Secure E-vote Using Visual Cryptography

Sai Abhinav Sikhakolli
KKR & KSR Institute of Technology and Sciences
saiabhinavsikhakolli@gmail.com

Lokesh Thadiparthi
KKR & KSR Institute of Technology and Sciences
lokesh55555xyz@gmail.com

Dayakar Reddy Vajrala
KKR & KSR Institute of Technology and Sciences
vajraladayakarreddy246@gmail.com

Velineedi Venkata Ajay Kumar
KKR & KSR Institute of Technology and Sciences
ajaykumarvelineedi@gmail.com

ABSTRACT

Visual Cryptography is a technique that's used for the encryption the data using SHA-256 or SHA-512 algorithm and the data is transformed in the pixel of the images, each image is treated as a shared keys, the decryption of the image is decrypted using those two shared keys by overlapping the images or using any decryption algorithm to obtain the original data and that data is used to our required purpose. In the voting process there is a probability of tampering the data using the phishing attacks to capture the credentials to register the vote in online. So by using the Visual cryptography concept the security of the online voting is much higher and easy to cast our vote. The above process which follows the CIA traid(Confidentiality, Integrity, Accessability).

CCS CONCEPTS

• Image Encryption, Image Decryption, Plain Text, Shared keys

KEYWORDS

Visual Cryptography, Shared Keys, Encryption, Decryption, Pixels

1 INTRODUCTION

Generally the elections are conducted in five phases.

- Filing of Nomination
- Analysis of Nomination
- Campaigning for Elections
- Voting Day
- Vote Counting and Result Declaration

Here we mainly discuss about the voting day, Because the all votes are counted as per the votes casted by the voter. These votes are very valuable and can change the life of our country as well as country GDP and so on. So many aspects are depends on our vote that we are casting in our elections. So in offline Voting there is a chance of tampering the data using the Electronic voting machines.

Electronic voting has also resulted in a substantial decrease in the number of rejected votes. While on a paper ballot an unclear stamping can lead to a rejection of the ballot, an EVM allows only one push of a button to register a vote. The paper finds that the introduction of EVMs led to the elimination of almost all rejected votes resulting in a 2.7 percent increase in the number of valid votes at the baseline. In an election with narrow margins of victory, such an improvement could change the outcome.

So our main aim is to prepare a well and secured voting System, I preferred Online because of in future everything is online, and the data transmission is very high in future, so e-voting is the best way to implement the elections.

2 Existing Problems with the e-vote

Online voting in elections might seem like a logical step forward considering the many other daily activities, like banking and shopping, that we complete online. However, voting online does present unique challenges that usually don't apply to other internet-based processes. These challenges are related to a variety of factors, including the security required for online voting, legal requirements and frameworks, public opinion, and investment.

With the help of malwares like adware, spyware ,ransomware etc, These malwares compromise the system security and data stolen by the attackers, they may be very confidential data in our system.

One of the cyber attack is most commonly used to Stole the data by creating the clone page of the site. With the help of this attack the e-vote deatails gonna stolen and this type of attack is called as phishing.

3 Proposed Solution

Our proposed solution is while sharing the secret key through the email the intruder grab the data and decrypt the content using bruteforce approach and easy to crack the data.

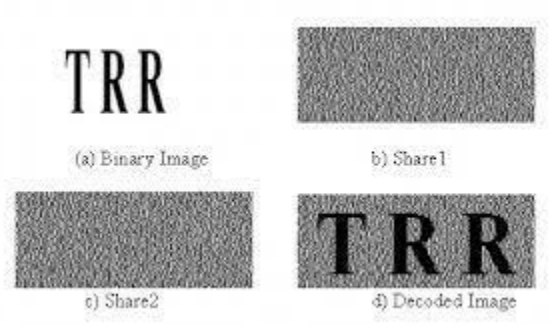
So instead of sharing a key, we shared an VC image generated by the Image encryption algorithm and send through the email, Even the intruder can capture the packet or data, He doesn't do anything with that data because of its encryption form in pixels.

The Image encryption algorithm is:

- **Step 1:** An input image will be selected. It must be an RGB image.
- **Step 2:**Red, Green and blue Channels are separated from an input Image.
- **Step 3:** Each Channel is then further encrypted into 8 shares. This encryption will depend on key used.
- **Step 4:** From Step 3, we get 24 shares, it means each channel has 8 shares each. These 8 shares of an each channel then further compress to 3 shares. Thus we get an o/p of 9 shares at step 4.
- **Step 5:** Compress 3 Shares from step 4 to one final encrypted image.

