Visual Cryptography in Internet Voting System using Face Detection and Recognition (FDR)

Vikas Chakranarayan[1] Gaurav Shinde[2] Rahul Jagtap[3] Shrikant Gagare[4] Prof. Anjali Musmade[5]
[5]Assistant Professor
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]SCSCOE, Rahuri Factory, India

Abstract— With the help of Visual Cryptography (VC), it allows the voter to cast his vote from remote location even if the voter is absent in the voting place. It allows the voter to cast his vote securely and full confidentiality. System allows permission to the voter which is participated in the election only when he entered correct password which is generated using visual cryptography after stacking of two shares. System/Admin sends share 1 to voters email id before election and share 2 will be present during election for his login. From observing these two shares hackers can't get any information. For this system we use 2 out of 2 visual cryptography scheme. It generates two shares even if the hackers get any one of the shares ,it is not possible to get the information about the second share which is send to the email id of the voter. Thus it provides two way security for efficiently use of internet voting system. For more security purpose Face Detection and Recognition system (FDR) is introduced in our system. Web based voting allows the voter to cast his/her vote from any remote location. The voter's image is uploaded and passed to a face detection algorithm in which the face detection from the image is done and saved it as the first matching point. The voter's National identification card number is used to get saved photo from the database of the Admin which is second matching point. If the result of these two matching points is identical then the voter allowed to cast his vote. If the result of these two matching points is not identical then the voter logs out from the system.

Key words: Internet Voting System (IVS), Visual Cryptography (VC), Visual secret sharing, Face Detection and Recognition system (FDR)

I. INTRODUCTION

In earlier days, Internet Voting System is not developed in our country. Manual voting system is used. There are various types of manual voting system. First type is Raise Your Hand or Raise Your Voice or Put Stick in Box it is held by raising hands or shouting out 'Ha' or 'Na'. Second type is Paper Ballot in this voter writes person's name on the paper and put that paper in ballot box. Third type is Lever Machine in that on mechanical lever voting machines, in front of the machine the name of each candidate is assigned a particular lever in a rectangular array. The voter push down selected levers to indicate eligible persons choices. Fourth type is Postal voting in which voter can cast their votes through post. Fifth type is SMS and Phone in which the voter can cast their votes through messages or call. Now a days Electronic voting machines are used in that the EVM consist of the electronic voting machine in which the voter should press the button in front of the specific candidate for whom the voter should cast their vote.

In corporate companies, elections are conducted to elect President, Secretary and other board members. Candidates may be working across the world and it is therefore difficult for them to vote from there. A web based polling system assists the process, with security measures by which they can vote confidentially from any part of the world. In the 2001 general election in Washington State, 69% of votes cast were cast by mail. This Internet voting system provides them good solutions with security using Visual Cryptography.

Internet Voting system refer as online voting system in that user's client server can connect to server system. Hence there is three way implement voting system over the internet: Kiosk, Remote, and poll-site voting. Each of these three ways has its own particular security requirements. In remote voting a third party, or the voter himself (rather than election officials) has control over the voting client and operating environment. In Kiosk voting, the voting client may be installed by election officials, but the voting environment is out of election officials control. In Poll- site voting, election officials have control over the voting client and the operating environment. The visual cryptography system develop for the mainly remote internet voting its nothing prevent being poll-site or kiosk voting, depending on the security requirements. Visual cryptography system having ability to carry out small and large-scale election procedures, or even surveys where strong security may be less of a concern. It is not unreasonable to ask that remote Internet voting be as secure as voting by mail. The authors note that although remote internet system has make large amount of attacks that may not be applicable to poll-site or kiosk Internet voting, it at least reduces the threat of insider attacks and allows less trust to be placed in the election officials.

To encrypt written material like printed text, hand written notes, pictures, etc. used Visual Cryptography. The decoding is done by the human visual system directly (By stacking share one over the other). For a set P of n participants, a secret image S(voter password) is encoded into n shadow images called shares, where each participant in P receives one share. To retrieve the image back all the participants share has to be place one over another then the image is got. VC in IVS aims at providing the voters a facility to cast their vote for the elections that are conducted. They can vote from any place without them coming to the place where the elections are conducted by using the features that are provided by VC that are implemented in IVS. The election will go on with good security measures because the voter can only vote for the candidate only if he logs into his login by entering the correct password getting by merging two blocks. IVS with 2-out-of-2 VC for an efficient authentication voting system. If hacker get one block of password for the login then he will not able to access second block as second block send on users Email-id. Thus our IVS provides two way securities to the voting system.

