Open access Journal International Journal of Emerging Trends in Science and Technology

Receipt-Free Multi-Authority Voting with (2,2) Secret Sharing Based Authentication

Authors
Ms. Ashwini Walake[1], Prof. Ms. Pallavi Chavan[2]
[1]Student-M.Tech.(CSE), B.D.C.O.E. Sewagram Pin code-442001
Email: *ashwiniwalke2013@gmail.com*
[2]Assistant Professor (Sr.Gr.), B.D.C.O.E. Sewagram Pin code-442001
Email: *pallavichavan11@gmail.com*

ABSTRACT
Election and voting are the important activities in the democratic countries. The traditional voting system becomes inconvenient for the people who cannot visit the polling booth for the vote casting. To overcome the drawback of traditional voting system web based voting systems are introduced. Security is an important issue in the web based voting system. The proposed system provides secured authentication through the visual secret sharing scheme.

Keywords: *Secret Sharing, Visual cryptography, Shares, Authentication.*

1. INTRODUCTION

For the democracy trustworthy elections are essential. Voting is the way to choose the representative for the democracy. It is a complex process which involve voter registration, voter authentication, voter casting, tallying and auditing. For the trustworthy election authentication is an important issue. It is important to establish trust between human to human and human to computer. Hiding secret for authentication is important in online voting system

Secret sharing is a method for splitting the secret. It distributes the secret among group of participants. Each of the participant is allocated with a share. The secret can be reconstructed only if sufficient number of shares are produced at the time of reconstruction. Individual share is of no use. It does not give any information about the secret. The authority who produces the shares and distribute among the group of participants is called as the dealer.

Visual cryptography is a new technique to solve the problem of secret sharing. Visual cryptography is use to hide the secret in the form of image. It consider the original image as a secret. The secret image is encrypted in the number of shares. At the time of decryption specified number of shares are collected and secret is recovered by the superimposing i.e stacking the specified number of transparencies. Visual cryptography does not require any mathematical computation to recover the secret. In proposed scheme we provide authentication through the visual cryptography. The system should satisfy the following requirements.

Unreusability- Voter should not be able to vote twice.

Eligibility- Only eligible voter should be able to vote.

Fairness- Nothing should affect the voting process. No one should be able to indicate the tally before vote counting.

Uncoerciability- Voter should not able to prove his vote and voter should not be forced to vote.

Receipt-freeness- Voter should not be able to prove his vote.

Privacy- All votes must be secret.

2. RELATED WORK

Number of visual cryptographic schemes are available. Some of the visual cryptographic schemes are described below.

(2,2) visual cryptography scheme

(2,2) visual cryptography is a simplest type of visual cryptography. This scheme divides the secret in two shares and for the reconstruction it requires both the shares. In our scheme for remote voting system we are using (2,2) secret sharing scheme for authentication purpose. Following figure represents the division of black and white pixel.

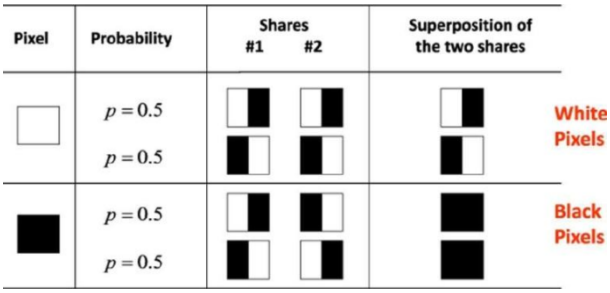

Fig1. Illustration of (2,2) visual cryptographic scheme with 2 subpixel construction.

(k,n) visual cryptography

In (k,n) visual cryptography scheme the secret is divided into n number of shares and at the time of reconstruction it requires k shares among n number of shares. The drawback of (k,n) visual cryptography is user have to maintain many shares. This system can be used in the banking system for the authentication of joint account user.

(k,k) visual cryptography

In (k,k) visual cryptography the secret is divided into k number of shares . for the reconstruction of secret it requires all k shares. Drawback of (k,k) visual cryptography is memory consumption is more.

