INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 3 ISSUE 1 -JANUARY 2015 - ISSN: 2349 - 9303

Enhanced Secure E-Gateway using Hierarchical Visual Cryptography

K.S.Suganya[1]
PG Scholar
Department of Computer Science and Engineering
SriGuru Institute of Technology,Coimbatore
suganayselvaraj06@gmail.com

K.Manikandan[2]
Assistant Professor Guide
Department of Computer Science and Engineering
SriGuru Institute of Technology,Coimbatore
manikarthi25@gmail.com

Abstract— With tremendous growth in electronic commerce, the e-shopping users are facing more and more problems in their day to day life. Most important of them are identity theft and spear phishing attacks. In this paper, we will be addressing those issues by the combined use of Hierarchical Visual Cryptography and keyless image steganography techniques. Firstly, we recommend the use of a certified third party payment gateway, which involves generating image shares using HVCS and secondly we recommend the use of image steganography technique to hide the user's passphrase or ATM Pin or password in the image share to achieve cheating prevention from malicious insiders of both merchant as well as third party payment gateway. Further, we propose the use of image share as secure SiteKey which prevents spear phishing attack targeting high profile customers.

Index Terms— E-shopping, Hierarchical visual cryptography scheme, HVCS, Identity theft, Spear phishing attacks, SiteKey.

1 INTRODUCTION

In India, Online shopping had gained popularity owing to Flipkart, Amazon and many online merchants especially in recent years. With rise in popularity, adversely there had been increase in threats and subsequently many users are becoming targets of identity theft, phishing attack and spear phishing attack and many more. The most important attack of them is phishing attack. In phishing attack, the attacker sends an electronic message to the users impersonating as a legitimate personnel. The user considering it as a legitimate request from their registered site, unknowingly, are redirected to the fake website which looks alike the genuine one. Thus, the users lose their confidential password credentials which will be used by the intruders to hack into their account of registered websites.

Among which, spear phishing attack is a special type of phishing attack where the intruder targets a specific individual or organization and steals their confidential information. According to FBI's IC3, spear-phishing attacks are mainly targeting industries, and their ultimate goal is to steal IP address or compromise banking credentials. Hence the need for new and plausible security method for the industries or organization also has increased.

As a result, many industries, bank and organization are taking many counter measures to prevent phishing attack and spear phishing attack. The most common among them is authentication. But there are varying level of authentication methods such as one way authentication and two way (also known as mutual) authentications. Some of the common factors of authentication measure involve the following namely username and passphrase, Smart card /ATM card, Biometrics (fingerprint, Iris, Retina, Signature, Sclera, etc...) and many more.

One way authentication is one direction in nature where the user authenticates them to an external entity with something the user has or knows. Mutual authentication occurs where there is a need for user authenticates themselves to an external entity and in turn an external entity authenticates themselves back to the user. SiteKey authentication is a form of authentication which involves mutual authentications with visual image.

The process of SiteKey authentication is as follows where the users of an external entity is prompted to enter their registered username and the entity in turn authenticates themselves by retrieving the previously registered user image. If the images are different, then the user has to consider the website as a fake one and leave it immediately without further proceeding.
Else the user can proceed with their login process and enter their password credentials.

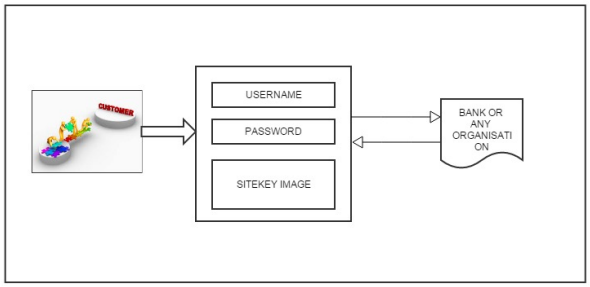

Fig 1.1 SiteKey authentication

But the SiteKey authentication is not effective against security image attack where the image column will be replaced with a maintenance message which may compromise the user's credibility leading to lose of bank credentials.