To increase security and authentication of IVS system Face Detection and Recognition system (FDR) is introduced. In this uploaded image and image saved in database are compared using Eigen Face detection algorithm.

II. LITERATURE SURVEY

In this scheme visual cryptography system can secret image will be divided in two blocks.This easiest way of kind of visual Cryptography. In these scheme we focus on security of voting as we using two share one of the get to user at the election time and second share will be send on users email id. To reveal the original image, these two shares are required to be stacked together. represents the division of black and white pixel in this scheme [1].

There are various types of voting system through which the election can be held. First type is Raise Your Hand or Raise Your Voice or Put Stick in Box in that earlier days of election was held by raising hands or shouting out 'Aye' or 'Nay'. Second type is Paper Ballot in that voter used to write eligible person's name on the paper and put that paper in ballot box secretly. Third type is Lever machine in that on mechanical lever voting machines, the name of each candidate is assign to a specific lever in a rectangular array of levers on the front of the machine. The voter pulls down the selected levers to show their choices. Fourth type is Postal voting in that people also cast their votes through posting their votes on the place of voting.Fifth type is SMS and Phone in which the voter can cast their votes through messages or call. Sixth type is electronic voting machine system in that the EVM consist of the electronic voting machine in which the voter should press the button in front of the specific candidate for whom the voter should cast their vote [2].

In this scheme allow for divide secret image into k numbers of shares. For example, In 3 out of 6 VC scheme, any 3 shares among the 6 shares are used to retrieve the secret data. The major problem associated with this scheme is that the user should maintain many unnecessary shares which results into loss of shares. Also more number of shares means more memory consumption [3].

Here original secret is divided into k number of shares and For reconstruction of the secret, all k shares are necessary. For example, in 6 out of 6 VC scheme, Secret is revealed only after stacking all the 6 shares, here value of k= 6. The scheme 6 out of 6 is not user friendly because to manage k number of shares is quite a difficult task and it also increases time complexity [8].

With traditional poll site voting, voters authenticate themselves by providing identification or an affirmation to a trusted poll worker; Internet-based voting offers great convenience, but does not offer such obvious authentication methods. Today, remote voting in governmental elections is done through absentee ballots that offer little security, and are slow and expensive to tabulate, and remote voting is becoming increasingly accepted and Popular[10].

In this scheme[11] author propose a system of face recognition in which he compare similar features of face in which he measures shade of hair, length of ears, lip thickness. They used linear embedding algorithms for comparing the features. In this scheme [12,13] author proposed a system of face recognition using an associative network that can recognize to classify face images using a simple learning algorithm and recall a face image and give input to the network. In this scheme [14] author used Eigen face algorithm for face recognition in which facial features are considered for recognizing known individuals. It uses 2-D method for face recognition. In these scheme [15] author proposed a system face recognition with eigen faces in which represent human face under several environmental conditions.

III. SYSTEM ARCHITECTURE

To overcome the drawbacks of the manual system proposed system should be developed.

The basic idea behind this is that the Candidates can cast their votes from any remote place during election time.
Features of proposed system:-

- Remote access voter
- High Security with face detection
- Session Management
- Reduced paper-work and human efforts
- Centralized Administration

Following figure shows the entire architecture of the proposed system.

