International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Stegano-Cryptographic Technique for Online Polling System

Monalisa Hati

Assistant Professor, Department of Computer Application, XITE, Jamshedpur, Jharkhand, India

Abstract: ***Election establishes democracy in the country. This process should be ensured to maintain integrity and confidentiality of the votes casted. Jamshedpur is a busy Industrial city where each and every person is on work. Now a days only few people go for voting because of their tight schedule. Everyone has to go to voting center, They have to stand in a long queue, many may be tired because of their tight schedule. Some people do not get even leave for voting from their work places. So we have developed online voting system Visual cryptography aims in automating the voting process so that the user can vote from his/ her home, office or anywhere without any geographical restriction . Visual cryptography and steganography is used to ensure secrecy of ballots. Visual Cryptography is a special type of encryption technique which is used to hide the information and data in images. In this technique the decryption process is done without any complex cryptographic computation. The encrypted data is decrypted using Human Visual System (HVS). The encryption technique requires a cryptographic computation to divide the image into a number of shares. Decryption can be done by someone without the knowledge of cryptography and does not require any decryption algorithm. Here we are dividing original image into two shares which are stored in separate database. Whenever these two shares are stacked with each other we get the original image. Once we get the original image it can be used as password. This system is very useful and safe for online remote voting. If this technology will be implemented in the busy city like Jamshedpur, it will save time, money, many more citizens can vote and voting process will be confidential and secret, it can not be intruded by the protesters.***

Keywords: Steganography, Cryptography, Anti-Phishing

1. Introduction

Visual cryptography is the scheme used for the secrete share of image in that secret share the original image is divided into number of shares and that share is distributed to same number of participants as each to one. That secret image is recoverable only when participant share their secret. Visual cryptography encodes a secret binary image into n shares of random binary patterns. The secret image can be visually decoded by superimposing a qualified subset of transparencies, but no secret information can be obtained from the superposition of a forbidden subset. By engaging a cryptographic encryption technique involving pixel shuffling and inter changing their position to create the ciphered image, this proposed method makes it difficult for decryption of the image without prior knowledge of the algorithm and the secret key used. Secret shared key and visual cryptography are two distinct types of cryptography.In Cryptographic Voting Systems the first step produces an encrypted, filled-in ballot on an untrusted voting machine. The second step is a method by which untrusted election officials take a publicly posted list of encrypted, filled-in ballots, each associated to a particular voter, and decrypt them, removing voter-identifying information, without being able to change the contents of the ballots. Both systems rely on key participants to enforce security or privacy: The Voters. Some voters must check that the encrypted receipts on which their votes are recorded were printed correctly and that the receipts appear in the virtual ballot box posted on the Internet. After the votes have been decrypted, voters can also verify the counts. The Election Trustees. Responsible for ensuring ballot secrecy, they decrypt and count the votes in a public forum, where all their actions can be monitored. A flexible fraction of the trustees or all the trustees would have to cheat in order to compromise the privacy of an election. Interested Third Parties and Observers. Any observer or voter can check to make sure that the voting machines are trustworthy and that an encrypted receipt is valid. Visual Cryptography Scheme is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares.**[Figure1]** denotes the shares of a white pixel and a black pixel. Note that the choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither shares provide any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel.

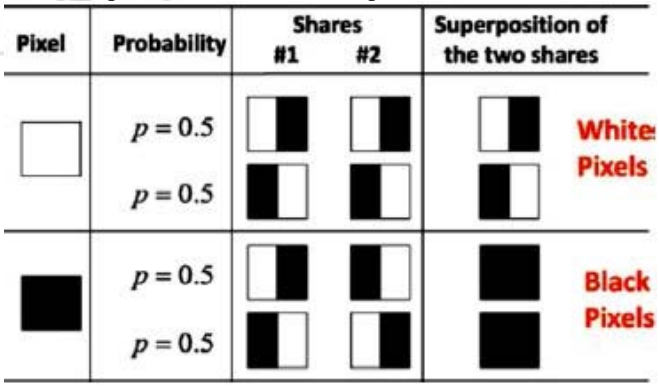

Figure 1: Illustration of a 2-out-of-2 VCS scheme with 2 subpixel construction.

Source: Mahalaxmi A. International Journal of Current Engineering and Technology.

