International Journal of Engineering & Technology, 7 (4.41) (2018) 185-187

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Candidate Selection Using Visual Symmetric Key Cryptographic Approach in Online Election Process

Krishna prakasha[1], Vasundhara Acharya[2]*

[1]Dept. of I&CT, Manipal Institute of Technology, MAHE, Manipal Karnataka INDIA
[2]Dept. of CSE, Manipal Institute of Technology, MAHE, Manipal Karnataka INDIA
**Corresponding author E-mail: vasundhara.acharya@manipal.edu*

Abstract

In the candidate selection process in polling, security is an important aspect. To protect the confidential information from unsuspecting victims for identity theft and other fraudulent activities, the authentication of images using visual cryptography is implemented in the proposed research work. An intelligent approach for polling and selecting a leader is proposed using cryptographic techniques. The process involves two phases namely management phase and client phase with some public key infrastructure techniques. The management phase will authenticate the user and generates one share of the image and it is a claimant process. The client phase is a verifier process where after authentication, the user gets another half. The elector needs to merge both the halves to succeed.

.

Keywords: *Authentication; Image Shares; Public Key Infrastructure; Security; Visual Cryptography.*

1. Introduction

In the rapidly growing internet world developing and maintaining a completely secured web application has become the biggest challenge. Protecting the application from intruders has become a major concern for almost all the industries which have critical data processing or traffic over the web. Nevertheless, there are thousands of security protocols avail- able in the market today, still, a lot of challenges are faced to protect the web applications. Keeping all these challenges in mind, the development of a secured web application using the best known technique is proposed. Cryptography is the art of sending or receiving encrypted messages which could be decoded to extract the actual information only by the intended receiver or the sender himself. It encrypts the data/information (printed text, handwritten notes, numeric data, pictures and etc) in a highly secured manner so that the information remains intact. The decoding/decryption are done by the human visual system. Visual Cryptography Scheme (VCS) was introduced for the first time in the year 1994 by Naor and Shamir [1]. Its a simple and secure way to protect the data that is to be transmitted. It involves secret sharing of images without any cryptographic computation and hence saving the computation time [2] [3]. The simplest form of Visual Cryptography divides an image into 2 layers so that only 1 layer serves no purpose because as it doesn't convey complete information. However, when the layers are combined back to the complete image, it will reveal the actual information [4].

2. System overview

The candidate selection process is started by an GUI and the management module to supply the contenders list and specify the eligible users. The candidate list and eligible users are made available beforehand. The authorized people are responsible for key generation in the system. The authorized people access the system and involves in an polling process. The creation of a public encryption key for the system, and a unique private decryption key for each authority is generated.The proposed system has following steps:

- Download the public key of the system and store in a public storage.
- Based on the private key of the user, send decoding information.
- By possessing both public and Private keys, the elector is able to choose the candidate.
- When the candidate choice is over, the result will be displayed and published, which is maintained by the system.

3. Literature review

The proposal proposed by [1] involves dividing the shares or layers of images further into sub shares. However, it ended up with complex computing tasks. All the research in the recent past has done mainly to focus on Pixel expansion and contrast. In all these cases it was considered that all the participants or users are honest and they respect the integrity, which is not true. Its likely that everyone keeps the information intact. There are chances that the user himself may produce a wrong share. In order to prevent this and check the cheating by a user himself, different methodologies were proposed. Hu et al., [2] determined that these methodologies dont assure complete authentication. The segment based visual cryptography proposed by Borchert [3] deals with encryption. of messages/information that contain only symbols like the bank account number, passwords, bill denomination etc.The visual cryptography scheme proposed by [4] could be applied only for printed text or image. [1] proposed recursive visual cryptography method which involved encoding the already encoded information. the scheme divides the shares further into

sub shares. However, it was turned out to be computationally complex.The visual cryptographic technique allows the encryption of visual information by dividing the image into sub images or shares, such that the decryption can be performed by basic human visual system [5]. This can be achieved by different available schemes. One such scheme is used in the proposed system. It is referred to as "*2 out of 2 Threshold Visual Cryptographic Scheme*" [6]. [7] explained the visual cryptography schemes using black and white images with one pixel is divided into two sub pixels. One among them is is black and the other half is the white. Traditional 2 out of 2 Visual Cryptographic schemes using four subpixels is illustrated in Fig .1. Every pixel that is present in the binary image has to be converted into four subpixels producing the two shares. It is obtained back by overlapping them. It can be achieved by performing logical OR between the two shares. From a pixel, four subpixels are generated from a pixel of the secret image withe two subpixels are white and two subpixels are black. In this scheme, the message in interest is encrypted by dividing the image into 2 different shares, so that when these two shares are overlaid they reveal the actual image [8]. In the proposed research work, the 2 out of 2 Threshold Visual scheme is used for user authentication. Here each pixel P in the original image is encrypted by dividing it into 2 sub- pixels called shares [9]. Figure.1 illustrates the share of a white and a black pixel. The choice of a white and black pixel has been randomly determined (2 choices are available for each pixel). Single share itself will not provide any clue of the actual image since all the pixels of an image are encrypted with different random choice of pixels. When these 2 shares are superimposed the value of the original/actual pixel P can be determined. There are two general schemes for visual cryptography [11].

