ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

Secure Online Polling System Using Visual Cryptography

Swati Yogesh Shinde, Prof. Amrit Priyadarshi

PG Scholar, Department of Computer Engineering, Dattakala Faculty of Engineering, Pune, Maharashtra, India

Professor, Department of Computer Engineering Dattakala Faculty of Engineering, Pune, Maharashtra, India

ABSTRACT: Being biggest democratic nation trustworthy elections are essential. The processes of Election is very complex and it involve many processes including voter registration, candidate registration, ballot preparation and distribution, voter authentication, vote casting, tabulation, result reporting, auditing, and validation. To make the process more secure and reliable, the standard mechanism should be deployed. Remote Voting system considers security & human factors carefully and mainly considers that they provide voters reliable and intuitive indications of the validity of the voting process. This gives rise to the concept of Secure Online polling System Using Extended Visual Cryptography; such a technique thus would be lucrative for security. It offers many benefits including low cost, increased voter participation and consider human factor carefully.

KEYWORDS: Visual cryptography, Visual Cryptography Scheme (VCS), ADHAAR ID, Secret image, share process, polling process

I. INTRODUCTION

Online polling System Using Extended 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 implementing the features provided by the extended VC. 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 shares using extended VC scheme. Voter will get the secret password to cast his vote by combining shares using extended 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. This stacking of shares can be done in decryption process.

II. LITERATURE SURVEY

Naor and Shamir [8] proposed a visual cryptographic scheme, i.e. contrast and expansion scheme. The basic model consists of printed page of cipher text that can be sent by mail or faxed and printed transparency serves as a secret key.The original cleartext is revealed by placing the transparency with the key over the page with the ciphertext.Adi Shamir[7] proposed (k,n) threshold scheme where the data 'D' is divided into D1...Dn pieces in such a way that 'D' can be reconstructable from 'k' pieces,however even (k-1) pieces will reveal nothing about 'D'.Rajendra and Sheshadri[6] proposed 2 out of 2 scheme in visual cryptography for conducting elections for a corporate company for their various internal posts.The system fascilitate their voter to caste their vote from any remote place.The system makes use of secret sharing scheme in which image is converted into two shares each with dotted black and white dots .The original image(voter password) will be revealed only after stacking two shares. Wholchock and Wustrow [10]described the digital vote by mail (DVBM) system. The system was a pilot project by Washinton, D.C for their overseas absentee voters to allow to caste their ballots using website.P.Shankar[1] , G.Atense[2] and Kai Hui[9] propsed 'k out of n'secret image sharing scheme where the secret image will be revealed when 'k' number of shares out of 'n' shares are stacked together.

III. 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 to maintain the security over network is important issue.

IV. PROPOSED SYSTEM

The basic idea is that the Candidates can poll their votes from anywhere during election time.

Features of proposed system:-

1. Remote access voter
2. High Security
3. Session Management
4. Reduced paper-work and human efforts
5. Centralized Administration

That all features can be obtained by implementing the extended visual cryptography.The proposed methodology is implemented using Zk framework. Fig 1, Shows the system architecture. In the registration phase the most important part is the creation of shares from the secret image where one share is kept with the user and of rest of the share can be kept with the server. For login, the user needs to enter a valid username and password which is provide by OPS system at the time of registration. So it is two layer security. This is implemented through extended visual cryptography using k out of n scheme.