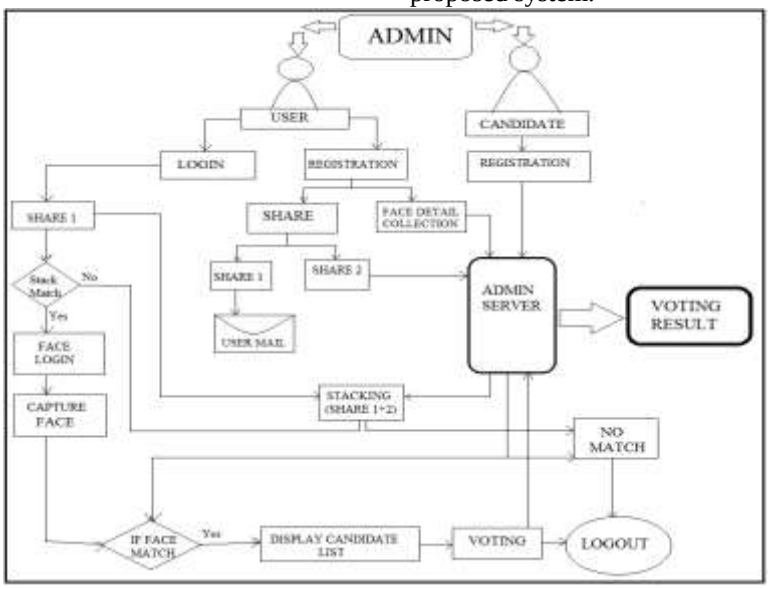

Fig. 1: The framework of the proposed system

The system Architecture consist of two session one is Admin session and another is user session. The system Architecture divides into two type of works first is preprocessing work and second is post processing work. In pre processing work admin register candidate details, user details, election details, set password for each user.

In post process work include voting process, result declaration, checks voter's identity.

The system architecture mainly consist of two types of scheme one is visual cryptography scheme and another is FDR scheme.

During registration process of user image captcha is displayed for each user. During voting process, we used 2 out of 2 VC schema in which secret image is divided into two shares. Next step is embedding of this two shares in which two shares are covered with white and black dotted image. it is called as embedding process. Out of these two shares one share is send to database and another share is send to voter's email id. Due to this, no information can be revealed to the hacker. Next step is stacking of two shares. Original image can be displayed only after stacking of this two shares.

From stacking of these two shares secret password is generated. The voter allowed to login for voting process only when he/she entered a correct password.

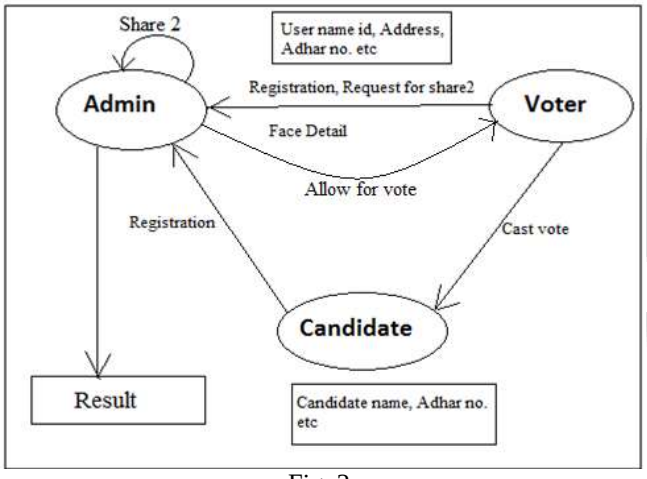

Fig. 2:

For more security purpose we introduce face detection and recognition (FDR). In that we used Eigen face detection algorithm. In this algorithm trained data sets made using images which are stored in database it is called as ORL or AT/T database. From these average face is calculated. Using these average faces mean image is calculated and from this mean image covariance matrix are generated. Eigen values are calculated from these covariance matrices. Larger the Eigen values means more is the facial feature.

Voter's face image which is uploaded during voting process is projected into face space then Euclidean distance is measured if this distance is less than face class then it is a recognized as a known person if these image identity matches then only the voter allowed to casting his vote. If mismatch is found then user logout from the system.

Final step is declaration of result. Admin collects all these information about polling process and declared the result at the prefix date which is decided by SCE.

IV. ALGORITHM USED

A. Share Generation Algorithm

Input: Image
Output: Stacked image

1) Suppose there are n number of voter then n number of shares are generated.
2) For secret share generation we use 2-out-2 cryptography used.
3) In this each image is divided into two share.
4) Each share is covered with white and black dotted pixel for security purpose
5) To reconstruct original image these two shares stacked over one another.