And the Image decryption Algorithm is:

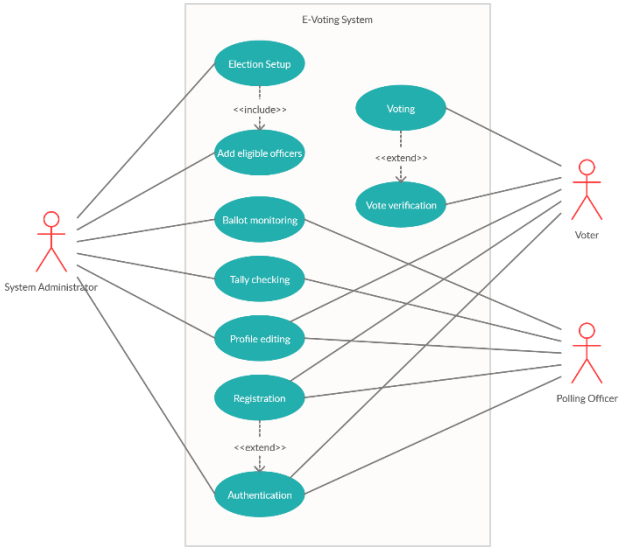
- **Step 1:** Select an Encrypted Image. It must be RGB Image.
- **Step 2:** Separate Red, Green and Blue Channels from an Encrypted image.
- **Step 3:** Create 3 Shares from each channel. So at step 3, 9 Encrypted images will be the output.
- **Step 4:** Create 8 Channels from Each channel.
- **Step 5:** From 8 shares each of step 4, Create 3 Shares (i.e red, green and Blue each).
- **Step 6:** Compress Step 5 Images to Plain Image (Decrypted Image).



Shared created after Encryption

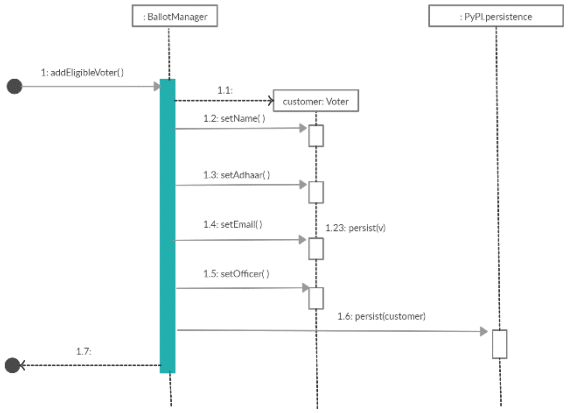
4 Architecture and models

The usecase diagram for the e-vote system is



In the use case diagram contains the 1.System Administrator 2.voter 3.Polling officer form the use case diagram we can easily identify the activities.

And the sequence diagram is:



The user authentication is as follows from the above diagram.

5 Conclusion

From our project that we explained from the above content, the evoting through online is more secured when compared with the offline voting system through electronic voting machines.

The text that in the decrypted image is entered to cast the vote after getting done by the vote system.

REFERENCES

[1] Lauretha Rura, Biju Issac and Manas Kumar Haldar. Online Voting System Based on Image Steganography and Visual Cryptography. [Journal of Computing and Information Technology, vol.25, No. 1, March 2017, doi: 10.20532/cit.2017.1003224].
[2] B. Adida, et al., "Helious: Web-based Open-Audit Voting", [in Proceedings of the 17th Conference on Security Symposium USENIX Association, Berkley, USA, pp. 335-348, 2008].
[3] E. Hubbers et al., "RIES-Internet Voting in Action", [in Proceedings of the 29th Annual International Computer Software and Application Conference, IEEE Computer Society, Washington DC, USA, pp.417-424,2005. http://dx.doi.org/10.1109/COMPSAC.2005.132].
[4] D Chaum et al., "Scantegrity II: End-To-End Verifiability for Optical Scan Election Systems Using Invisible Ink Confirmation Codes", [in Proceedings of the Conference on Electronic Voting Technology, USENIX Association, Berkley, USA, no. 14, 2008].
[5] P.Y.A Ryan et al., Pret a Voter:a Voter-Verifiable Voting System [IEEE Transaction on Information Forensic and Security,vol.4,No.4, doi:http://dx.doi.org.in/10.1109/TIFS.2009.2033233].