Visual Cryptography in Internet Voting System

Rajendra A B [1] and Sheshadri H S [2]
[1]Vidyavardhaka College of Engineering,Mysore,Karnataka,India,Asia
[2]PET Research Centre, PES College of Engineering,Mandya, Karnataka, India,Asia
{rajendraab[1], hssheshadri[2] }@hotmail.com

Abstract -
Internet Voting System (IVS) Using Visual Cryptography (VC) aims at providing a facility to cast vote for critical and confidential internal corporate decisions. It has the flexibility to allow casting of vote from any remote place, even when key stakeholders of election process are not available at workplace. This is enabled by leveraging and implementing the features provided by the VC in IVS. The election is held in full confidentiality by applying appropriate security measures to allow the voter to vote for any participating candidate only if he logs into the system by entering the correct password which is generated by merging the two shares (Black & White dotted Images)using VC scheme. Where, Administrator (Election officer) sends share 1 to voter e-mail id before election and share 2 will be available in the voting system for his login during election. Voter will get the secret password to cast his vote by combining share 1 and share 2 using VC .Visual Cryptography (VC) is a secret sharing scheme in which an image is converted into shares. No information can be revealed by observing any share (Black & White dotted Image). The information about the original image (Voter Password) will be revealed only after stacking sufficient number of shares. There are various schemes present in VC, 2 out of 2, k out of n, n out of n, etc. In the proposed method, IVS with 2-out-of-2 VC has been used for an efficient authentication voting system. Even if the hacker gets one share of the password, it is impossible to get the other share of the password, as it will be sent to the E-Mail Id of the voter. Thus IVS provides two way securities to the voting system, which is very much in need.

Index Terms- **Internet Voting System (IVS), Visual Cryptography (VC), Shares, Voter Password, Visual secret sharing**

I. INTRODUCTION

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 [1, 2].

A. Internet Voting System

When the Internet voting [3] generally refers to Remote Internet voting, where the client software communicates over the Internet to the server software from a voter's PC. However, there are at least three other ways to implement voting over the Internet: Remote, Kiosk 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. Although the Visual cryptography system was designed especially for remote Internet voting, nothing prevents it from being deployed for poll-site or kiosk voting, depending on the security requirements. Visual cryptography system also has the ability to carry out small-scale 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 voting opens itself up to a wide range 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. In many cases, voting machines arrive at polling places days or weeks early, making the threat of an on-site attack a real concern [4]

B. Visual Cryptography

VC is used to encrypt written material (printed text, handwritten notes, pictures, etc). 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 [5, 6]. To retrieve the image back all the participants share has to be place one over another then the image is got.

978-1-4799-0048-0/13/$31.00 ©2013 IEEE

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 that is got by merging the two shares.

IVS with 2-out-of-2 VC for an efficient authentication voting system. Even if the hacker gets one share of the password, it is impossible to get the other share of the password, as it will be sent to the E-Mail Id of the voter. Thus our IVS provides two way securities to the voting system.

This paper is organized as follows. Section II introduces the fundamental principles of Visual Cryptography and voting systems. The application of 2-out-of-2 Visual cryptography scheme in the Internet voting system can be viewed in section III. Finally, conclusions are drawn in section IV.

II. INTERNET VOTING SYTEM WITH VISUAL CRYPTOGRAPY

There are number of visual cryptography schemes in existence. A selection are described below

A. 2 out of 2 Visual Cryptography Scheme

In this type of visual cryptography scheme, the secret image is divided into two shares. This is the simplest kind of visual cryptography. The major application of this scheme is found with IVS that uses 2 out of 2 Visual secret sharing schemes [7] for authentication purpose. To reveal the original image, these two shares are required to be stacked together. Table 1 represents the division of black and white pixel in this scheme [8].

Table I. THE PIXEL PATTERN FOR 2-OUT-OF-2 VC [9]

Pixel color	Original Pixel	Share1	Share2	Share1+ Share2
Black	■	■□	□■	■■
Black	■	□■	■□	■■
White	□	■□	■□	■□
White	□	□■	□■	□■

B. n out of k Visual Cryptography

This kind of scheme allows dividing a secret image (secret data) into k number of shares. Then the secret image can be revealed from any n number of shares among k. For example, In 3 out of 6 VC scheme, any 3 shares out of 6 shares are sufficient to reveal the secret data. The major problem associated with this scheme is that the user needs to maintain many shares which may result into loss of shares. Also more number of shares means more memory consumption.