IV. A SYTEM ARCHITECTURE

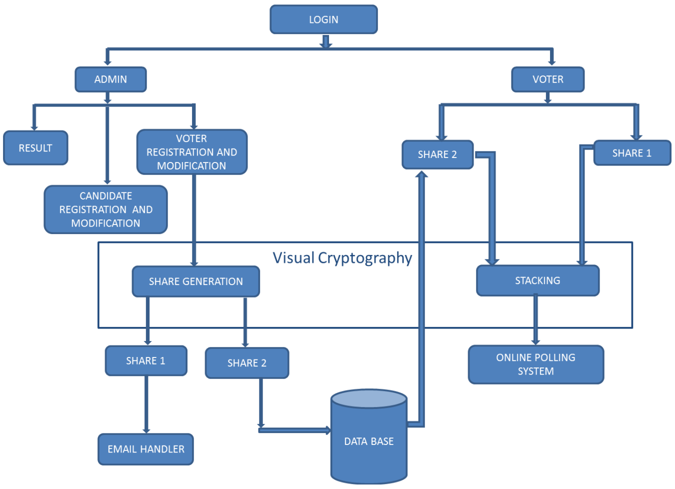


Fig. 1 System Architecture

B MAIN MODULES

1. Admin
2. Voter Registration
3. Voter modification
4. Candidate registration
5. Candidate modification
6. Share process
7. Email handler
8. Polling process
9. Result

Modules Description:

1. Admin

Admin module controls generation of election, voter registration, voter modification according to user/voter request, candidate registration, candidate modification, election generation process and displaying result.

2. Voter registration

Voter registration module controls registration process of the new user/voter in the supervision of admin.

3. Voter modification

Voter modification module controls the modifications of the already registered user/voter's information as per the request to the admin.

4. Candidate registration

Candidate registration module controls the registration process of the candidate who is nominated for election.

5. Candidate modification

Candidate modification module controls the modification of the candidate who was previously registered as a candidate in election process.

6. Share process

Share process module controls generation and stacking of the shares.

7. Email handler

Email handler module sends mail containing one of the shares generated in the voting process.

8. **Polling process**

Polling process module handles polling process.

9. Result

Result module displays result of the election. Result can be displayed only by the admin.

Algorithm:

1. Generate the secret image from user's unique ADHAAR ID.
2. Convert the secret image into no of shares (Encryption method).
3. Send one share out of ‘ n ‘ share to the voter email ID and send rest of the shares to the OPS database system.
4. Authentication can be done using stacking of shares from both side such as download share from voter email ID and rest of the share fetch from OPS database.
5. Comparison between secret image and stacked image will decide if voter is valid or not.

V. PERFORMANCE EVALUATION

For evaluating the performance of the system, following metrics are used

- NPCR is number of pixel changing rate in the share image.
- UACI is the unified average changing intensity and it gives the measure of intensity of differences between the secret image and share images.

$$D(i,j) = \begin{cases} 0, if\, C^1(i,j) = C^2(i,j) \\ 1, if\, C^1(i,j) \neq C^2(i,j) \end{cases} \quad (1)$$

$$\text{NPCR: } \mathcal{N}(C^1, C^2) = \sum_{i,j} \frac{D(i,j)}{T} \times 100\% \quad (2)$$

$$\text{UACI: } \mathcal{U}(C^1, C^2) = \sum_{i,j} \frac{|C^1(i,j) - C^2(i,j)|}{F \cdot T} \times 100\% \quad (3)$$

The range of NPCR is [0, 1].

Scheme	NPCR(%)	UACI(%)
Proposed	99.60	32.58
Huag[4]	98.70	27.46
Ye[5]	98.75	37.68

Table 1: Performance evaluation

The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI) are two most common quantities used to evaluate the strength of image encryption algorithms/ciphers with respect to differential attacks. Conventionally, a high NPCR/UACI score is usually interpreted as a high resistance to differential attacks. Proposed method gives the better values.

VI. HISTOGRAM ANALYSIS

An image histogram is a graph showing the number of pixels in an image at each different intensity value found in that image. The histogram of cipher-image should have uniform distribution and is completely different from that of the plain-image. The histogram of a plain image Jane and the cipher image are plot in the following figures. The histograms of cipher-image are fairly uniform and significantly different from those of the plain image. They imply that there is no useful statistical information in the cipher-image for an attacker to launch any statistic attacks to the cryptosystem.

