Internet Voting System using Visual Cryptography

Hiray Rahul Pralhad[1] Ghorpade Vaibhav Shivaji[2] Patil Renuka Anil[3] Choudhari Shubham Pritamchand[4] Prof. Jagtap A.M[5]

[1,2,3,4,5]Department of Information Technology

[1,2,3,4,5]SKN College of Engineering, Pune-411041, India

Abstract— Today, most of the problems are occurred in Tradition Voting System. The problems like fake voting, large manpower, large security, more finance required, and complexity in report, paper work, poor management and confidentiality issue. This type of problems is overcome by our proposal Internet Voting System. For more security, reasons we are using Visual Cryptography. By using visual cryptography voting will be more secured with the help of two kinds of secured password. "ONLINE VOTING SYSTEM" is a latest technique of voting system. In this system people who have registered and who have all requirements of voting can vote online without going to any physical polling station. There is a database which is maintained in which all the names of voters with complete information is stored.

Key words: Visual Cryptography, Shares, Online Voting, OTP

I. INTRODUCTION

Elections are complex and involved processes that involve many components including voter registration, ballot preparation and distribution, voter authentication, vote casting, tabulation, result rep orting, auditing, and validation. Either a technical or a human factors flaw in any part of the system can lead to an incorrect election result or reduce public confidence in an election "ONLINE VOTING SYSTEM" is a latest technique of voting system. In this system people who have registered and who have all requirements of voting can vote online without going to any election center or polling booth. In IVS, database can maintained all voter information with necessary details which is required for voting. In "ONLINE VOTING SYSTEM" a voter can vote from any location, voters has rights to vote without any difficult. Before election start, they are just registered to our site. Registration is required for security purpose by the system administrator. Admin is responsible for all activities which are running on background site. Admin is not only one authority they are number of different authority and they are maintained all information in confidentially. So revealed of chances is not possible because corruption is not done to all levels of different authorities. So our site is very secured and easy to access from different locations without any difficulties.

A. Voting Over the Internet

When the term Internet voting is used, it generally refers to remote Internet voting, where the client software communicates over the Internet to the server software, say, from a voter's PC. However, there are at least two other ways to implement voting over the Internet: kiosk voting and poll-site voting. Each of these three ways has its own particular security requirements.

Remote: In this scenario, a third party, or the voter himself (rather than election officials) has control over the voting client and operating environment.

Kiosk: In this scenario, the voting client may be installed by election officials, but the voting environment is out of election officials' control.

Poll-site: In this scenario, election officials have control over the voting client and the operating environment.

B. Design & Security Goals

1) Transparency - All data on the bulletin board should be access by public. This contains the encrypted data and total count. The bulletin board does not store secrets.
2) Universal Verifiability - Any election result should be verifiable by any third party from the System. It should be confidential and possible to perform a complete audit of any procedure.
3) Privacy –All Voters votes are hidden and it's confidential from others and they are just see the total count on their screen.
4) Distributed Trust – Each procedure is tackled by multiple different authorities, and the final sum cannot be declared results without the number of prior authorities.

II. LITERATURE REVIEW

There are number of visual cryptography schemes in existence.

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 for authentication purpose. To reveal the original image, these two shares are required to be stacked together.

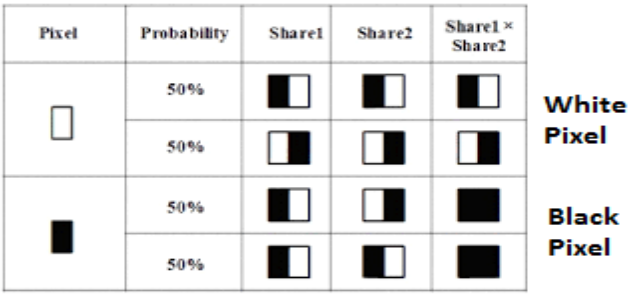

Fig. 1: Basic Concept of 2 out-of 2 scheme

B. K out of N Visual Cryptography

This kind of scheme allows dividing a secret into K number of shares. Then the secret can be revealed from any N number of Shares among K. 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. The application of this scheme is found with banking system. For the joint accounts, three shares are generated. One is kept with bank's server, second is delivered to the one

customer for the joint account and third share is delivered to the second customer. Hence both customers are able to access the account.