B. Eigen Face Detection Algorithm

Input: captured image
Output: match/mismatch retrieval image

1) The Eigen face technique uses general facial patterns.
2) Eigen face system needs a database of known faces in which all images are of same size (in terms of pixels), and gray scale with values ranging from 0 to 255.
3) Each face image is resized into 128*128 dimension and converted into a vector of length N (where, N=image width*image height).
4) Eigen face system use of Fourier analysis reveals that a sum of weighted sinusoids at differing frequencies can recompose a signal perfectly. In the same way, a sum of weighted Eigen faces can seamlessly reconstruct a specific persons face.
5) The algorithm calculates the average face in face space and returns the top Eigen face vectors then it uses these differences to compute a covariance matrix for our dataset. The covariance between two sets of data reveals how much the sets correlate.
6) The output of the Eigen faces system is the first point extraction of the persons face which we will be used to verify the voter's identity. The voter will enter his ID number which is used to fetch his image from the database of SCE. This image later on considered as first point.
7) The voters image captured using a webcam is the input to the Eigen face system to detect the face from image and this will be the second point. The two points are checked for matching using pattern matching algorithm.

V. RESULTS ANALYSIS

To compute the performance of three VC scheme the accuracy of each scheme is measure which is shown below.

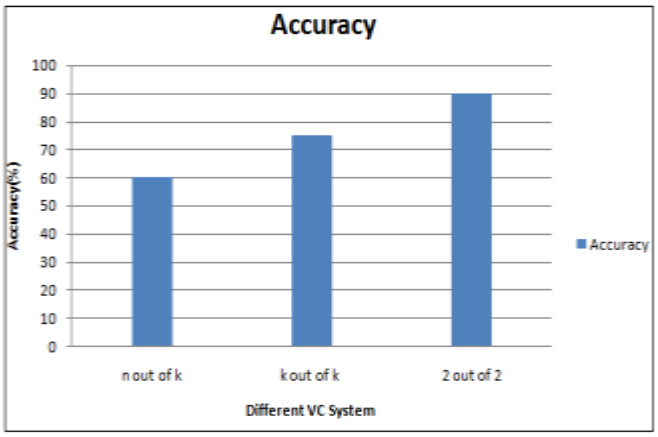

Fig. 3: Accuracy

Database is created using 10 different persons using 20 different positions. For each person 20 different images were tested using line edge detection technique and Eigen face detection technique. Result analysis using accuracy measurement shown in a graphical format.

In Eigen face detection algorithm we have taken 4 persons and make a training dataset. At first we take 3 different position of one person. And then take 5 different images of next person. And then take 7 and 9 images of remaining persons.

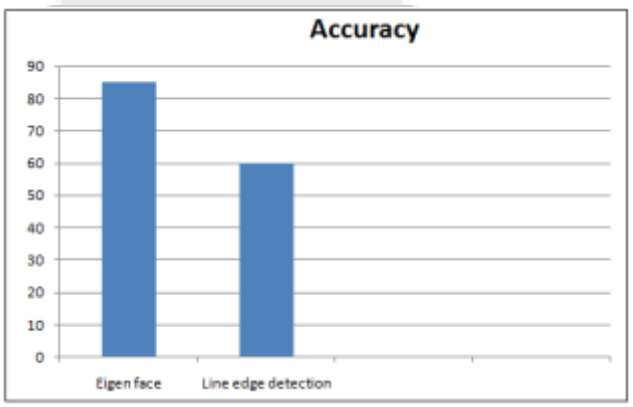

Fig. 4:

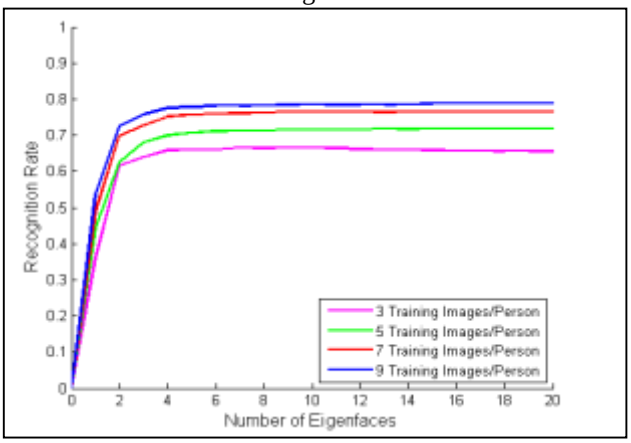

Fig. 5: Number of Eigen faces

S.No.	Training images per class	Testing images per class	Correct Outputs (out of 80 tests)	Recognition Rate
1	9	2	77	95.26%
2	7	2	75	91.25%
3	5	2	71	86.25%
4	3	2	65	78.75%