In May 2008, Kh. Mangium Singh, Sukumar Nandi, S. Birendra Singh and L. Shyamsundar Singh proposed a scheme for stealth steganography in visual cryptography for halftone images. It is a cheating detection method in visual cryptography. Author used the steganography concept for hiding the digital signature. It convert the digital signature in binary form and for hiding the 0 it does not perform any change in subpixel of share. And for hiding 1 it performs flipping of white(black) subpixel in one of the block of black (white) subpixel of share. All shares are required to recover the hidden signature.

In 2010, P.S. Revenkar, Anisa Anjuman and W.Z. Gandhare gives a system to provide secured authentication using visual cryptography. Author uses iris image for the authentication. It provide more security.

In March 2012, Mrs. A. Vinodini, M. Premanand and M. Natarajan proposed a scheme for trustworthy authentication using visual cryptography. It uses two factor biometric system. It involve manual intervention and integrity of user. It accept biometric image from user and perform steganography with pin number.

In Jan. 2013, R. Yadagiri proposed a secure visual cryptography. This scheme avoids cheating. The dealer takes secret image and verification image these two images are encoded to form the shares. One secret share and verification share send to participant. It uses random number generator to form the shares.

In Feb. 2013, B. Priyanka and E. Purushottam proposed a visual cryptographic technique for authentication of grayscale image. For authentication image is transformed into binarized block in which the watermark is embedded and then Shamir's secret sharing scheme is used to form shares. For reconstruction reverse shamir's secret sharing scheme is applied. The reconstructed image is used for authentication. It checks the watermark.

In May 2013, S. Kavitha Murugesan and Shanavas K. A proposed a scheme for secure image authentication of grayscale image using

secret sharing method and chaotic logistic map with data repair capability. The authentication signal is generated by each block of gray scale image. It is transformed into shares using shamir's secret sharing scheme. The PNG image is form by combining original grayscale image with alpha channel plane. The stego image is form by encrypting PNG image by chaotic logistic map. This stego image is decrypted for authentication. If authentication fails then data repairing is performed on the tampered block.

In May 2013, Mrs. A. Angel Freeda, M. Sindhuja and K. Sujitha gives authentication scheme using visual cryptography. It uses capatcha image for authentication. This scheme solve the problem of phishing attack. It uses textual keyword for validation. It uses splitting and rotating algorithm. It generate capatcha image dynamically.

In June 2014, Pooja, Dr. Lalitha Y.S. proposed a scheme for non expanded visual cryptography for color images using pseudo randomized authentication. This scheme is based on pixel reversal, randomized reduction in original pixel and subtraction of this original pixel. This scheme discloses reduced pixel expansion required for retrieval of the secret image. There is no loss in contrast of the decrypted image.

In 1979, Adi Shamir[1], proposed a scheme to share the secret among the group of users to provide the better security. If the secret D is distributed into n shares then it can be rebuilt from any (k+1) or more shares. Secret can not be reconstructed using k or less shares.

Cramer et al[9] gives a new model for election. This model uses some properties of homomorphic encryption technique. It uses homomorphic operation $\oplus$ for the message space and an operation $\otimes$ for the cipher space. If the encryption of any two votes is E(v1) and E(v2) then product of E(v1) $\otimes$ E(v2) is nothing but E(v1$\oplus$ v2) encryption of two votes.

3. PROPOSED METHODOLOGY

The election system should be secure and robust against a variety of fraudulent actions. Authentication, scalability, and accuracy these are important criteria's to be satisfied by a typical voting system. Authentication can be considered as the most important issue among all the above mentioned criteria. As the role of online voting system is crucial, it is difficult to come up with a system which is highly secure & accurate in all senses. In this project we have implemented the security mechanism by means of Shamir's secret sharing scheme.

Following fig shows the phases of the voting system.