Licensed Under Creative Commons Attribution CC BY

In Cryptography sensitive messages(plain text) are encrypted using encryption key are converted to cipher text for transmission across insecure network so that the intruder can not access the original message without having decryption key. visual cryptography attempts to recover a secret image via the human visual system by stacking two or more transparencies. In their approach, the secret was partitioned into n shadow images (shares), and each participant would receive only one share. Once any k or more shares of a secret are stacked together, the secret image will be visually retrieved without the help of the computer. That is to say that the secret image will be invisible if the number of stacked shares is less than k'. Steganography is the process of hiding and transmitting data through innocuous carrier in an effort to conceal the existence of data from an eavesdropper as sometimes sending encrypted data over invisible communication do not draw attention. Stegano-cryptographic modeling technique for secure data communication is used for ballot protection and preservation of electoral for remote e-voting.

2. Literature Review

Elections are conducted in small scale organizations, corporate institutes and on a larger scale, in parliaments too, for appointing board members of that organizational body. These elections restrict the voters to be present at that voting location thus causing inconvenience. This causes an alarming need to bring remote voting systems to effect. Internet voting system using visual cryptography fulfills this need of being able to vote from anywhere without causing security concerns. Almost all fields of life are now automated. But still people have to wait in long queues to do their fundamental right voting. This paper aims in making the voting more secure and effective at the same time making it available for people from any geographical location.

Internet Voting System:
Internet voting system enables a voter to vote over the internet while providing accuracy and security. Internet voting system can be of two types-Poll-site and remote voting. Poll-site voting enables the voter to vote over the internet, at a voting poll. Remote voting enables the voter to vote from anywhere around the globe thus removing geographical restrictions.

Cryptographic Voting Systems:
Each of the systems described in this article is accomplished in two steps, which can be handled independently. The first step produces an encrypted, filled-in ballot on an untrusted voting machine. The second step is a method by which untrusted election officials take a publicly posted list of encrypted, filled-in ballots, each associated to a particular voter, and decrypt them, removing voter-identifying information, without being able to change the contents of the ballots. Both systems rely on key participants to enforce security or privacy:

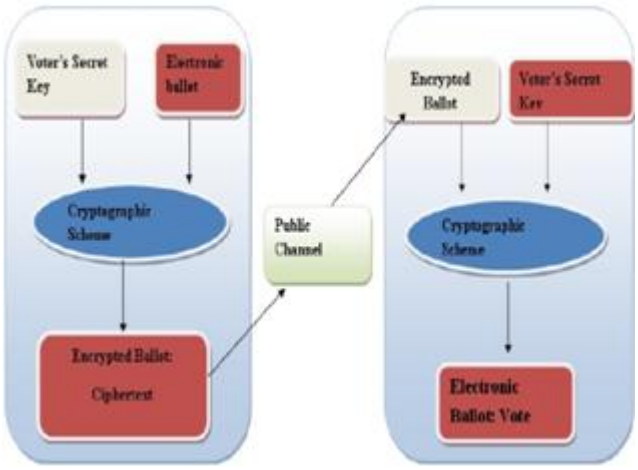

Figure 2: Cryptographic model to secure E-Voting.
Source: Covenant Journal of Informatics and Communication Technology

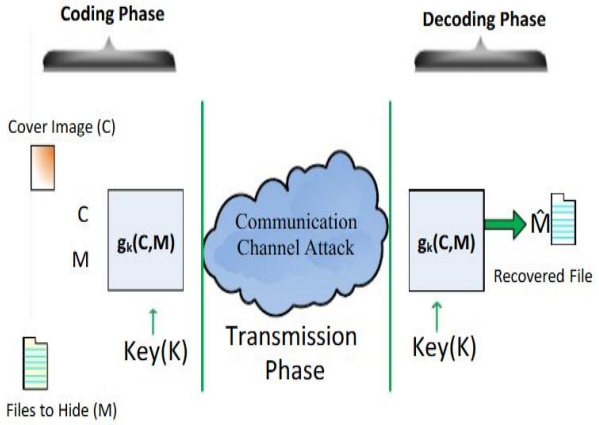

Figure 3: Steganographic embedding process

Source: Covenant Journal of Informatics and Communication Technology

K is key to encrypt and decrypt. M is the message for communication. C is the cover carrier that contains image and the file. g_k is stenographic function.

3. Objectives

Visual cryptography implementation aims in automating the voting process so that the user can vote from his/her home, office or anywhere without any geographical restrictions. To ensure secrecy the paper in cooperates the advantages of steganography and visual cryptography together. The secret password is embedded inside an image which is split into two shares. User on entering both the shares correctly can go for voting. Another feature is that the complex tasks going behind the project is hidden from the user so that the system becomes user friendly. In this paper I approach to provide remote authentication for both voters and voting systems using visual cryptography.

4. Analysis

Stegano-cryptographic modeling technique for secure data communication is used for ballot protection and preservation of electoral for remote e-voting.

