face Recognition:

This method is based on information theory which will decompose the face images. Then forms the minute set of the characteristics features images which are called as "Eigen faces".

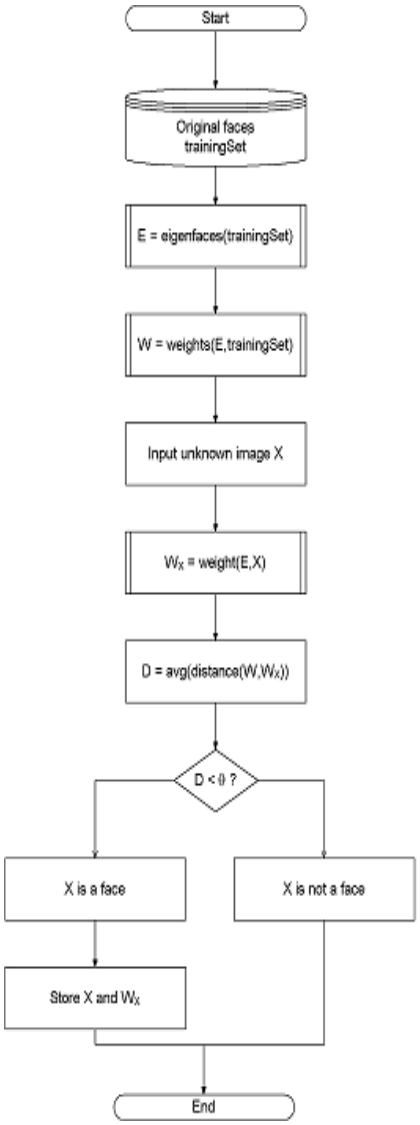

Fig.Data Flow Diagram of Eigen face-based facial recognition algorithm

This is nothing but the principal components of the face images of the training set. For face recognition, the Eigen face technique is one of the nearly all efficient and simplest approach.In Eigen face method, the distance is being measured between couples of images. If that distance is less than a provided threshold value, then it is an identified faces or else it is an unidentified faces.In the above Figure , we have two set of image blocks, first one is training set image block and second one is check set image chunk. In training set picture block, initially the Eigen face of image in the database i.e. trained image is obtained. Then the weight W1 is considered by using the Eigen face and the training set. In the testing set image block, image X is the unknown input image which is nothing but the captured image. The weight W2 is calculated using the input image andthe Eigen face. Value of D is calculated by finding the average of distances between W1 and W2. If the D value is less than 0, then the face is recognized. Then the input image X and W2values are stored. If the D value is larger than 0, then the face is not predictable.

III.RELATED WORK

Now a day's there is need of e-voting system due to digitalization of every work. E-voting system is more secure than manual system. In our E-voting system we used the Biometric for system is more secure. In biometric we used face detection and fingerprint recognition module is used. Biometric based system is those in which human characteristic like face shape, fingerprint etc. are being used identification and authentication.

Face detection module can be divide in two part for working like face verification and face identification. The verifying face is the first stage; it includes identifying and locating a face in an image. The identification is the second stage; it includes feature extraction, where important information for discrimination is saved, and the matching, where the recognition result is given with the help of a face database.

Fingerprint recognition module also used for e-voting system. This is also two step for fingerprint recognition first fingerprint is verified and the identified for those particular voter. Every voter fingerprint is different so this system is more secure for e-voting.

In this paper performance three biometric algorithms are define. Which are 1) Principal component analysis 2) Template matching 3) Eigen face 4) Advanced Encryption Standard 5)Naïve Bayesian classifier

Performances of these algorithms are

Principal Component Analysis:

Principal component analysis algorithm work by separately analyzing part of face like eyes, nose, ear etc. This algorithm time complexity also increased. Principal component analysis algorithm steps are following:

Transform an$N\times d$ matrix X into an $N\times m$ matrix Y:

1) Centralized the data (subtract the mean).

2) Calculate the $d\times d$ covariance matrix: C=$1N-1XTX$

- Ci ,= $1N-1$ Xq,$i.Xq$, jNq=1
- Ci, (diagonal) is the variance of variable i.
- Ci, (off-diagonal) is the covariance between variables i and j.

3) Calculate the eigenvectors of the dispersion matrix.

4) Select m eigenvectors that correspond to the largest m eigen values to be the new basis.

Template matching

Template matching algorithm is salient region of the facial image are extracted.

This region is compared on pixel-by-pixel basic with an image in database.

The template matching algorithm step following:

1. Compute distance matrix Dij; i: ith region of image 1, j: jth region of image 2.
2. Calculate forward matching matrix Cij: Cij = 1 if Dij<Dik for all k 6= j; otherwise,
Cij=0.
3. Calculate backward matching matrix Bij: Bij = 1 if Dij<Dkj for all k 6= i; otherwise, Bij = 0.
4. Match regions i and j if CijBij = 1.
5. Remove established correspondences from Dij.
6. Iterate until no further matching is possible.