Visual cryptography is a special kind of encryption technique, where the visual information such as text, image is encrypted using various VC schemes to generate 2 or more meaningless shares. These image shares are then transmitted or distributed over untrusted communication channel by the sender. At the receiver side, the image shares are stacked together to retrieve the original visual information. This secret sharing scheme was proposed by Shamir and Naor in 1990[1].In this proposal, we make use of hierarchical visual cryptography scheme where key image share and another share are generated from visual secret image at three levels as explained in the figure 4.1.

Steganography is the technique of information or data hiding. It is an age old technique which has its roots in history but still in use. The basic concept behind it is that data is hidden in some cover objects such as text, image, video and audio and the most commonly used cover object is digital image. A method proposed by Chen, Pan, Tseng popularly known as CPT method, where the binary secret message is hidden in a cover image using a weighted matrix [3].In this proposal, we make use a variation of CPT method which will be explained in the section 3.Our system framework requires the bank to provide encrypted password to the users preferably using AES or any encryption algorithm. In our proposal, we use the symmetric encryption technique AES to prevent the third party payment gateway from learning the password credentials.

2 RELATED WORKS

A brief survey of the related works to this proposal has been discussed in this section. Shamir and Naor [2] proposed a visual secret sharing scheme known as Visual Cryptography in 1990. Souvik et al. [1] proposed an authentication system for online payment using both visual cryptography and Steganography which prevented form identity theft.Yet,cheating is possible which was a huge drawback.To overcome this, Tzeng [8] proposed a scheme where cheating in visual cryptography by generating fake share can be prevented by the combined use of it with steganography. Yang et al. [5] proposed a modification to Lin proposal to prevent dishonest participants from cheating. And also this scheme increased the quality of the stego image. According to Judge [2], the various steganography schemes employed in the past, present and future were discussed and their various forms and legitimate and illegal use of steganography have been discussed in brief. Among which, CPT image steganographic algorithm proposed by Chen et al[3] which can be combined with visual cryptography to achieve cheating prevention. Chen et al. [6] discussed the procedures of phishing attack and various approaches to prevent phishing attack. Then, the characteristics of hyperlinks in relation to phishing attack were studied and linkguard algorithm was proposed to detect them.

We then made a study of SiteKey authentication proposed by Bank of Americas as in [11].Then the vulnerabilities, their ineffectiveness and how to overcome their fault were briefly discussed by Youl in [9] and Hearst in [12].

3 PROPOSED IMAGE STEGANOGRAPHY

To prevent cheating by generating fake share in visual cryptography scheme, we combine this with image based steganography technique to enhance security. The CPT is a popular algorithm for embedding binary coded secret message into a binary image. In here ,we are going to use a variation of CPT as in [3].In our proposal, we are going to generate a random binary secret message at the payment gateway and embed the secret message into the account information snapshot image and then encrypt using HVCS scheme as explained in detail in the following section.

Algorithm for hiding the secret message in chosen image:

Step 1: A secret message is encoded into binary codes (s1, s2, s3, s4….) and the snapshot image is taken as input.

Step 2: The cover image is divided into blocks (M) of size 5x5.

Step 3: For each block, do as follows

i. For each row in the first four rows of the block, XOR all the bits in that row to get a1a2a3a4.
ii. For each column in the first four columns of the block, XOR all the bits in that column to get b1b2b3b4.
iii. XOR the results in i and ii to get c1c2c3c4 where c1=a1⊕b1, c2=a2⊕b2, and so on.
iv. We need to compare the result obtained from c1c2c3c4 with the four secret message bits s1s2s3s4. If found no difference, no change of bits of M. Otherwise , do the following:
    - If the difference in one bit s_i, the bit $[M]_{i,5}$ or $[M]_{5,i}$ need to be changed
    - Else if difference in two bits s_i and s_j, then the bit $[M]_{i,j}$ or $[M]_{j,i}$ need to be changed.
    - Else if difference in three bits s_i, s_j and s_k, then the bits $(([M]_{i,j}$ or $[M]_{j,i})$ and $([M]_{k,5}$ or $[M]_{5,k}))$ or $(([M]_{i,5}$ or $[M]_{5,i})$ and $([M]_{k,i}$ or $[M]_{j,k}))$ or $(([M]_{5,j}$or$[M]_{j,5})$ and $([M]_{k,i}$ or $[M]_{i,k}))$ need to be changed .
    - Else (difference in four bits bi, bj, bk and bm) then the bits $(([M]_{i,j}$ or $[M]_{j,i})$ and $([M]_{k,m}$ or $[M]_{m,k}))$ or $(([M]_{i,m}$ or $[M]_{m,i})$ and $([M]_{k,i}$ or $[M]_{j,k}))$ or $(([M]_{m,j}$ or $[M]_{j,m})$ and $([M]_{k,i}$ or $[M]_{i,k}))$ need be changed .

