International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Enhanced Phishing Detection based on Image Differentiation

B. Jenny Jyoshna[1], Shaik Nyamathulla[2]

[1]Computer Science Engineering, Guntur Engineering College, Guntur, India

[2]Computer Science Engineering, Guntur Engineering College, Guntur, India

Abstract- ***Phishing is an art of creating a illegal look-a-like website of ethical trusted legal website , and dupe customer by sending an wrong information or link asking them to use their private passwords and username or pins to gain access. When the customer mistakes or unknowingly use their essential of access to website, this phishers collect mainly email, banking, company login accounts that are targeted. This paper proposes an image differentiation methodology or architecture to detect legality of the website with a well know captcha technology and Google's ranking where user cross checks with multiple authentication procedures in order to tackle with phishing problem.***

Keywords: Phishing, ethical, image captcha, shares, private passwords, differentiation.

1. Introduction

The Phishing fraudulent web site email is designed be mirror the legitimate web site it is purporting to be. The phisher-agent use several methods to do this, including using unique looking posters, frames and texture, disguising the URL in the address bar or removing the address bar altogether. Such web site trick consumers into thinking they are at the company's unique web site, and giving their personal information to the trusted company they think they are dealing with.

In order to trick victims into falling for their traps, the attacker needs to either create a domain to use for their attacks or spoof an existing domain. Taking a closer look in to the reference "http://www.allspammedup.com/2012/09/phishing-a-look-inside-the-statistics/"

Such an impact of phishing is on the verge of growth every year which can be an observed in the statistics stated above which has prompted for ongoing Research to find the anti phishing methodologies.

The act of Phishing serves the main aim in acquire information such as usernames, passwords, and credit card details and sometimes, in directed money transactions by masquerading as a trusted entity. Mainly targeting popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.

Phishing irregularities have been popular with press coverage extensively because such attacks have been increasing in number and sophistication. Online service providers believe that their reputation is at stake and fear that users will lose confidence in electronic commerce. According to a study by Gartner [1], 57 million US Internet users have identified the receipt of e-mail linked to phishing scams and about 2 million of them are estimated to have been tricked into giving away sensitive information. The phishing problem has become so serious that the German Minister of Internal Affairs recently drew attention to the urgency of the problem and called upon researchers and industry to find solutions [2].

"Anti phishing Framework using a Modified captcha technique" is a framework which on adoption associates multiple benefits:

- Early detection of phishing
- Less network resources are used for anti-phishing frame work
- Easy Access and Maintenance System
- Provides high Privacy preserving Technique
- Out Performs other anti- Phishing Techniques
- Provides high Secured Environment

The concept of image processing and an improved visual cryptography is used. Image processing is a technique of processing an input image and to get the output as either improved form of the same image and/or characteristics of the input image. Visual Cryptography (VC) is a method of encrypting a secret image into shares, such that stacking a sufficient number of shares reveals the secret image.

This paper is organized as follows: Section II deals with the related work using Visual Cryptography and Section III & IV presents the current and proposed Methodologies. Section V presents the implementation and Section VI deals with Results and Discussions. Section VII contains the conclusion.

2. Visual Cryptography

One of the best known techniques to protect data is cryptography. It is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Naor and Shamir [2] introduced the visual cryptography

Licensed Under Creative Commons Attribution CC BY

scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations.

A brief survey of the related work in the area of visual cryptography is presented. Visual cryptography schemes were independently introduced by Shamir [3] and Blakley [4], their original motivation was to safeguard cryptographic keys from loss. These schemes also have been widely employed in the construction of several types of cryptographic protocols [5] and consequently, they have many applications in different areas such as access control, opening a bank vault, opening a safety deposit box, or even launching of missiles. A segment based visual cryptography suggested by Borchert [6] can be used only to encrypt the messages containing symbols, especially numbers like bank account number, amount etc. The VCS proposed by Wei-Qi Yan et al., [7] can be applied only for printed text or image.