Eigen faces:

Eigen face algorithm is tries to capture the face ratio of each and every part like nose, eyes, ear, mouth etc. And position remains constant from new born stage to until depth. Eigen image are projected into feature space that encodes the variation among known as face image. Algorithm steps are following:

1. Initialization: Acquire the training set and calculate eigen faces which define eigen value (ƛ) and eigenvector(X)

AX = ƛX

2. Calculate the Eigen value and eigenvector.

(A- ƛI)X=0

Where, I is the n*n identity matrix.

3. Determine if the image is face.

Det (A-VI) =0

4. If yes, classify the weight pattern as known person or not.

AXi = ƛXi

Where i=1, 2, 3…n

5. If the same unknown face is seen several times incorporate it into known faces.

(A- ƛ I)

Advanced Encryption Standard

Advanced Encryption Standard algorithm implemented by hardware and software. It provides extra security but the result are infeasible to current technology and it also does not support most system libraries and protocol. Advanced Encryption Standard algorithm step following:

1) AddroundKey transformation: is a simple XOR between the working state and the round key (the key output from the key-scheduling operation).

2) Subbyte transformation: is a non-linear byte substitution, using a substation table (s-box), which is constructed by multiplicative inverse and affine transformation.

3) Shiftrows transformation: is a simple byte transformation where the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift varies from zero to three bytes according to the row number.

4) Mixcolumns transformation: is equivalent to matrix multiplication. The matrix output from the shiftrow operations multiplied by a fixed matrix,

Bayesian Classifier

Bayesian classifier is statistical approach. It can predicate the membership of probability such as probability give to particular class. It is not give more accuracy.

Bayes theorem: The classification problem may be formalized using a-posteriori probabilities:

P(C|X) = prob. that the sample tuple

X=<x1,…,xk> is of class C.

P(C|X) = P(X|C)·P(C) / P(X)

P(X) is constant for all classes

P(C) = relative freq of class C samples

C such that P(C|X) is maximum = C such that P(X|C)·P(C) is maximum

Problem: computing P(X|C) is unfeasible!

IV.IMPLEMENTATION

The E-Voting system using face recognition and Dactylogram (fingerprints) in order to do vote online by using eigen faces algorithm for face recognition has been implemented. The System results given below describe trade-off criteria for online voting for our application need. Eigen faces is used for face recognition, Face recognition and Dactylogram is the parameter for the voting system.

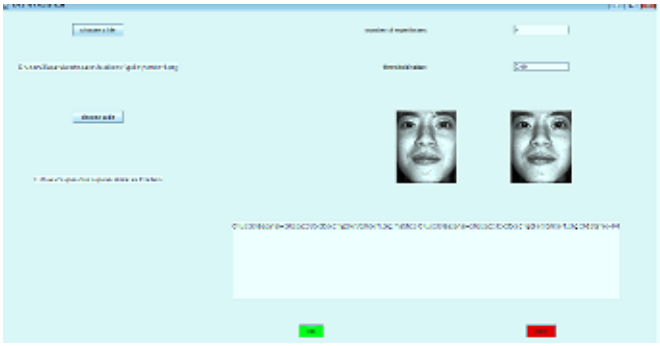

Figure 1 Face recognition

Face recognition is the first step of system, which can be recognize voter's face. Eigen faces algorithm is implemented for recognize the face. Eigen value takes a number that can be used for creating specified number of eigen faces as shown in figure 1. Threshold value is used of calculating error rate between two faces.

In Figure 2 shows the finger prints scanner where voter has to match his/her fingerprints to do vote. It is second step of system which can be part of biometrics. Voter has to wait for 5 second until scanner blink the light. After scanner blink the light voter has to put his/her fingerprints for the scanning. Scanner repeatedly scans for 5 times and each time it is wait for the 3 second. So, total matching process is 20 second.

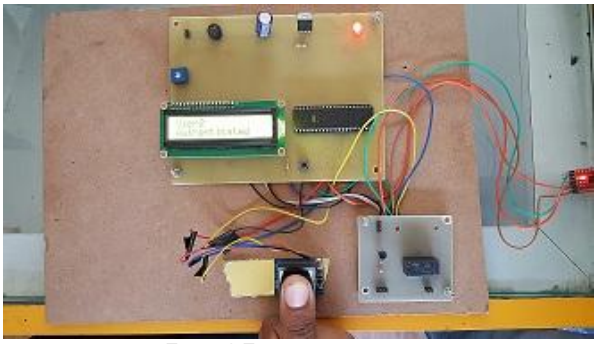

Figure 2 Fingerprint scanning process

After successful matching of above two steps, voting module is shows up and created session of 20 seconds as below in figure 3. It shows the candidate name, party name and symbol etc those are stand in election. Voter has to click on vote button in front of candidate name until session expires. When voter click on vote button is also check whether he/she Voted or not. If not then vote can be counted. If voted then system shows up already voted.