Algorithm for extracting the phrase from the chosen image:

Step 1: The decrypted image share is taken as input for the extracting phase.

Step 2: The stego image is divided into blocks (M) of size 5x5.

Step 3: For each block, do as follows

i. For each row in the first four rows of the block, XOR all the bits in that row to get a1a2a3a4.
ii. For each column in the first four columns of the block, XOR all the bits in that column to get b1b2b3b4.
iii. XOR the results in i and ii to get c1c2c3c4 where c1=a1⊕b1, c2=a2⊕b2, and so on which is the secret message which is compared to acheive cheating prevention of creating fake visual share image by the malicious insiders of third party payment gateway and online sopping merchants.

4 PROPOSED VISUAL CRYPTOGRAPHY SCHEMES

In our proposed solution, there are two phases namely registration and login phases. After registration, the users of online shopping enter their bank's account information and bank's encrypted password/passphrase/ATM Pin number which will be taken as a snapshot image. Then the user enters a secret message which is encoded into binary codes which are hidden in the user's snapshot image using above mentioned image steganography technique. Then by using hierarchical visual cryptography encryption scheme, we encrypt the stego snapshot image to generate a key image share and image share in three levels as follows.

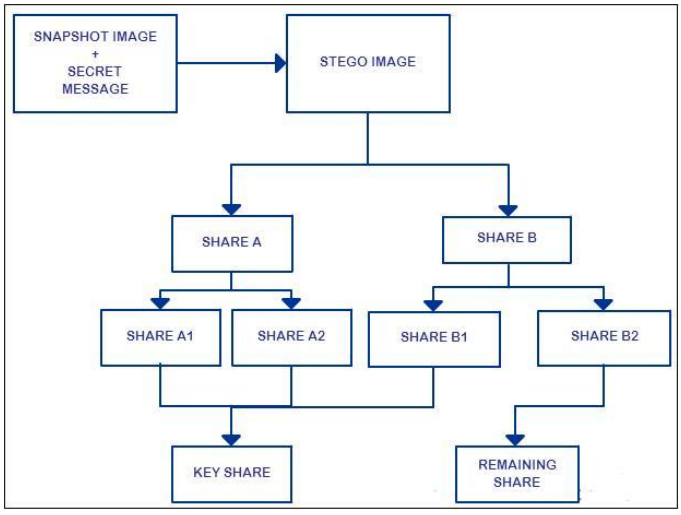

Fig 4.1 HVCS flow

In the first level, two image shares are generated from the snapshot image by the payment gateway namely Share A and Share B. In the next level, the Share A is encrypted again to generate two shares namely Share A1 and Share A2.Likewise, the Share B is encrypted again to generate two shares namely Share B1 and Share B2.Randomly, any three shares form (Share A1/A2/B1/B2) is combined to form the key image share and remaining share is kept aside as an image share. Key image share is shared with the user over a secure communication channel. Then the remaining share is stored in their payment gateway secure database. The above process is explained in the figure.During login phase, user enters their username or customer id along with their image share to authenticate them to the payment gateway website. The payment gateway website retrieves the share for the corresponding user from their database using customer id.

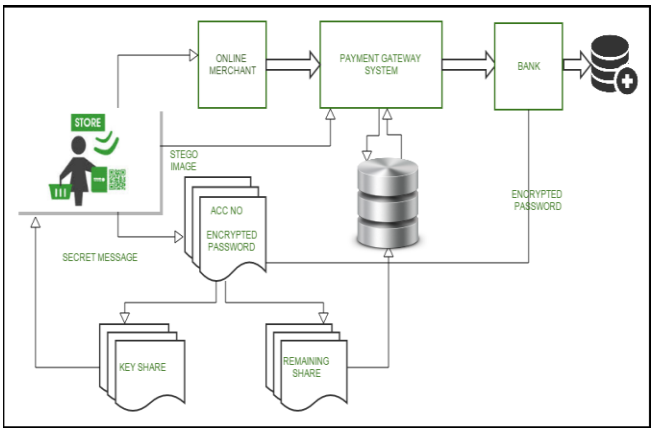

Fig 4.2 System Framework

Then the user's key image share and bank's remaining image share retrieved from the bank's database are stacked over one another to retrieve the original snapshot image which will have reduced grayscale density compared to the regular (2,2) VCS scheme.To prevent cheating from generating fake visual share by the malicious insiders, we have two level of security as explained below