A recursive VC method proposed by Monoth et al., [8] is computationally complex as the encoded shares are further encoded into number of sub-shares recursively. Similarly a technique proposed by Kim et al., [9] also suffers from computational complexity, though it avoids dithering of the pixels. Most of the previous research work on VC focused on improving two parameters: pixel expansion and contrast [10],[11],[12]. In these cases all participants who hold shares are assumed to be honest, that is, they will not present false or fake shares during the phase of recovering the secret image. Thus, the image shown on the stacking of shares is considered as the real secrete image. But, this may not be true always. So cheating prevention methodologies are introduced by Yan et al., [13], Horng et al., [14] and Hu et al., [15]. But, it is observed in all these methodologies, there is no facility of authentication testing.

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. We can achieve this by one of the following access structure schemes.

1. (2,2) Threshold VCS scheme- This is a simplest threshold scheme that takes a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.
2. (2, n) Threshold VCS scheme-This scheme encrypts the secret image into n shares such that when any two (or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants.
3. (n, n) Threshold VCS scheme-This scheme encrypts the secret image to n shares such that when all n of the shares are combined will the secret image is revealed. The user will be prompted for n, the number of participants.
4. (k, n) Threshold VCS scheme- This scheme encrypts the secret image to n shares such that when any group of at least k shares are overlaid the secret image will be revealed. The user will be prompted for k, the Threshold,, and n, the number of participants.

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Fig.1 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 share provides 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.

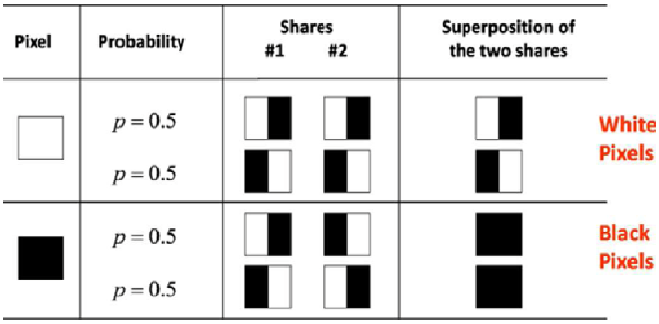


Figure 1: Illustration of a 2-out-of-2 VCS scheme with 2 sub pixel construction.

3. Current Methodology

In the current scenario as shown in the Fig. 2, when the end user wants to access his confidential information online (in the form of money transfer or payment gateway) by logging into his bank account or secure mail account, the person enters information like username, password, credit card no. etc. on the login page. But quite often, this information can be captured by attackers using phishing techniques (for instance, a phishing website can collect the login information the user enters and redirect him to the original site). There is no such information that cannot be directly obtained from the user at the time of his login input.

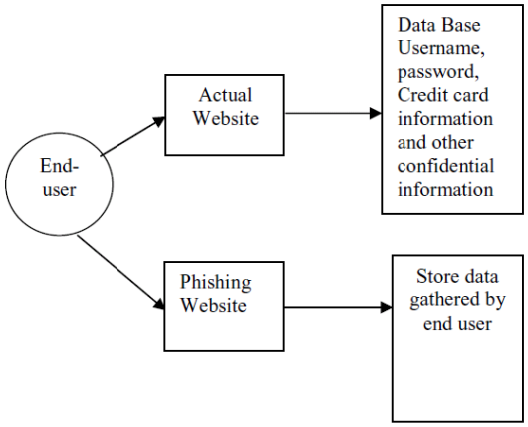


Figure 2: Current scenario

4. Proposed Methodology

In this Work we have proposed a new approach named as “Anti phishing Framework using a Modified captcha technique "to solve the problem of phishing. Here an image based authentication using Visual Cryptography is implemented. The use of visual cryptography is explored to

Licensed Under Creative Commons Attribution CC BY

preserve the privacy of an image captcha by decomposing the original image Captcha into two shares (known as sheets) that are stored in separate database servers (one with user and one with server) such that the original image captcha can be revealed only when both are simultaneously available; the individual sheet images do not reveal the identity of the original image captcha. Once the original image captcha is revealed to the user it can be used as the password. Using this website cross verifies its identity and proves that it is a genuine website before the end users.

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 [16][17] is generated. The image captcha is divided into two shares such that one of the shares 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 Fig.3.