Table 1:

VI. CONCLUSION

This system is designed for corporate companies to conduct their elections for different posts such as the presidential election, manager election etc. even companies branches spread in different countries then also all members can cast their votes easily and effectively in a secure way by using Internet voting system using visual cryptography because the voter can vote from the place where he is working by using this system .This can also be used for conducting the elections in Clubs like Country Club, Country Vacations etc. It can be converted for public elections and also parliament elections. Proposed online Internet voting system is trustworthy and it will become useful for voters and organization in many ways and it will reduce the cost and time. Internet-based voting offers many benefits including low cost and increased voter participation. Internet voting system must handle human factors and security concerns carefully and in particular make sure that they will provide reliability to the voters during voting process. The system we propose uses visual cryptography and FDR system to provide more security for voters to cast their votes and to provide high authority to election servers.

VII. REFERENCES

[1] Rajendra Basavegowda, Seenappa Sheshadri, "Visual Cryptography in Internet Voting System", In IEEE Transactions onVisual Cryptography978-1-4799-0048-0/1 ©2014.
[2] Madhuri Borkar, Rohini Deshmukh, Mrunal Kaware, Ritika Jujgar," Secure Internet Voting System using QR code and Face Recognition", (IJIR),Vol-2, Issue-2,2016.
[3] Adi Shamir (1979), "How to share a Secret", Communications of the ACM, pp .612-613.
[4] [4] M. Naor and A. Shamir (1995), "Visual Cryptography", Advances in Cryptology-Euro crypt '94 Proceeding, LNCSvol. 950, Springer-Verlag, pp. 1-12.
[5] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman, (2012) "Attacking the Washington, D.C.Internet Voting System", In Proc. 16th Conference on Financial Cryptography & Data Security,pp .1-18
[6] Hussein Khalid Abd-alrazzq1, Mohammad S. Ibrahim2 and Omar Abdurrahman Dawood (2012), "Secure Internet Voting System based on Public Key Kerberos", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, pp. 428-434.
[7] Adhikari Avishek and Bimol Roy (2007) "Applications of Partially Balanced Incomplete Block Designs in Developing (2,n) Visual Cryptographic Schemes". IEICE Trans. Fundamentals, Vol.E90–A, No.5 ,pp. 949-951

[8] Marek R. Ogiela, Urszula Ogiela (2009) "Linguistic Cryptographic Threshold Schemes", International Journal of Future Generation Communication and Networking.Vol.2, No.1,pp. 33-40
[9] Carlo Blundo, University of Salerno, Alfredo De Santis and Douglas R Stinson (1998), "On the contrast in visual cryptography scheme".pp. 1-28
[10] Thomas Monoth, Babu Anto P (2009), "Achieving optimal Contrast in Visual Cryptography schemes without pixel expansion". International Journal of Recent Trends in Engineering, Vol 1, No 1, pp. 468-471.
[11] Fisher, M.A., & Eschlager, R.A, "The Representation and matching of pictorial structures. IEEE Transactions on computers, c-22(1).
[12] Kohonen, T,"Self-organization and associate and associative memory", Berlin: Springer- Verlag 1989.
[13] Kohonen, T. & Lethtio, P, "Storage and processing of information in distributed associative memory systems", in G.E. Hinton & J. A. Anderson (Eds.), Parallel models of associative memory hillsdale, NJ: Erlbaum, pp. 105-143, 1981.
[14] Matthew A. Turk and Alex P. Pentland, "Face Recognition using Eigenfaces", CVPR'91, pp. 586-591 IEEE Computer Society, 1991.
[15] Zhujie; Yu, Y.L, "Face Recognition with Eigenfaces" , industrila Technology, Proceedings of the IEEE International Confrence on Digital object identifier, pp. 434-438, 1994.