The secret message is decoded from the original image by image steganography technique and is then compared as an additional verification process. The malicious insiders of both payment gateway and online merchant cannot learn the bank's password/passphrase/ATM Pin number since they are encrypted using AES encryption technique.

The original image is now displayed to the user by which the payment gateway website authenticates themselves to the users. Upon which, the user are redirected to their banking website where the user's banking account information and encrypted bank's password/passphrase/ATM will be forwarded over a secure communication channel and the uses can proceed with their transaction and they will be redirected back to the online shopping merchant.

5 EXPERIMENTAL RESULTS

The 2 out of 2 VCS scheme randomly chooses one of the two pixel patterns (black or white) from the table below for the image shares 1 and 2. The pixel selection is random so that the shares 1 and 2 usually consist of same number of white and black pixels. As a result, by inspecting one image share, it is not possible to identify the pixel of the next image share as black or white. By using Hierarchical Visual cryptography scheme, we overcome the difficulties like increased grayscale density, pixel expansion faced in the paper [1].

Original pixel	Pixel value	Possible share 1	Possible share 2	Merged share
	0			
	1			

Table 5.1: VCS Pixel pattern selections

According to the proposed methodology, we create a snapshot image as in figure 5.2 (a). Later, we embedded the secret message in the snapshot image using the above proposed steganography method. Then we generated two image shares namely image share A and B using (2, 2) VCS as in figure 5.2 (b) and (c) respectively. Furthermore, we generated two image shares namely image share A1 and A2 using (2, 2) VCS from Share A as in figure 5.2 (d) and (e) respectively. Likewise, we generated two more image shares namely image share B1 and B2 using (2, 2) VCS from Share B as in figure 5.2 (f) and (g) respectively. Then we combined randomly to form a key image share and a remaining share as in figure 5.2 (h) and (i) respectively. Upon overlaying those image shares, we received the merged shares as in figure 5.2 (j).

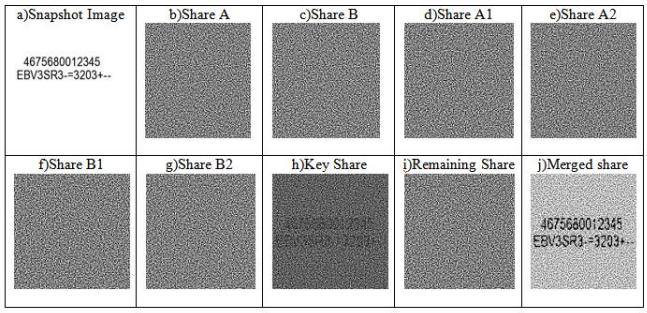

Fig 5.2 Experimental Results

6 SECURITY ANALYSIS

In this section, we are analyzing the security of our proposed solution against some security attacks to know their resisting quality, advantages, disadvantages and method extension.

6.1 Secret sharing

The proposed solution is implemented using hierarchical visual secret sharing scheme where the user's key share and bank's share are both required to retrieve the secret image. The key share is kept by the user and the second share is stored the payment gateway's database in a secure manner.

6.2 Man-in-the-middle attack

Since only one share is sent across secure communication channel, the man-in-the-middle attack will not succeed in obtaining the access.. Adversely, if the share is intercepted by the intruders and the share is duplicated to generate fake share. If the intruders provide the fake share in the payment website which when stacked together with bank share may retrieve the original image but the payment gateway website will detect anomalies since the fake secret message decoded will not match the user entered secret message stored in the payment gateway website secure database.