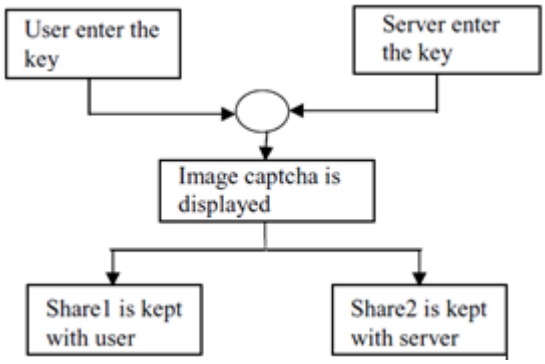


Figure.3 when user performs registration process for the website

B. *Login Phase*

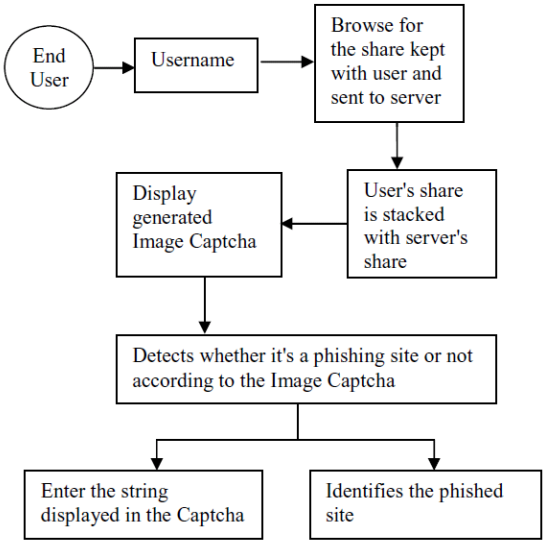


Figure 4: when user attempts to log in into site

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 Fig.4.

5. Implementation and Analysis

The proposed methodology is implemented using Java. Fig 5, Shows the result of creation and stacking of shares.

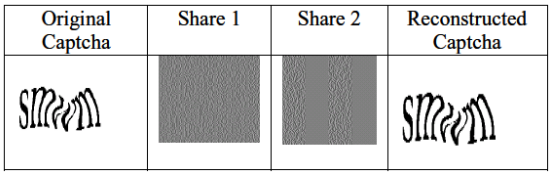
In the registration phase the most important part is the creation of shares from the image captcha where one share is kept with the user and other share can be kept with the server.

For login, the user needs to enter a valid username in the given field. Then he has to browse his share and process. At the server side the user's share is combined with the share in the server and an image captcha is generated. The user has to enter the text from the image captcha in the required field in order to log in into the website.

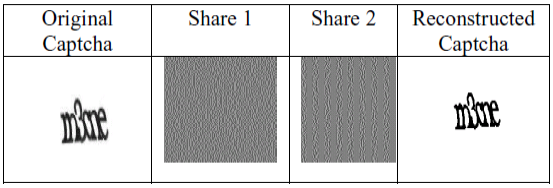
The entire process is depicted in Fig.5 as different cases.Case1 and Case 2 illustrates the creation and stacking of shares of two image captcha's resulting in original captcha. In Case3 share1 of first image captcha (Case.1) is combined with share2 of second captcha (Case.2) resulting in an unrecognizable form of captcha.

Licensed Under Creative Commons Attribution CC BY

Case.1



Case.2



Case.3

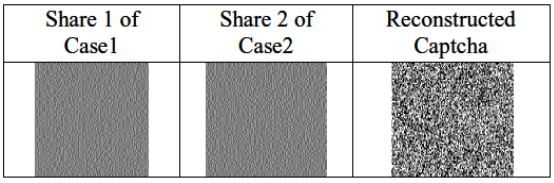


Figure 5: Creation and stacking of shares

6. Results and Discussions

It is observed that both original and reconstructed image captcha's are related with high degree of correlation. The correlation coefficient of original captcha and reconstructed captcha are shown in TABLE I. Also when two different shares are stacked their corresponding correlation co-efficient is obtained as -0.0073.This shows that there will be zero degree of correlation between original and output images for two different shares.

TABLE I

Original Captcha	Reconstructed Captcha	Correlation Coefficient
		0.9679
		0.9598
		0.9627
		0.9578
		0.9657

7. Conclusion

Currently phishing attacks are so common because it can attack globally and capture and store the users' confidential information. This information is used by the attackers which are indirectly involved in the phishing process. Phishing websites as well as human users can be easily identified using our proposed "Anti-phishing framework based on Visual Cryptography". The proposed methodology preserves confidential information of users using 3 layers of security. 1st layer verifies whether the website is a genuine/secure website or a phishing website. If the website is a phishing website (website that is a fake one just similar to secure website but not the secure website), then in that situation, the phishing website can't display the image captcha for that specific user (who wants to log in into the website) due to the fact that the image captcha is generated by the stacking of two shares, one with the user and the other with the actual database of the website.