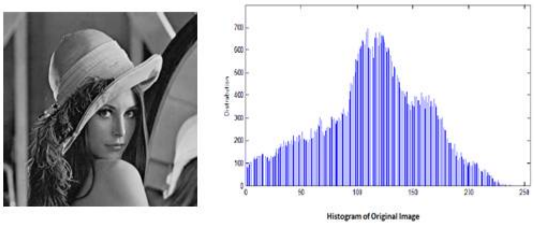


Fig. 2. Histogram of Secret Image

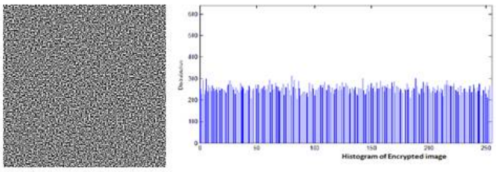
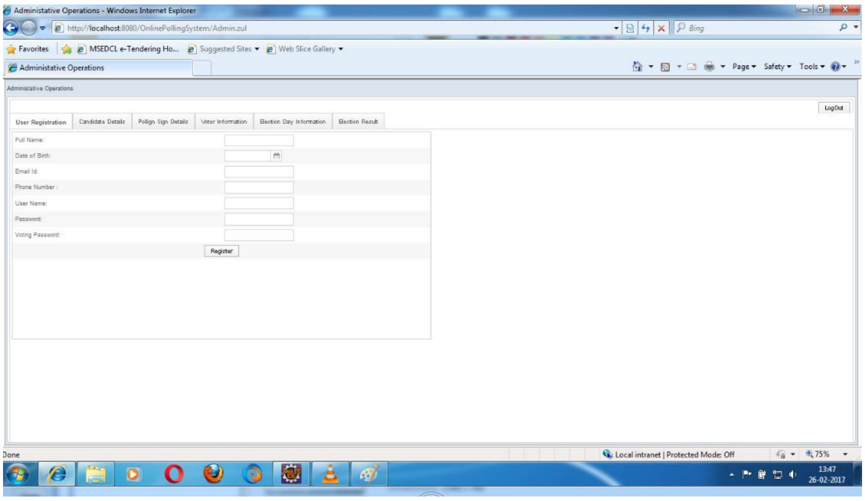


Fig.3 Histogram of Share image

VII.EXPERIMENTAL RESULTS


Administative Operations - Windows Internet Explorer

http://localhost:8080/OnlinePollingSystem/Admin.zul

Administative Operations

User Registration | Candidate Details | Pollign Sign Details | Voter Information | Election Day Information | Election Result

Full Name:

Date of Birth:

Email Id:

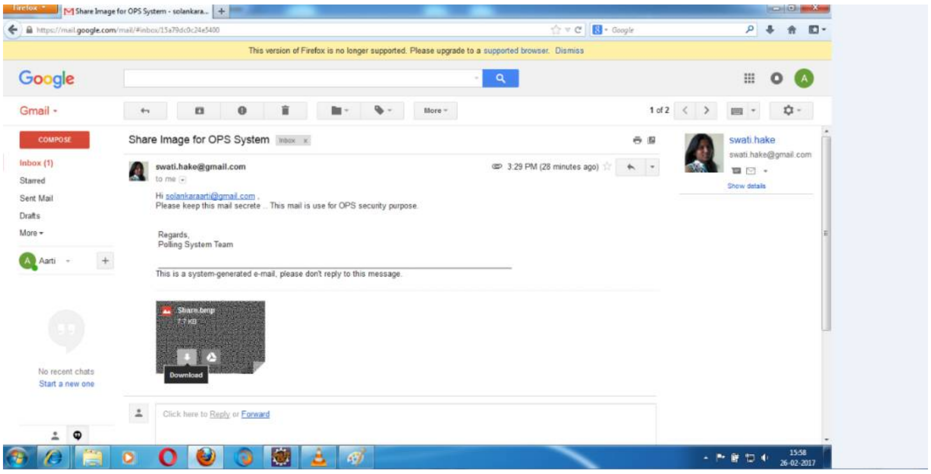
Phone Number :

User Name:

Password:

Voting Password:

Fig.4. Admin operation


This version of Firefox is no longer supported. Please upgrade to a supported browser. Dismiss

Share Image for OPS System

swati.hake@gmail.com
to me

3:29 PM (28 minutes ago)

Hi solankaraarti@gmail.com ,
Please keep this mail secrete .. This mail is use for OPS security purpose.