6.3 Security image attack

Security image attack is a special type of attack against SiteKey where the image and phrase column will be replaced with a maintenance message in the fake website which will look legitimate. This can be avoided only through proper awareness among users about this attack

6.4 Advantages

- Proposed solution protects against spear phishing attack by the use of SiteKey authentication
- SiteKey authentication with HVCS protects against the security image attack and increases customer's integrity with their merchant, payment gateway and bank.
- Further the use of CPT Steganography prevents cheating in HVCS. Suppose the attacker generates a fake share similar to the original image share and use it to impersonate them to the payment gateway website. The site detects the phishing attack since the fake share would not contain hidden secret message.

6.5 Disadvantages

According to Harvard survey, the use of SiteKey is ineffective if the users are not properly educated against the phishing attacks and security image attack. The other most important deterrent is the users had to keep track of their image share in addition to their authentication credentials.

7 PERFORMANCE ANALYSIS

The proposed method's performance is investigated by performing steganalysis and conducting benchmarking test for analyzing parameters like Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR).

The MSE is calculated by using the equation,

$$MSE = \frac{1}{PQ}\sum_{x=1}^{P}\sum_{y=1}^{Q} M_{x,y} - N_{x,y} \quad \text{---------- (1)}$$

The terms in the equation **(1)** is explained below

P = the total number of pixels in the horizontal dimensions of the image

Q = the total number of pixels in the vertical dimensions of the image

$M_{x,y}$ = the pixels of the original image

$N_{x,y}$ = the pixels of the stego image.

The PSNR is calculated by using the equation

$$PSNR = 10\log_{10}\left(\frac{Y^2}{MSE}\right)dB \quad \text{..... (2)}$$

The term in the equation **(2)** is explained below

Y = pixel's intensity value which is equal to 255 for 8 bit gray scale images.

8 CONCLUSION

In this paper, we have overcome the difficulties of VCS such as grayscale density and pixel expansion by the use of hierarchical VCS. Furthermore, it prevents the identity theft by malicious insiders and phishing attack by malicious outsides by the combined use of visual cryptography and steganography along with AES symmetric encryption technique. It also limits the information shared between the merchant and the customer. It provides protection for high profile users by the use of SiteKey authentication from spear phishing attack.This method can also be extended to specific organisation website and employees authentication.

REFERENCES

[1] Souvik Roy and P.Venkateswaran , "Online Payment System using Steganography and Visual Cryptography". ," Proceedings of 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science, pp.165-172, 2014

[2] M. Naor, and A. Shamir, (1994) "Visual Cryptography", Advances in Cryptography-Eurocrypt '94, vis Lecture Notes in Computer Science 950, pp. 1-12.

[3] Chen, Y., Pan, H., Tseng, Y.: A secret of data hiding scheme for two-color images. In: IEEE symposium on computers and communications (2000).

[4] Chetana Hegde, S. Manu, P. Deepa Shenoy, K.R. Venugopal, L M Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications,"Proceedings of 16th International Conference on Advanced Computing and Communications, pp. 65-72,Chennai,India, 2008.

[5] C.N. Yang, T.S. Chen, K.H. Yu, and C.C. Wang, "Improvements of image sharing with steganography and authentication", Journal of Systems &Software, 80:1070-1076, 2007.

[6] Juan Chen, Chuanxiong Guo , "Online Detection and Prevention of Phishing Attacks," Proceedings of First International Conference on Communications and Networking in China (ChinaCom '06), pp. 1 - 7, Beijing, China, 2006.

[7] Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography," Proceedings of 2011 World Congress on Information and Communication Technologies, pp. 1181-1186, Mumbai, India, 2011.

[8] C. M. Hu and W. G. Tzeng, "Cheating Prevention in Visual Cryptography", IEEE Transaction on Image Processing, vol. 16, no.1, Jan- 2007,pp. 36-45.

[9] Jim Youll, "Fraud vulnerabilities in SiteKey security at Bank of America" Challenge/Response LABS,Security & privacy for e-commerce, July 18, 2006.

[10] Bank of America,"SiteKey FAQs" https://www.bankofamerica.com/privacy/faq/sitekey-faq.go

[11] J.C. Judge, "Steganography: Past, Present, Future," SANS Institute, November 30, 2001.

[12] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in Proceedings of the SIGCHI Conference on Human Factors in Computing