Second layer cross validates image Captcha corresponding to the user. The image Captcha is readable by human users alone and not by machine users. Only human users accessing the website can read the image Captcha and ensure that the site as well as the user is permitted one or not. So, using image Captcha technique, no machine based user can crack the password or other confidential information of the users. And as a third layer of security it prevents intruders' attacks on the user's account. This method provides additional security in terms of not letting the intruder log in into the account even when the user knows the username of a particular user. The proposed methodology is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market.

References

[1] Ollman, G. (2004) The Phishing Guide – Understanding and Preventing, White Paper, Next Generation Security Software Ltd.
[2] Heise Security (2005) German Interior Minister Schily requests protection against online scams, http://www.heise.de/security/
[3] James, D.; Philip, M. Power, Signals, Controls and Computation (EPSCICON), 2012 , pp. 1-5.
[4] Wei-Bin Lee; Hsing-Bai Chen; Shun-Shyan Chang; Chia-Chi Yang Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2011, pp. 141-144.
[5] Tich Phuoc Tran; Pohsiang Tsai; Jan, T. Pattern Recognition, 2008. ICPR 2008, pp. 1-4
[6] B. Borchert, .Segment Based Visual Cryptography,. WSI Press, Germany, 2007.
[7] W-Q Yan, D. Jin and M. S. Kanakanahalli, .Visual Cryptography for Print and Scan Applications,. IEEE Transactions, ISCAS-2004, pp.572-575.
[8] T. Monoth and A. P. Babu, .Recursive Visual Cryptography Using Random Basis Column Pixel Expansion,. in Proceedings of IEEE International Conference on Information Technology, 2007, pp. 41-43.
[9] H. J. Kim, V. Sachnev, S. J. Choi and S. Xiang, .An Innocuous Visual Cryptography Scheme,. in Proceedings of IEEE-8th International Workshop on Image Analysis for Multimedia Interactive Services, 2007.
[10] C. Blundo and A. De Santis, .On the contrast in Visual Cryptography Schemes,. in Journal on Cryptography, vol. 12, 1999, pp. 261-289.

Licensed Under Creative Commons Attribution CC BY

[11] P. A. Eisen and D. R. Stinson, .Threshold Visual Cryptography with speci_ed Whiteness Levels of Reconstructed Pixels,. Designs, Codes, Cryptography, vol. 25, no. 1, 2002, pp. 15-61.
[12] E. R. Verheul and H. C. A. Van Tilborg, .Constructions and Properties of k out of n Visual Secret Sharing Schemes,. Designs, Codes, *Cryptography*, vol. 11, no. 2, 1997, pp. 179-196.
[13] H. Yan, Z. Gan and K. Chen, .A Cheater Detectable Visual Cryptography Scheme,. *Journal of Shanghai Jiaotong University*, vol. 38, no. 1, 2004.
[14] G. B. Horng, T. G. Chen and D. S. Tsai, .Cheating in Visual Cryptography,. *Designs, Codes, Cryptography*, vol. 38, no. 2, 2006, pp. 219-236.
[15] 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.
[16] CAPTCHA: Using Hard AI Problems For Security Luis von Ahn1, Manuel Blum1, Nicholas J. Hopper1, and John Langford.
[17] A Text-Graphics Character CAPTCHA for Password Authentication Matthew Dailey Chanathip Namprempre.

Author Profile

B. Jenny Jyoshna Obtained the MCA pg degree from C. R. Reddy college for women, Eluru . At present she is pursuing the M. Tech in Computer Science and Engineering (CSE) Department at Guntur Engineering College, Guntur.

Shaik Nyamathulla obtained the B. Tech. degree in Computer Science and Information Technology (CSIT) from **Hi-Point college of Engineering and Tech,** Hyderabad in 2009 and M. Tech from Guntur Engineering College in 2013. He has 5 years of teaching experience and working in Computer Science and Engineering (CSE) Department at **Guntur Engineering College**, Yanamadala, Guntur District.

Licensed Under Creative Commons Attribution CC BY