Licensed Under Creative Commons Attribution CC BY

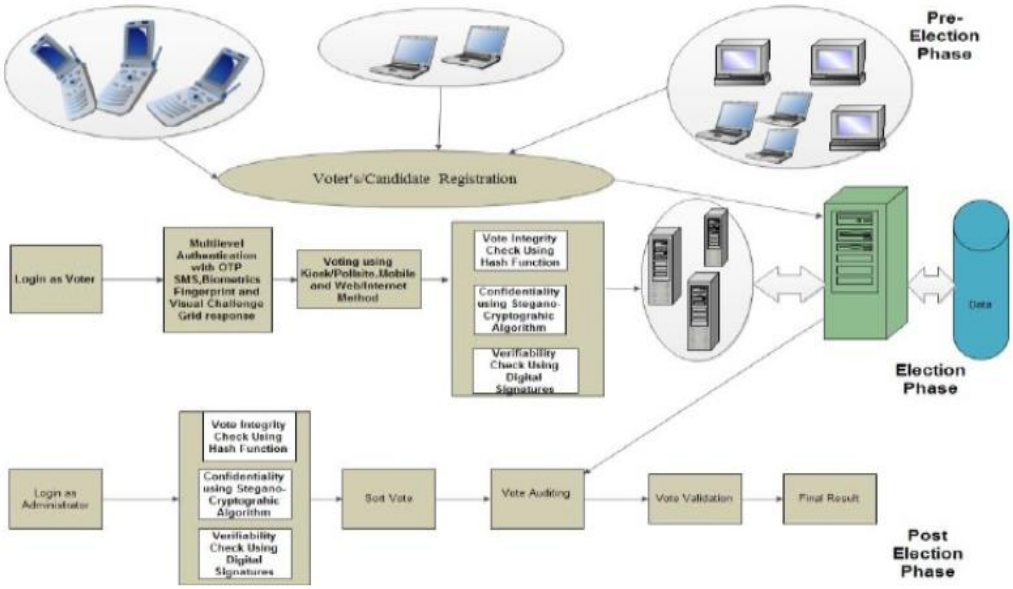

Figure 4: The various methods of Voting and the phases.
Source: Covenant Journal of Informatics and Communication Technology

Three methods of voting are allowed from **[figure 4]** the remote mobile voting, web/internet voting and polls site voting. The mobile terminal voters vote using his credential which is verified using both two-way one-time short message service (SMS) code and accurate response to visual challenge response from the grid. The mobile voter is validated by accurate comparison of remotely entered one-time SMS code; accurate remote response to visual response on the grid in mobile voting as well as verification of system generated voters ID to establish remote voters are who they claim they are. The mobile ballot is thus encrypted using elliptic curve cryptographic technique to obtain cipher text for speed and memory constraints reasons of mobile device. The cipher text is hidden into system generated picture using modified scattered Least Significant Bit (LSB) spatial image steganographic technique to produce stego-image. For further confidentiality of the vote, the stego- image is further hidden into a video cover using Wavelet frequency domain video steganographic technique to produce stego video which is eventually submitted to application server for decryption by the administrator. A remote web voter casts vote remotely with the voting device (PC/Mobile device) through the Uniform Resource Locator (URL) address of the secure e-voting system. The voting application runs remotely on the remote voter's device. The credential of remote web voter is verified using both two-way one-time short message service (SMS) code and accurate response to visual challenge response from the grid. The web voter is validated by accurate comparison of remotely entered one-time SMS code; accurate remote response to visual response on the grid in mobile voting as well as verification of system generated voters ID to establish remote voters are who they claim they are. The ballot is encrypted using RSA cryptographic technique to obtain cipher text. The cipher text is hidden into system generated picture using modified LSB spatial image steganographic technique to produce stego-image. For further confidentiality of the vote, the stego- image is further hidden into a video cover using wavelet frequency domain video steganographic technique to produce stego video which is eventually submitted to application server for decryption by the administrator. The stego video is decrypted using Integer inverse wavelet steganographic technique to extract the hidden ballot in a spatial image. The spatial image is further processed using modified LSB image steganographic algorithm to extract the hidden ballot scattered over the jpeg image for all method of voting (Poll site, Web and Mobile)

Remote Voting Authentication Process: In this process, before an election the election officials generate the shares**3**. After the generation of transparencies, the election officials send the generated transparencies to eligible voters through a third party who sends each eligible voter a randomly selected transparency along with a unique id. There is no mapping between voter identities and the transparency they receive. The user will go to the voting site and will enter the unique id. After that, server will check whether the unique id is new or used. If the id is used then it means the user has already casted his vote and is not allowed anymore to cast vote. If the user is new, then the voter is allowed to enter a random string. After this, share2 is generated and displayed on the password screen along with the random string. Now using the transparency provided to user, the user gets to see the password to cast the vote.

