© 2016 IJSRSET | Volume 2 | Issue 3 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Online Voting : Using Visual Cryptography

Ginjin Raj, Jithamol P M, Nikhil Narayanan, Aby Abahai T

Department of Computer Science , M. G. University, Kerala , India

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. 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. The information about the original image (Voter Password) will be revealed only after stacking sufficient number of shares. 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.

Keywords: Visual Cryptography, Color Based Authentication

I. INTRODUCTION

The voting percentage of India is very less and is considerably declining day by day. The illiterate people can be fooled and their votes can be cast to different candidates. Also incidents like booth capturing are increasing and some undeserving candidates are getting elected. Thus the objective is to put a stop to all these malicious activities and to safeguard the right of voting of an individual. Thus the plan is to make the voting process a secure and effective one. Visual cryptography scheme is one of the most secure techniques for privacy, that allows the encryption of secret image or data by transferring it into the secure share and the decryption is done without any computation devices.

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.

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. 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 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.

II. METHODS AND MATERIAL

1. Existing System

The Current Voting System is critical to our Election Commission of India for conducting elections and announcing the results because the money involved in employee remuneration and the complexity of the legal requirements is more. In traditional elections, a voter usually goes to the voting stations. After direct person-person verification with some IDs, the voter is allowed to vote. The voter is then given a ballot which allows a single vote. Once the ballot is used, it cannot be used again. However, this ballot must also be anonymous. The ballot must identify the voter as being permitted to vote, but not reveal their actual identity, and the voter must also be given assurances of this. Traditional polling methods trust a lot of parties during the election. The current methods require an attacker interact directly with the voting process to disrupt it. There is a greater chance of getting caught as there will be physical evidence in the traditional polling. On the other end, internet is harder to control and manage the security as Network and internet related attacks are more difficult to trace. In the traditional polling, you know who is in the election room. Also with the internet or network related voting, from all around the world you will have attackers, not only by the few people in the room. In a voting system, privacy and security are desired, but are not always simultaneously achievable at a reasonable cost. In online voting systems, verification is very difficult to do accurately, and anonymity is difficult to ensure.so maintain the security over network is important issue.

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. 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. 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.

2. Proposed System

One of the best known techniques to protect data is cryptography. It is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Naor and Shamir introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations.

A. Visual Cryptography

The main technology applied here is the visual cryptography. In here we use the 2 out of 2 cryptographic method. The main advantage of this method is that the hackers have to put a lot of effort to break the security of the system, which is impossible to do in here.

1) 2 out of 1 Visual Cryptography: The proposed scheme generates the shares of visual cryptography using basic visual cryptography model and then encrypt both shares using RSA algorithm of public key cryptography, in order to secure the secret shares and shares must be protected from the vicious opponent who may try to alter the bit sequences to form the fake shares. During the phase of decryption, secret shares are extracted by RSA decryption algorithm & stacked to reveal the secret image. The methodology of proposed scheme is given below figure 1.

1st Phase Generating the Shares of Secret Image: In this phase implementation of Visual Cryptography is done. It involves the creation of shares from secret image using Visual Cryptography (2, 2) scheme. Very first the secret image is taken and is converted to a binary image then every pixel in the secret image is divided into eight sub pixels, four pixels in each share by selecting the random pixel encoding scheme out of three given in the figure 2.