3.1. K out of N threshold visual cryptography scheme (k,n)

Under this scheme, the image in interest is encrypted into n shares such that when a group of at least k shares is overlaid to get the actual image in interest. The major concern associated with that the end user needs to preserve different shares. Sometimes loss in any share will lead the scheme in vain. The user needs to carefully maintain all the shares. It also adds for more cost as a number of shares lead in more calculation and memory consumption. This methodology is found to be implemented in applications that host the banking systems. For an example, in the case of a joint account, there are two people accessing the same account and both need to be authenticated. In order to facilitate both the account holders to gain access to the account 3 shares of the actual image are created. 1 share would be kept in bank server and the each 1 of the remaining 2 shares are given to account holders, so that both the account holders individually could authenticate themselves with the bank and gain access to their account.

3.2 N out of N threshold visual cryptography scheme (n,n)

This scheme allows encrypting the image in interest into n shares such that the actual image would be revealed if and only if all then shares are overlaid. Its mandatory that the entire set of shares is required. Any 1 share missing will not help to retrieve the actual image. This scheme is not popularly implemented as it does have some flaws. Managing n shares would turn out to be challenging and also it requires complex calculation. It will further end up increasing processing and maintaining cost.

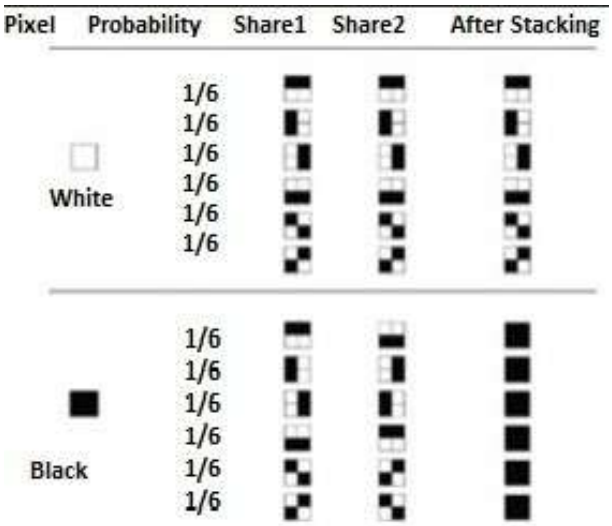

Fig. 1: 2 out of 2 scheme using 4 sub pixels [10].

4. Proposed methodology

In order to authenticate the end user, secured credentials are used. User can gain access to the application using those secured credentials. Communicating these credentials is again a concern. For secured communication of the credential the administrator passes the information using secured images which are encrypted by Visual Cryptography Scheme. The operation of authenticating the user involves two phases.

1. Management Phase :The system administrator is responsible for managing the credentials. After user authentication using Public Key Infrastructure, the administrator creates and sets these credentials on an image and key string. The key string can be a combination of alphabets and numbers to provide more secure environment [1]. The image is encrypted based on the methodology of Visual Cryptography i.e. the image is divided into 2 shares. 1 of the shares (Share 1) is provided to the voter and another share (Share 2) is accessed by the voter at the time of casting vote. The user downloads the share 1 after registration to the system which is preserved for further use and share is available at later stage before poll.
2. Client Phase: An OTP is sent to registered mobile number of the user this phase, the user is prompted to enter the credentials and supplied OTP to log in to the application. After user authentication, user is allowed to download share 2 from the database. Now the user has Share 1 and Share 2, and overlap both images to get the actual image containing the password [2]. Using this password the user could log in to the application and cast his vote. As it involves human interpretation for analyzing the actual image, the system makes sure that it won't allow the viral programs to take over. Hence protects the integrity of the system.