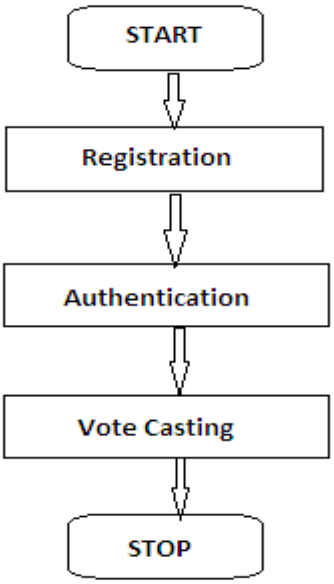

Fig 2. Phases of the proposed scheme.

1. Registration Phase:

First step in voting system is a registration process. While registration process voter have to provide the user name, password along with the recent photo and signature of the voter. The server will make entry in voter table in database and send the signature of the voter as a secret image to the matlab. While storing the entries in the database it will perform the encryption on the password. For password encryption it uses SHA1 cryptographic algorithm.

Share Formation:

Server sends the signature as an secret image to the matlab. Matlab accept the image and perform encryption using Shamir's (2,2) secret sharing algorithm.

Algorithm to form shares

Input: d is secret in the form of an integer, n is number of participants, and k is threshold .

Output: shares for the n participants to keep.

Step 1. Choose randomly a prime number p that is larger than d.

Step 2. Select (k-1)integer values c1,c2….c_{k-1} within the range of 0 to p-1 .

Step 3. Select n distinct real values x1,x2….xn.

Step 4. Use the following (k-1)-degree polynomial to compute n function values ,F(xi) called *partial shares for i=1,2…n.*

$F(x_i)=(d+c_1x_i+c2x_i^2….+c_{k-1}x_i^{k-1})$ mod p

Step 5. Deliver the two-tuple (xi,F(xi))as a *share to the ith* participant where i=1,2…n.

Using above algorithm matlab will divide the secret image into two shares. These two shares are transfer to the server. Server will send one share to the voter and saves the entries of user name, password in the hashed form and the second share to the database. Voter have to remember the user name and password and also have to keep voter share safely for log-in process.

2. Authentication Phase:

Authentication is the important part of the online voting system. For vote casting voter have to log-in first. Voter have to produce user name password and the voter share which is given to the voter at the time of registration process. After uploading user name, password and voter share, server will take user name and password match the entered password with the stored password in the database if matched then it retrieve the share and original secret image stored in the database with the entry of user name and password. The voter share, server share and secret image are transferred to the matlab. Matlab perform inverse (2,2) Shamir's secret sharing algorithm and reconstruct the image. If the reconstructed image is matched with the original image then matlab will send 1 to the server and log-in will be successful.

Algorithm for reconstruction

Input: k shares collected from the n participants and the prime number p .

Output: secret d hidden in the shares.

Step 1. Use k shares

$(x1,F(x1)),(x2,F(x2))……(x_k,F(x_k))$

To form

$F(x_i)=(d+c_1x_i+c2x_i^2….+c_{k-1}x_i^{k-1})$ mod p

where i=1,2….k.

Step 2. Solve the k equations above by Lagrange's interpolation to obtain as follows

$d=(-1)^{k-1}[F(x_1)*(x_2x_3…..x_k)/((x_1-x_2)(x_1-x_3)….(x_1-x_k))$

$+F(x_2)*(x_1x_3…..x_k)/((x_2-x_1)(x_2-x_3)…..(x_2-x_3))…….$

$+F(x_k)*(x_1x_2….x_{k-1})/((x_k-x_1)(x_k-x_2)….(x_k-x_{k-1}))]$ mod p

Here d is the original secret.

3. Vote Casting:

After authentication process done if the voter is a valid voter then voter can cast his/her ballot. Vote duplication is avoided no voter can cast vote more than one.

4. RESULT ANALYSIS

In this section some of the requirement for efficient voting system are evaluated for our system.

Security: Security is an important parameter in any online voting system. In our system we are providing the security through the authentication mechanism. Voter can login to cast the vote only if he is a authenticated one for that voter have to produce the valid share.

Mobility and Convenience: This is one of the features that most end to end system could not provide. Many of the end to end system use one or more election technologies that force the user to vote in particular location. Here we offer remote voting so that voter can cast the vote irrespective of location.