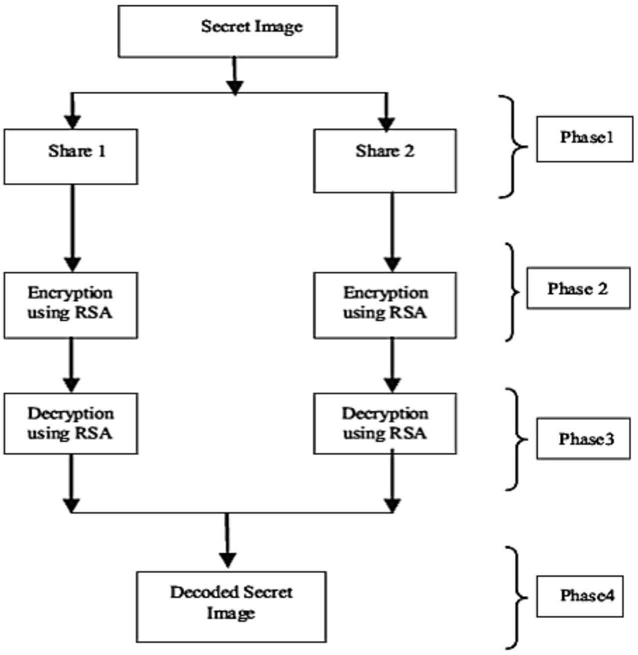


Figure 1. Methodology of system

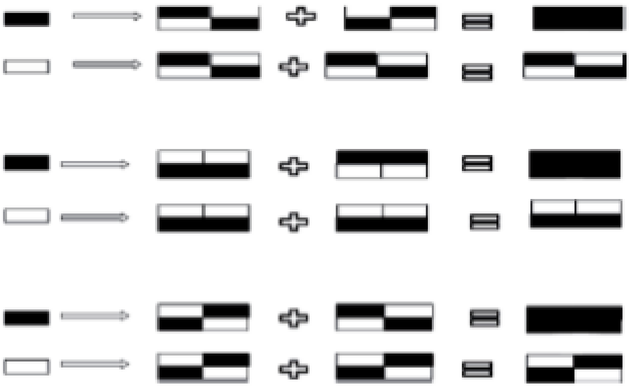


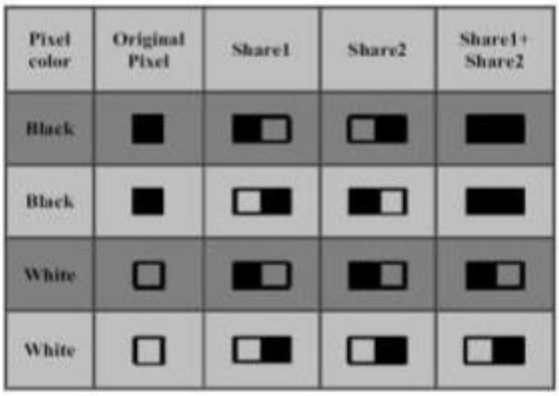
Figure 2. Pixel encoding schemes

2nd Phase Encrypting the generated Shares: This is the second phase of our proposed approach where we will encrypt the shares that are generated in the first phase. The RSA algorithm is taken to encrypt the shares. First we have generated the key for RSA and then we perform the encryption using public key. Thus, encrypted shares are the result of 2nd phase.

3rd Phase Decrypting the Shares using RSA: The process of decrypting the shares takes place at destination side. Using RSA decryption algorithm, we again convert the encrypted shares into their actual form, which were encrypted at the sender side. Here, for decrypting the shares.

4th Phase Visual Cryptography decryption: In the last phase, the process of Visual Cryptographic decryption is performed. Here by applying the binary XOR operation, on both decrypted shares, we are going to get back the original secret image.

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. Figure 3 represents the division of black and white pixel in this schema.



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

Figure 3. Division of pixel

2) Buffered Shares: The basic idea used here is buffered share technology of the visual cryptography. It create to buffered shares as by the algorithm which is mentioning below.

It select pixel density at each point then it assign this pixel density get arranged into to shares according to the value obtained at each pixel density. If the value obtained is an odd add to server side or else add to the client side through which we generate to shares which is an input that provided by the corresponding user. The output from the shares somewhat looks like as in figure 4.

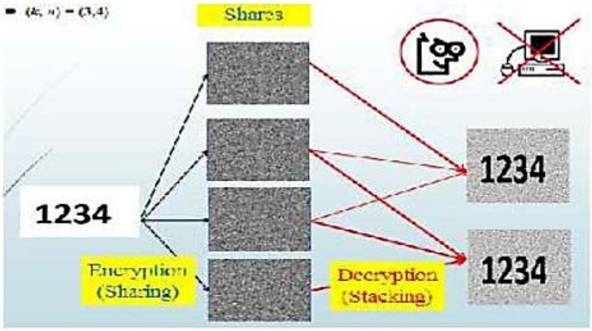


Figure 4. Buffered shares

B. **Color Based Authentication**

The next algorithm which used is the color based authentication technique, which mainly deals with the session passwords. In here we used this method to generate an OTP for users to provide more secure. It's the one of the new technique use now days. In here user generate his own color combination grid for further security enhancement. The user rates each color with a value. The user have different color combination grid upon which the one-time password get generates. During the registration phase user enter the details along with a grid having 8 colors. This color grid are randomly created.

The color grid consist of 4 pairs of color. Each pair of color represents the row and the column of the grid. Depending upon the rating and the color grid entered by the user we get a session password from the 8X8 matrix, which having 0 to 9 randomly placed integers. The first color of every pair in color grid represents row and second represents column of the number grid. The number in the intersection of the row and column of the grid is part of the session password. And this is send to client as an one time password.

III. RESULTS AND DISCUSSION

1. Implementation

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and its constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

A. ***System Design***

The system comprises of three modules namely admin module, client module and server module. The working of the system is as shown in the figure 5. The admin module consists of functions like add/manage user, add/manage candidate, add/manage parties and view votes. The admin can add, update, and delete information related to the users, candidates and parties through this module. The client module consists of the android application installed on the user's smart phone. The application requires the user to register himself after which he needs to sign up using the same username and password as used while registering. Then the user is to select the candidate he wishes to vote. Once the user clicks on the 'Vote' button he is supposed to upload the share 1 sent to him via his e-mail id while the share 2 is automatically uploaded by the server. Authenticated users will be shown a captcha which the users have to enter correctly. Upon entering the captcha correctly the user's vote will be registered successfully.