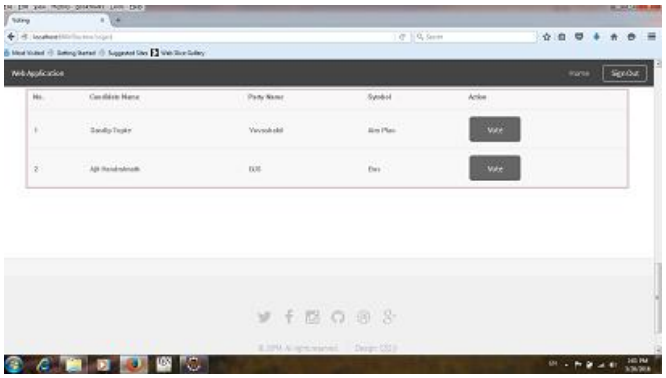

Figure 3 Vote module

Finally, if election process is over, then winner of the election is declare as shown in figure 4. System can takes 25 to 30 seconds for each vote.

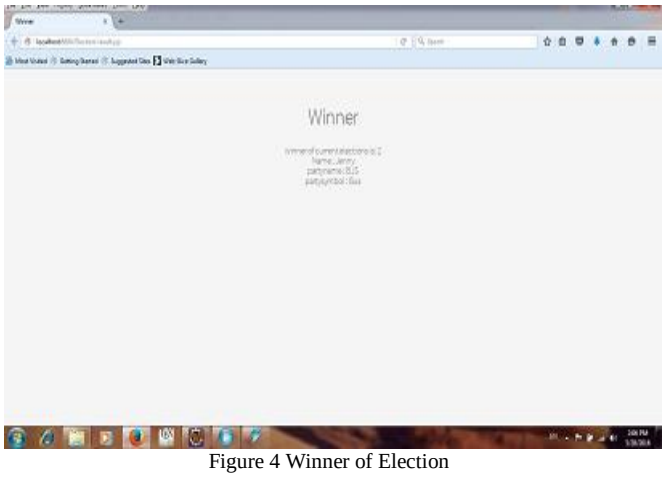

Figure 4 Winner of Election

V. RESULT AND DISCUSSION

The result in Figure 1 shows the face recognition by using Eigen faces algorithm, it is very high as compared to PCA algorithm of face recognition. Matching process of Eigen face technique is high. The result in Figure 2 shows fingerprint scan for the authentic voter can do vote to the registered candidate. The result in Figure 3 shows the vote module for to do voting, it is shows up after the successful recognition of voter face and his/her fingerprints. The result in Figure 4 shows the Winner of Election, after the voting process done winner of election is declares. The entire process is very easy and fast execution. It requires less human resource for operate the system.

VI. CONCLUSION AND FUTURE WORK

ASecure E-voting system uses face recognition and fingerprint methodsto provide additional security has been discussed in this paper. As per our study and discussion, Eigen faces algorithm is superlative for face recognition because it provides high accuracy than other algorithm discussed in paper.

The implemented system focuses on avoiding fake and duplicate voting by providing additional security. In future system can be built on android platform for online voting using same techniques. In this project, we have considered only face recognition and fingerprint. In future, it can be possible to use OTP method for voting.

REFERENCES

[1] Tadayoshi Kohno, ADAM STUBBLEFIELD, AVIEL D. RUBIN and DAN S. WALLACH, AVIEL D. RUBIN," Analysis of an Electronic Voting System, 2004".

[2] KashifHussainMemon, Dileep Kumar and Syed Muhammad Usman," Next Generation A Secure E-Voting System Based On Biometric Fingerprint Method, 2011".

[3] B. Swaminathan, J. Cross Datson Dinesh, "Highly Secure Online Voting System with Multi Security using Biometric and Stegonography, 2012".

[4] Ashwini Ashok Mandavkar and Rohini Vijay Agawane," Mobile Based Facial Recognition Using OTP Verification for Voting System, 2015"

[5] Donovan Gentles, Suresh Sankaranarayanan," Application of Biometrics in Mobile Voting,2012".

[6] S anjay Kumar, Manpreet Singh," DESIGN A SECURE ELECTRONIC VOTING SYSTEM USING FINGERPRINT TECHNIQUE, 2013".

[7] J ones Kevin Arthur, Thomas Robinson, R.Latha," Implementation aspects of Bio-Metric system in Electronic Voting Machine by using embedded security and big data approach,2014"

[8] J avier Galbally, Sebastian Marcel, and Julian Fierrez," Image Quality Assessment for Fake BiometricDetection: Application to Iris, Fingerprint, and Face Recognition, 2014".