Eligibility: Only those voters who have been registered and authenticated can become the eligible voter and thus only eligible voters will only able to express their right.

Receipt-free: the proposed scheme is receipt free as the voter can not reveal his/her ballot to the others. It doesn't produce any receipt for the cased vote.

Uncoercibility: In the proposed voting system the voter cannot be coerced into casting a particular ballot by coercer. As our scheme is receipt free voter can prove to whom he has casted vote. Hence it satisfy the requirement of uncoercability.

Comparison of different voting schemes is shown in following table.

Table 1. Comparison of various voting systems.

Scheme	Benefits	Drawback
Traditional Paper Based Scheme	It is very simple. Illiterate people can cast vote.	Very much time consuming. Booth capture is the major drawback.
Blind signature based scheme	This are simple and efficient schemes. It uses flexible vote format.	Blind factor can be used as receipt.
Mixnet based scheme	Shuffling of mix servers makes votes unlinkable.	It requires huge operations for shuffling.
Homomorphic encryption based scheme	Homomorphic schemes directly combines encrypted votes to get the tally.	It requires the huge concern of zero knowledge proog.
Proposed scheme	Simple to interact. Voter can cast vote irrespective of location. Very much secured. Two way security is provide through password encryption using SHA1 and Shamir's secret sharing algorithm.	User should have the basic knowledge of computer.

5. CONCLUSION

Online voting systems are more advantageous as compare to the traditional voting system as it offers low cost of establishing the election process. And it also increases the percentage of voter participation. Along with this the system should be secured thus here we are providing the security through the authentication.

REFERANCES

1. Kh. Manglem Singh, Sukumar Nandi, S. Birendra Singh, L. Shyamsundar Singh."Stealth steganography in visual cryptography for HalfTone Images", *proceeding of the International Conference on Computer and communication Engineering,2008,IEEE*. pp. 1217-1221.
2. P.S. Revankar, Anisa Anjum, W.Z. Gandhare,"Secure Iris Authentication using Visual Cryptography", *IJCSIS*, Vol. 7, No. 3,2010, pp. 217-221.
3. Mrs. A. Vinodini, M. Premanand, M. Natarajan,"Visual Cryptography Using Two factor Biometric System for Trustworthy Authentication", *International Journal of scientific and Research Publication*, vol. 2,Issue 3, March 2012,pp. 1-5.
4. R. Yadagiri Rao,"Secure Visual Cryptography ",International Journal of Engineering and Computer Science, vol. 2, Issue 1, Jan. 2013,pp. 265-303.

5. B. Priyanka, E. Purushottam,"A survey on Authentication for Grayscale Images Based on Visual Cryptographic Technique", *International Journal of Modern Engineering Research*, vol. 3, Issue. 1, Jan. – Feb. 2013, pp. 354-359.
6. S. Kavitha Murugesan, Shanavas K. A. "Secure Image Authentication of a Grayscale document using Secret Sharing Method and Chaotic Logistic Map with Data Repair Capability", *International Journal of Innovative Technology and Exploring Engg*., vol. 2, Issue. 6,May. 2013, pp. 232-235.
7. Mrs. Angel Freeda, M. Sindhuja, K.Sujitha,"Image Captcha Based Authentication using Visual Cryptography", *International Journal of Research in Engineering and Advance Technology*, Vol. 1, Issue 2, April- May 2013, pp. 1-6.
8. Pooja,Dr. Lalitha Y.S,"Non Expanded Visual Cryptography for Color Images using Psuedo- Randomized Authentication", *International Journal of Engineering research and development*, Vol. 10, Issue 6, June 2014, pp. 1-8.
9. Adi Shamir, 1979, "How to Share a Secret", *in Communications of ACM*, Vol.22, no.11, pp. 612-613.
10. R. Cramer, R. Gennaro and B. Schoenmakers, 1997,"A Secure and optimally Efficient Multi- Authority Election scheme" *in EUROCRYPT 97, LNCS 1233,Springer-verlag*,pp.103-118.