C. k out of k Visual Cryptography

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, where k= 6. This scheme is not so popular because managing k number of shares is difficult task and it also increases time complexity.

D. Traditional voting systems

With traditional poll site voting, voters authenticate themselves by providing identification or an affirmation to a trusted poll worker; a poll site authenticates itself to a voter by being at a well-publicized physical location and having officials representing several different organizations present (including police and political party representatives). 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 the most recent election in Albemarle County, Virginia, voters enter a poll site and are given a numeric PIN by the poll worker after they check the voter's identity and inclusion on the list of eligible voters. The voter enters this PIN into the machine on which the vote is entered. There is no reason for the voter to be confident the assigned PIN will not be associated with the vote that was cast and the identity verified when the PIN was provided. With traditional voting, most voters are willing to accept this because they believe the poll workers are trustworthy. With remote voting, stronger measures are required, and it is important that the existence of those measures is clearly conveyed to voters in a way that establishes an appropriate level of trust [11].

In the proposed method, election is held in full confidentiality by applying appropriate security measures to allow the voter to vote for any participating candidate only if he logs into the system by entering the correct password which is generated by merging the two shares (Black & White dotted Images)using VC scheme. Where, Administrator (Election officer) sends share 1 to voter e-mail id before election and share 2 will be available in the voting system for his login during election. Voter will get the secret password to cast his vote by combining share 1 and share 2 using VC.

III. METHODOLOGY

This system has two user sessions namely Admin Session & User (Voter) Session. As soon as we run this system the home page will be displayed with the following links one for the admin session and the other for the user session .The working of the system is as shown in the Fig 1.

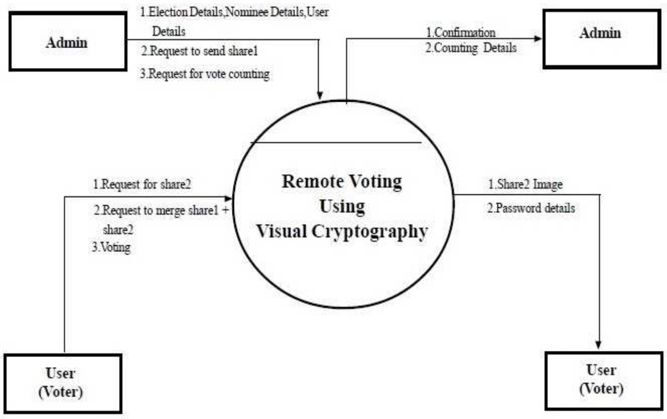

Fig .1. Process Overview

The admin home page has the following links: User Details, Election Details, Candidate Details, Image Details, SetPassword, Election Report, Change Password and Sign Out. When the admin clicks the user details link a page is displayed with the user details in a grid like having the headings as user id, user name, date of birth, cell number, address, email id etc. It consists of a button called “Add User” when admin wants to add a new user he has to press this button. Once admin has filled the relevant details he has to press command button by name register. It will check for user id validation & other validations if all the validations pass, a new user will be inserted in m_user table. When cancel is given the user is not deleted. The table used in this module is m_user.

When the admin clicks the election details link a page is displayed with the election details in a grid like having the headings as election date, election name, election remarks, start time & end time. It consists of a button called “Add Election Details” when admin wants to add a new election detail he has to press this button. It will check for validations & if all the validations are correct, a new election detail will be inserted in m_election_master table. When admin presses OK button the election is deleted & admin will get the message. When cancel is given the user is not deleted. The table used in this module is m_election_master.

When the admin clicks the candidate details link a page is displayed with the candidate details having the headings as candidate image, election details, edit & delete. In the election details column there are some more fields like name, post name, age & remarks. It consists of a button called “Add Candidate Details” when admin wants to add a new candidate detail he has to press this button. It will check for validations & if all the validations are correct, a new candidate will be inserted in m_election_candidate table. When cancel is given the candidate is not deleted. The table used in this module is m_election_candidate.

When the admin clicks the image details link a page is displayed with the image details in a table like having the fields as image, image details &delete button. Under image details we have the word & the file name. It also consists of a button called “Add Image Details” when admin wants to add a new Image; he has to press this button.