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. This scheme is not so popular because managing k number of shares is difficult.

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.

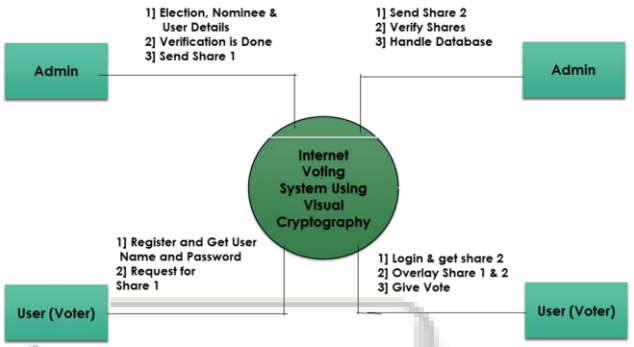

Fig. 2: Process Overview (Framework)

In our project, Users can do registration and get the username and password. After getting password user got the mail (Share 1) from the website (Admin) and request for the share 2 image.

At the admin site, admin verifies the users registration and send the share 1 and share 2 image to the users those are registered.

After getting share 2 image users can do the voting.

Admin can handle the database and admin is responsible for to create the election and display the results. After done the voting, all data removed from website.

A. Algorithm For System Flow

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

B. Algorithm for Visual Cryptography

Step 1 : Load Source Image
Step 2 : Division of image into black and white pixel.
"java.awt.image.BufferedImage" this package used for properties related to images
int WHITEPIXEL = (255<<24)|(255<<16)|(255<<8)|255;
int BLACKPIXEL = (255<<24);
where threshold = 128;
Step 3 : Pre Encryption Step :
Initialize two matrix for black and white pixels.
Apply Permutation
Vector C0 = White matrix value;
Vector C1 = Black matrix value;
Typecasting Of Values

White[i] = (IntMatrix)C0.get(i);
Black[i] = (IntMatrix)C1.get(i);
Step 4 : Storing of image in the form of luminance and chrominance
red = pixel >>16
green = pixel >>8
blue = pixel
*Factor = (red*0.299) + (green*0.587) + (blue*0.114)*
if(Factor > threshold) then WHITEPIXEL
else
BLACKPIXEL
Step 5: Encryption By Transpose Operations

W W B B	W W B B
W W B B	B B W W
Share 1	**Share 2**

Step 6 : Overlay Of Shares
if (Share 1 & Share 2) then
Display Original Image
else if (Share 1 & ! Share 2)
Display Share 1
else if(Share 2 & ! Share 1)
Display Share 2
Example: *Share 1 Matrix = WWBB BBWW*
Share 2 Matrix = WWWW BBWB
Share 1 + Share 2 = WWBBBBWB

IV. Conclusion

This system is designed for corporate companies to conduct their elections for different posts such as the presidential election, manager election, etc. OR to conduct Vidhansabha and Loksabha Elections. 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. 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.

V. Future Scope

1) In Future, we will develop Android App and with the help of this app we will conduct Election.
2) For Illiterate people we will provide one helping booth to each and every village / city.
3) We will provide one tutorial video for helping in voting process.

References

[1] Rajendra A.B and Sheshadri H.S, Visual Cryptography, in "Visual Cryptography in remote voting system", Vidyavardhaka College of engineering, Mysore, Karnataka, India, Asia.
[2] M. Naor and A. Shamir (1995), "Visual Cryptography", Advances in Cryptology-Eurocrypt'94 Proceeding, LNCSvol. 950, Springer-Verlag, pp. 1-12.
[3] Mohammed Ismael Ahmed and Dr. Mohammed Abo-Rizka (2013), "Remote Internet Voting: Security and Performance Issues", 978-1-908320-22/3/$25.00©2013 EEE, Arab Academy for Science and Technology Cairo, Egypt.
[4] Anusha MN and Shrinivas B.K, Visual Cryptography, in "Remote Voting system for corporate companies using visual cryptography", Vol. 2 of Lecture Notes in Computer Science, Springer- Verlag, Berlin, pp. 1–12, 1995.