5. Results

In the Client phase, the most important task is to create the shares from the original image where one share can be kept with the user/voter and other share is kept with the server. In the Login phase, the user needs to enter a valid username in the given field. After that he/she has to browse the share and process. On the server side, the user share is stacked with the share which is on the server. Stacking of the shares will generate a reconstructed image. The user has to enter the text from the generated image in the password field in order to login into the website.

The entire process is shown in the following figures. Case 1 and Case 2 illustrates the creation of shares from an original image and how they are overlaid to obtain the actual information. In Case 1 and Case 2, the image in interest is divided into share 1 and share 2. Later the image is reconstructed by overlapping these shares. Case 3 illustrates the result when shares of 2

different images are used. It will not reveal any useful information and illustrates a failure case.

Fig. 2: Original image

The original image with textual information is taken as the input image and correspondingly the two shares are generated.

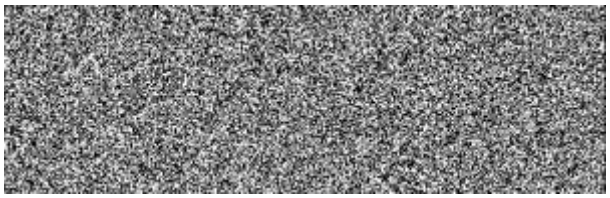

Fig. 3. Share 1 of image

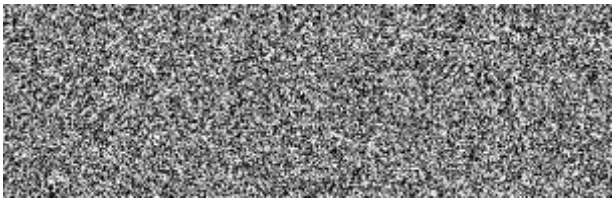

Fig. 4. Share 2 of image

Share 1 of Fig.3 and Share 2 of Fig.4 are stacked to form original images. The result is illustrated in Fig .5.

Fig. 5. Result of addition of images

6. Conclusion

The Visual Cryptography Scheme plays a major role in the secured communication and remote candidate selection process. The system authenticates the user by secure transmission of logging in credentials and validating those with the help of a centralized server. It encrypts the logging credentials that are imprinted into an image later this encrypted data could be decoded by the user by Visual interpretation to reveal the credentials. The System provides for highest elector turn out and makes the electoral process a success. Different available software development methodologies were reviewed, considered their specifications and a careful study was made to determine the best suitable method for the proposed system.

References

[1] Monoth and A. P. Babui, "Recursive visual cryptography using random basis column pixel expansion," Proceedings of IEEE International Conference on Information Technology, (2007), pp: 41–43.
[2] C. Hu and W. G. Tzeng, "Cheating prevention in visual cryptography," in IEEE Transaction on Image Processing, vol. 16, no 1 (2007), pp:36-45.
[3] B. Borchert, "Segment based visual cryptography," in WSI Press, Germany, 2007.
[4] D. J. W-Q Yan and M. S. Kanakanahalli, "Visual cryptography for print and scan applications," Proceedings of IEEE International Symposium on Circuits and Systems, (2004), pp: 572– 575.
[5] F. Liu, C. Wu, and X. Lin, "Step construction of visual cryptography schemes," IEEE transactions on information forensics and security, Vol. 5, No. 1 (2010), pp: 27–38.
[6] L. J. Anbarasi, M. J. Vincent, and G. A. Mala, "A novel visual secret sharing scheme for multiple secrets via error diffusion in halftone visual cryptography," Proceedings of , 2011 International Conference on. IEEE, (2011), pp:129–133.
[7] M. S. Reddy and S. M. Mohan, "Visual Cryptography Scheme for Secret Image Retrieval," International Journal of Computer Science and Network Security (IJCSNS), Vol. 14, No. 6 (2014), pp: 41–46.
[8] P. R. R. Neelima Guntupalli and S. cheekaty, "An introduction to different types of visual cryptography schemes," International Journal of Science and Advanced Technology, Vol. 1, No. 7 (2011), pp: 198–205.
[9] D. M. A. Pallavi V Chavan and D. A. R. Mahajan, "An intelligent sys- tem for secured authentication using hierarchical visual cryptography- review," Proceedings of Int. Joint Colloquium on Emerging Technologies in Computer Electrical and Mechanical, (2011), pp:11-13.
[10] M. Naor and A. Shamir, "Visual cryptography," Proceedings of EUROCRYPT, (1994), pp.:1–12.
[11] W. Dang, M. He, D. Wang, and X. Li, "K out of K Extended Visual Cryptography Scheme based on Xor", International Journal of Computer and Communication Engineering, Vol. 4, No. 6 (2015), pp: 439-453.