Another link is the set password link when this is clicked a window is displayed with two command buttons called “Set Password” & “Reset Password”. After the completion of this process set password the share 1 image will be sent to user’s email id & Click reset password button to reset the password to all the users. When the images are less than the user & we try to set the images to the users then it displays a message showing that “total images less than users or password set to all the users”.

Before an election, the election officials need to generate and mail image transparencies to eligible voters. To generate them, they need a random number. The election officials generate n random voter passwords, where n is the number of eligible voters. A transparency is generated for each voter, using the result of Visual Cryptography. In addition to the image, the transparency includes the password in a human-readable and type able format. Note that there is no mapping between voter identities and the transparency they receive, and the corresponding screen image for password is yet to be generated. After the generation of transparencies, the election officials send the generated transparencies and an address list of eligible voters to a third party who sends each eligible voter a randomly selected transparency along with a voter information packet including voting instructions. We rely on the integrity of the E-mail as does absentee ballots. Anyone intercepting a transparency in the mail could cast an extra vote, but there are already well-established severe penalties for e-mail tampering to deter this. As with traditional absentee ballots, there is nothing to prevent voters from selling their votes. An opportunistic voter could sell the transparency to another voter, who can then use it to cast the desired vote. Without identity-based authentication in the voting process, it is unlikely that vote selling can be prevented. Our design assumes that the election officials generating the transparencies do not collaborate with the third party sending out voting packets. This property could be guaranteed by requiring an open process.

For instance, the placing of transparencies in envelops could be conducted in public where voters could observe that the transparencies are selected randomly.

A voter visits the election web site and enters the type able username. The election web site maintains a list of the username values used to generate the transparencies and checks that the entered key is on the list and has not been used already (extensions that would allow a voter to change a previously cast vote are possible but not considered here). If the entered username is valid, the election server can calculate the corresponding transparency image. The election server then generates a random string to use as a password, and generates an image containing that string rendered as a bitmap image. The complementary image to the password image for the voter's transparency is generated and displayed on a web page returned to the voter. After the web server displays the corresponding image generated from username, the voter combines both the transparency to reveal the password as shown in Fig 2.

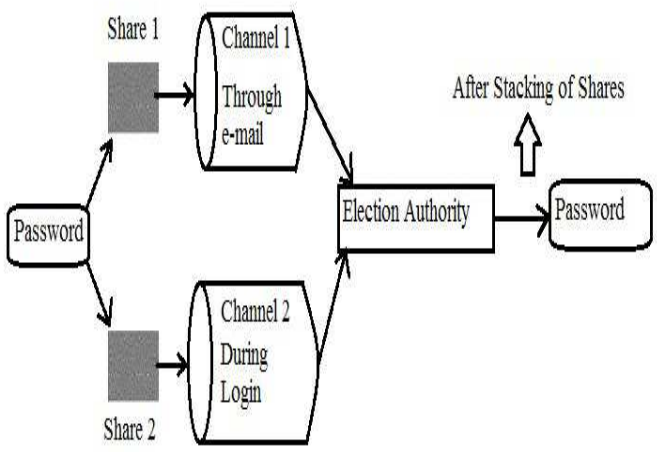

Fig 2. Encryption and Decryption of Password

To continue the voting process, the voter enters the revealed password. This protocol serves to both authenticate the voter to the election server and the election server web site to the voter. Only someone with the correct username transparency could decode the password in the generated image; only something with knowledge of the transparency sent to the voter could generate a sensible password image. In addition, we suspect from anecdotal evidence (but no scientific user studies yet) that nearly everyone will find the process of revealing a secret by holding a transparency up to an image on a monitor to be a satisfying and reassuring experience. Previous studies have analyzed how much a user needs to know in order to make rational decisions in the security of computer services, and the users showed they did not have a solid grasp on the security aspects of the system. With our system, voters do not need to understand how visual cryptography works, but are directly involved in performing the decryption in an intuitive and physical way. Our authentication scheme ensures that the voter cannot continue with the voting process without also verifying the server is legitimate.

The admin is only responsible for creating the users by using the add user option, he has the right to edit the information of any users that are created & also he can delete the users from a list of users that have been created. The access rights for the admin are for the following links. The links are user details, election details, and candidate details, image details, set password, election report, change password and sign out. These links can only be accessed by the admin and none other person. The admin can view and alter the details of user, election, candidate and the images that are used. Admin has the option to set the password for the users and also change the password; Admin can view the election details.