For phishing detection and prevention, the Anti-Phishing Image Captcha validation scheme using visual cryptography is used. It prevents password and other confidential information from the phishing websites. The proposed approach can be divided into two phases
A. Registration Phase
B. Login Phase

A. Registration Phase
In the registration phase, a key string(password) is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to provide more secure environment. This string is concatenated with randomly generated string in the server and an image captcha is generated. The image captcha

Licensed Under Creative Commons Attribution CC BY

is divided into two shares such that one of the share is kept with the user and the other share is kept in the server. The user's share and the original image captcha is sent to the user for later verification during login phase. The image captcha is also stored in the actual database of any confidential website as confidential data. After the registration, the user can change the key string when it is needed. Registration process is depicted in **[Figure 5].**

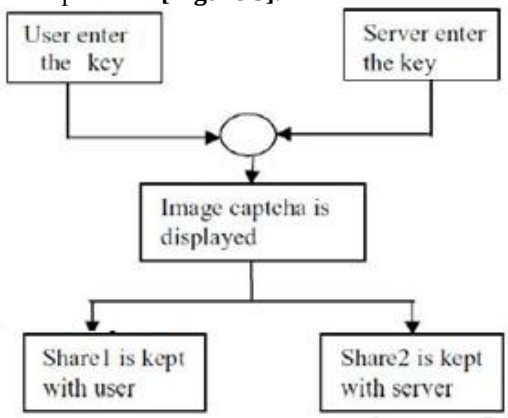

Figure 5: Process of registration
Source: : International Journal of Computer science and Information Technology

B. Login Phase

When the user logs in by entering his confidential information for using his account, then first the user is asked to enter his username (user id).Then the user is asked to enter his share which is kept with him. This share is sent to the server where the user's share and share which is stored in the database of the website for each user, is stacked together to produce the image captcha. The image captcha is displayed to the user .Here the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. The end user is required to enter the text displayed in the image captcha and this can serve the purpose of password and using this, the user can log in into the website. Using the username and image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website and can also verify whether the user is a human user or not. This phase is depicted in**[Figure6].**

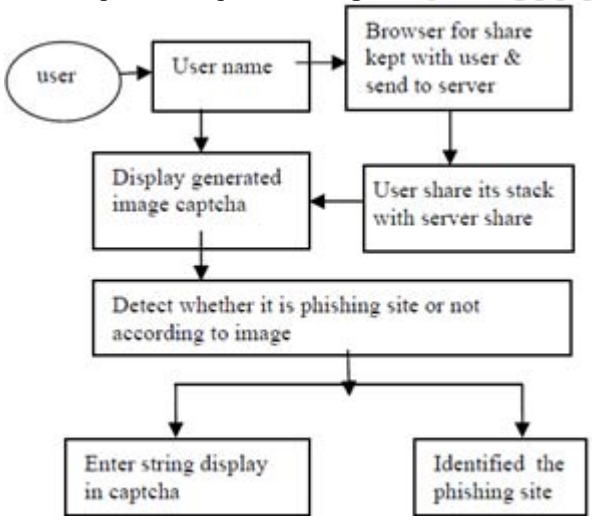

Figure 6: Login methodology
Source: International Journal of Computer science and Information Technology

5. Limitation

This technology is not cost effective. In Jamshedpur the people who live in rural areas and even some people in urban areas are not computer literate.

6. Conclusion

This paper many visual cryptography technique are used for privacy protection such as Expansion less share, Image captcha base authentication technique . This paper formulates a conceptual framework for secure e-voting with the view of increasing participation, confidence and trustworthiness in electronic democracy.

References

[1] M. Naor and A. Shamir (1994), Visual cryptography, in *Proc. Eurocrypt*,pp. 1–12.
[2] Anushree Suklabaidya, G. Sahoo, " Visual Cryptographic Applications", IJCSE, Vol. 5 No. 06 Jun 2013, ISSN : 0975-3397
[3] Mrs. A.Angel Freeda, M.Sindhuja, K.Sujitha, "Image Captcha Based Authentication Using Visual Cryptography", IJREAT, Volume 1, Issue 2, April-May, 2013 ISSN: 2320 - 8791
[4] Jayalaxmi M. Online polling system based on visual cryptography. *International Journal of Current Engineering and Technology, Special Issue1 (Sept 2013)*
[5] O.Olayemi Milail.A survey of Cryptographic and Stegano-cryptographic models for secure Electronic voting system, Covenant journal of informatics and communication technology, vil.1, No.2, December 2013

Licensed Under Creative Commons Attribution CC BY