www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 6 June 2015, Page No. 12340-12344

Online Polling System Using Extended Visual Cryptography

Pooja Jadhav, Mayuri Pawar, Pramod Ahire, Vishesh Kumar, Prof J.B. Kulkarni

Department of Computer Engineering
Sinhagad College of Engineering, Vadgaon (BK),
Pune, Maharashtra, India

Abstract:

Trustworthy elections are essential to democracy. The process of Election is complex and involve many components including voter 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. 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. 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.

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.

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.

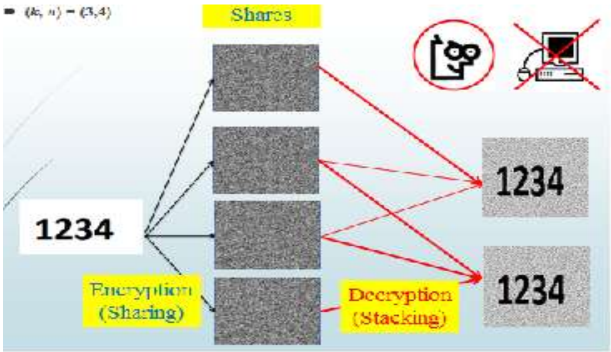
Proposed System: The basic idea is that the Candidates can poll their votes from anywhere during election time.

Features of proposed system:-

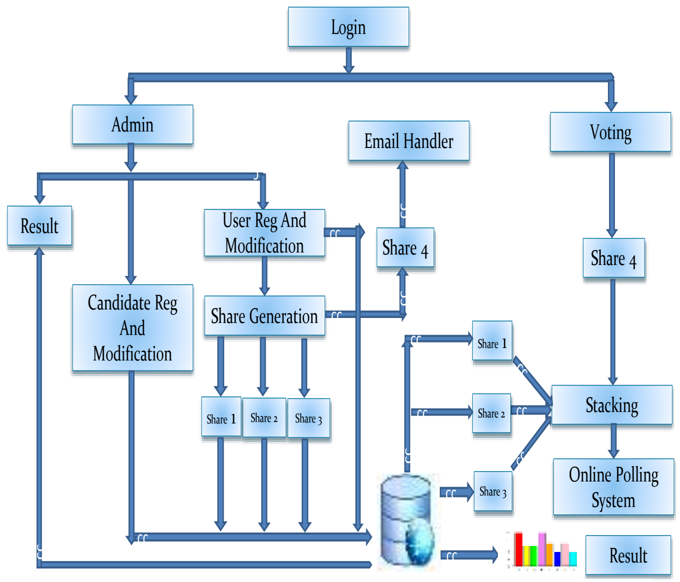
1. Remote access voter
2. High Security
3. Session Management
4. Reduced paper-work and human efforts
5. Centralized Administration

That all features can be obtained by implementing the extended visual cryptography. The proposed methodology is implemented using Zk framework. Fig 5, Shows the result of creation and stacking of shares. 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.

Example:-



System Architecture:



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 voter 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.

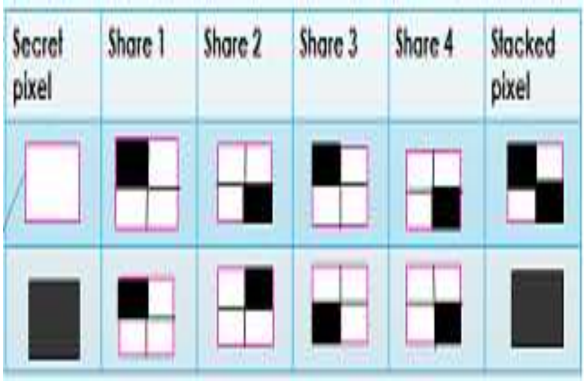
4. Authentication can be done using stacking of shares from both side such as download share from voter email ID and rest of the share fetch from OPS database.

5. Comparison between secret image and stacked image will decide if voter is valid or not.

Algorithm for Encryption:

1. Initialize initial white matrix.

2. Initialize initial black matrix.



3. Initialize white matrix-

$$\begin{pmatrix} 1\ 0\ 0\ 0 \\ 0\ 0\ 0\ 1 \\ 1\ 0\ 0\ 0 \\ 0\ 0\ 0\ 1 \end{pmatrix}$$

4. Initialize black matrix-

$$\begin{pmatrix} 1\ 0\ 0\ 0 \\ 0\ 1\ 0\ 0 \\ 0\ 0\ 1\ 0 \\ 0\ 0\ 0\ 1 \end{pmatrix}$$

5. Generate permutation for index matric m=n! (where n is no of subpixel)

C0={All matrices obtained by permutation for white pixel }

C1={All matrices obtained by permutation for Black pixel }

6. Using pixel grabber java class readout all pixels of the original image.

```
For (x=0; x<width; x++)
     {
          for (y=0; y<height; y++){
            p= getpixel ((x, y)! = 0);
          encrypt.pixel[] = encrypt(p);
          }
     }
```

7. .Encrypt() {

```
1.Identify pixel.
2.Use random sequence generator to use particular permutations
          x= random(1…m)
3.Select index matrix from the set of permutations matrices C0 or C1 based on whether pixel is white or black.
4.Transepose matrix reorder column operation
           result[0]=share1[p];
           result[1]=share2[p];
           result[2]=share3[p];
           result[3]=share4[p];
5.return result;
}
```

Conclusion & Future Work:

At present our government is spending more than 125 crores for conducting a Lok-Sabha election. This money is spent on issues such as security, electoral ballots etc. The average percentage of voting is a less than 60% .Moreover voting fraud can be easily done in the present system. Also the percentage of literates coming to vote is very less. But with our system the money spent on election can be reduced to less than 10 crores.

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. In near future we can even implement the system in mobile application. The user can access through mobile phone and cast the vote.

References:

- M. Naor and A. Shamir, Visual Cryptography, Springer
- Moni Naor and Adi Shamir, "Visual Cryptography", advances in cryptology–Eurocrypt, pp 1-12,1995.
- http://ieeexplore.ieee.org/visual cryptography, Zhi Zhou; Arce, G.R.; DiCrescenzo
- http://en.Wikipedia.org/wiki/file format
- http://www.iosrjournals.org / Anti Phishing Method Based on Visual Cryptography
- http://www.ijetae.com/A Visual Cryptographic Encryption Technique for Securing Medical Images
- Young-ChangHou∗ Department of Information Management, National Central University, Jung Li, Taiwan 320, ROC Received 6 June 2002; accepted 26 August 2002
- International Journal of Computer Applications (0975 – 8887) Volume 25– No.11, July 2011 / k-n Secret Sharing Visual Cryptography Scheme on Color Image using Random Sequence
- International Journal of Science and Advanced Technology (ISSN 2221-8386) / an introduction to different types of visual cryptography schemes
- International Journal of Scientific and Research Publications, Volume 3, Issue 3, March 2013 / An Implementation of Algorithms in Visual Cryptography in Images.

POOJA JADHAV, pursuing computer engineering (B.E.), from Sinhagad College Of Engineering, Email: pjjadhav153@gmail.com

MAYURI PAWAR, pursuing computer engineering (B.E.), from Sinhagad College Of Engineering, Email: mayuripwr28@gmail.com

PRAMOD AHIRE, pursuing computer engineering (B.E.), from Sinhagad College Of Engineering, Email: pamahire.ahire@gmail.com

VISHESH KUMAR, pursuing computer engineering (B.E.), from Sinhagad College Of Engineering, Email: vishurox07@gmail.com