A. Algorithm

```
If ADMIN LOGIN link is clicked then
        Login as admin using administrator userid and password
If USERDETAILS link is clicked then
        View user details
        Click on edit to edit the user details
        Click on delete to delete a particular user details
        Click on Add New to add a new user.
Else if ELECTION DETAILS link is clicked then
        View election details
        Click on edit to edit the election details
        Click on delete to delete a particular election details
        Click on Add New to add a new election.
Else if CANDIDATE DETAILS link is clicked then
        View candidate details and photo
        Click on edit to edit the candidate details and photo.
        Click on delete to delete a particular candidate details
        Click on Add New to add a new candidate and photo.
Else if IMAGE DETAILS link is clicked then
        View password images
        Click on delete to delete a particular Image
        Click on Add New to add a new image.
        Enter image word and image file.
Else if SET PASSWORD link is clicked then
        Set the image word as password for the user in the database
        Split the image in to two shares using visual cryptography algorithm
        Send the first share of image to the particular user's email id.
Else if reset password is clicked
        Set the –null- as password for all the users in the database
        End if
Else if ELECTION REPORT link is clicked
        Select the election name of which report to be generated
        View results
        Send election result to all users through mail
```

```
Else if CHANGE PASSWORD link is clicked
        Enter userid and old password
        Enter and confirm new password
        Click on submit button to change the password.
Else if SIGNOUT link is clicked
        Delete the session
        Redirect to login page.
        End if
Else if USER LOGIN IS clicked then
        Enter user id and click on get password button
        Download link will be displayed and click on the link to download second share
        Use STG picture merge to merge the two shares to view the  password
        Login using the password
If VIEW PROFILE is clicked
        View the user details
Else if ELECTION DETAILS is clicked
        View the active elections
        View the candidates
        Cast vote
Else if SIGN OUT is clicked
        Delete the session
        Redirect to login page
        End if
End if
```

IV. CONCLUSION

This system is designed for corporate companies to conduct their elections for different posts such as the presidential election, manager election etc. Even though the branches of the companies are situated in different parts of the country or the world, the elections can be conducted easily and effectively in a proper manner by using this Internet based 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 voting system is very effective and it will be 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. Voting systems must consider security and human factors carefully, and in particular make sure that they provide voters with reliable and intuitive indications of the validity of the voting process. The system we propose uses visual cryptography to provide mutual authentication for voters and election servers.

ACKNOWLEDGMENT

I avail this opportunity to express profound sense of gratitude and thank my guide Dr H S Sheshadri. This Project is sanctioned by the Karnataka State Council for Science and Technology, IISC, Bangalore (Reference No. 36S0372) and I thank team members Prof. Shashank D, Afnan, Namratha Alva, Adhya, Aishwarya and Jayathi. We thank all reviewers for their valuable comments.

REFERENCES

[1] Adi Shamir (1979), “How to share a Secret”, Communications of the ACM, pp .612-613.

[2] M. Naor and A. Shamir (1995), “Visual Cryptography”, Advances in Cryptology-Eurocrypt ’94 Proceeding, LNCSvol. 950, Springer-Verlag, pp. 1-12.

[3] 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

[4] 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.

[5] 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

[6] 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

[7] Carlo Blundo, University of Salerno, Alfredo De Santis and Douglas R Stinson (1998), “On the contrast in visual cryptography scheme”.pp. 1-28

[8] 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.

[9] A B Rajendra and H S Sheshadri (2012), Study on Visual Secret Sharing Schemes Using Biometric Authentication Techniques, AJCST, Vol 1, pp.157-160.

[10] Anusha MN and Srinivas B K (2012), “Remote Voting System for Corporate Companies using Visual Cryptography,” vol. 2, pp. 250–251.

[11] Pallavi V Chavan, Mohammad Atique, and Anjali R Mahajan, (2011) “An Intelligent System for Secured Authentication using Hierarchical Visual Cryptography-Review”, ACCE Int J. on Network Security, vol. 02, No. 04.pp. 7-9

[12] Rajendra Basavegowda, Sheshadri Seenappa(2013) “Electronic Medical Report Security Using Visual Secret Sharing Scheme”,

IEEE UKSim 15th International Conference on Computer Modeling and Simulation Proceedings, pp, 78-83