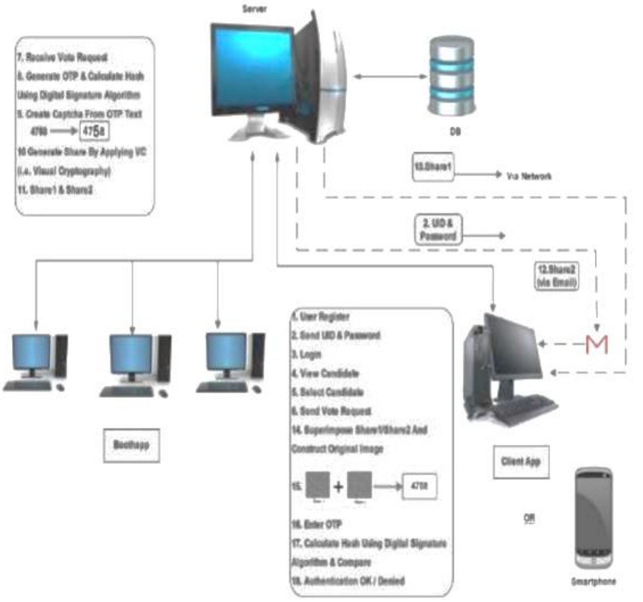

Server
7. Receive Vote Request
8. Generate OTP & Calculate Hash Using Digital Signature Algorithm
9. Create Captcha From OTP Text
4758
4758
10 Generate Share By Applying VC (i.e. Visual Cryptography)
11. Share1 & Share2
DB
13.Share1
Via Network
2. UID & Password
12.Share2 (via Email)
M
1. User Register
2. Send UID & Password
3. Login
4. View Candidate
5. Select Candidate
6. Send Vote Request
14. Superimpose Share1/Share2 And Construct Original Image
15.
+
4758
16. Enter OTP
17. Calculate Hash Using Digital Signature Algorithm & Compare
18. Authentication OK / Denied
Boothapp
Client App
OR
Smartphone

Figure 5. System Architecture

The server module is concerned with generation of shares, generation of captcha and authentication of users. This process of encryption/decryption is illustrated in the fig 1.6.

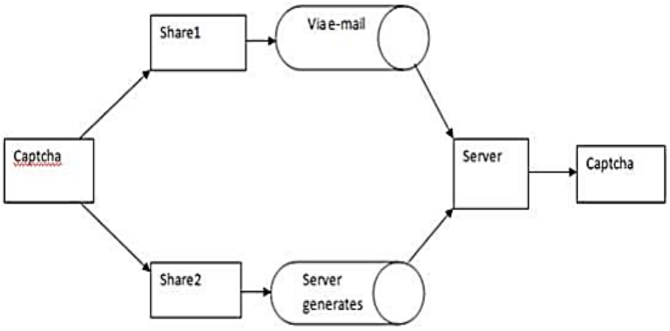


Figure 6. Encryption/decryption

B. **Algorithm Used**

1) *RGB Seperation*:

- Consider the pixel having R, G, and components (in Hexadecimal format) as:- 9966ff where,

99: is R component
66: is G component
Ff: is B component

Next is to perform different Boolean operations on these components

- To obtain B component (AND with ff)

9966ff AND ff
Ans=0000ff
Here ff is the B component

- To obtain G component (right shift by 8-bits AND with ff)

9966 AND 00ff
Ans=66

Here 66 is G component

- To obtain R component (right shift by 16 bits AND with ff)

99 AND ff
Ans=99
Here 99 is R component

2) *Gray Scale (to simplify operations on pixels):*Take the average of all three components which will give grayscale value
GS=R+G+B/3
Thus GS=R=G=B

3) *THRESHOLD(to separate background and foreground image):* If (GS>TH) then
GS= 255 [pixel is white]
Else GS=0 [pixel is black]
Where TH is threshold value which is=128 and GS= Gray Scale value.

IV. CONCLUSION

Online voting using visual cryptography overcome limitations of traditional voting system. This system provide more security, take less time. Also there is no chance of voter frauds and the money spent on security can be drastically decreased. Main aim of this methodology is to provide complete privacy to the voter and to make the best integration of the voting system. The core concept of this system is to use strong security mechanism for voter authentication. Visual cryptography encrypts the information in such a way that decryption can be done without using any mathematical computations. Persons who have an internet connection at home can vote without taking the strain to come to voting booths.

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. Internet-based voting offers many benefits including low cost and increased voter participation. This voting systems 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.

V. 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.