Regards,
Polling System Team

This is a system-generated e-mail, please don't reply to this message.

Share.bmp
7.7 KB

Click here to Reply or Forward

Fig.5 User share to the email ID

VIII.OBSERVATIONS

Better encryption strength giving high values of NPCR and UACI thereby better encryption strength against differential attackcs. There is no statistical information in the share image so that it can be manipulated to create a fake share. Thereby no chance to launch any attack in the encryption system.

IX. ADVANTAGES

Visual Cryptography separates a secret image into two parts knows as shares which give no hint about the secret image. The secret image is revealed only whe shares are combined together by superimposition. First advantage is , it is simple to use and no mathematical computations required to reveal the secret image. Secondly, those who don't posses any knowledge about of cryptography can indirectly gets involved in the process of decryption.

X. CONCLUSION

The propose system is very useful and safe for online polling. This system is web based application so that it can be accessed by any authorized person anywhere in the world through internet. This is two layer security which is useful to avoid the unauthorized users. Online Polling System offers many benefits including low cost & increased voter participation. Remote Voting system considers security & human factors carefully and mainly considers that they provide voters reliable and intuitive indications of the validity of the voting process.OPS is currently not used in India. To simplify job of election officers, to provide fast election process, with minimal cost, reliable and secure process, the remote voting systems are evolved. In traditional voting system there was no strong security mechanism for voter authentication. With traditional 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. 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.

ACKNOWLEDGEMENT

I would like to express my gratitude towards my guide prof. Amrit Priyadashi and H.O.D of computer engg. Department Prof. Sayyed M. M for their support and guidance in my work.

REFERENCES

[1] K.Shankar,Dr. P. Eswaran," A new k out of n Secret Image Sharing Scheme in Visual Cryptography,"10th Int. Conf. On Intelligent Systems and Control,Nov. 2016
[2] G.Atenise,C.Blundo,A.D.Santis and D.R.Stinson,"Visual Cryptography for general access structures,"*Inform. Comput.*,Vol.129,pp.86-106,1996
[3] Pei-Ling Chiu and Kai-Hui Lee,"A Simulated Annealing Algorithm for Genral Threshold Visual Cryptography Schemes," *In.Forensics and Security*,Vol.6,No.3,2011,pp.992-1001
[4] C.K.Huang,H.Nien,"Multi Chaotic Systems based shuffle for image encryption," *Elsevier Optics Commun*.,2009,pp.2123-2127
[5] R. Ye, "A novel Chaos-Based Image Encryption Scheme with an efficient permutation on Diffusion mechanism," *Elsevier Optics Commun*.,2011,*pp*. 5290-5298
[6] Rajendra A. ,B and Sheshadri H. S," Visual cryptography in Internet Voting System, " *Int. Conference On Security*,pp.60-64,2013
[7] Adi Shamir(1979),"How to share a Secret, "Communication *of ACM*, pp. 1979,pp.612-613
[8] M. Naor and A. Shamir "Visual Cryptography," *Springer* ,1995,*pp*. 1-12
[9] Kai-Hui Lee and Pei-Ling Chiu,"An Extended Visual Cryptography Algorithm for Genral Access Structures,"*In. Forensics and Security*,Vol.7,No.1,2012,pp.219-229
[10] Scott Wolchok,Hari Eric Wustrow ,"Attacking the Washington D.C Internet Voting System",In proc. Int. Conf. on Financial and Data Security 2012,pp.1-18

BIOGRAPHY

MRS. SWATI YOGESH SHINDE Pursuing Master of engineering (M.E. COMPUTER), from Dattakala Faculty of Engineering, Pune