Volume 6, Issue 1, January 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Visual Cryptographic Scheme Framework to Avert Phishing

[1]Deepika, [2]Sumati, [3]Prateek Thakral
[1, 2] Assistant Professor, Department of Computer Science, Arya P.G. College, Haryana, India
[3]Assistant Professor, Department of Computer Applications, National Institute of Technology, Haryana, India

Abstract---Phishing is an attempt made by attackers to retrieve useful personal information about an individual by tempting him with creative and attractive links. A phishing website is a mock website that looks similar in appearance but different in destination.Nowadays phishing has become one of the major issuesandthe number of phishing attacks is increasing at high rate. In this paper, an image based authentication technique has been implemented using visual cryptographyscheme to prevent phishing. The use of visual cryptography technique is scrutinize to preserve the privacy of image captcha by disintegrating the image into two shares that are stored in separate database servers such that the original image captcha can be revealed only when both of the shares are simultaneously available; the individual share of images do not expose the identity of the original image.

Keywords: Phishing, Visual Cryptography, Shares, Image Captcha, Security

I. INTRODUCTION

The concept of fishing in a lake is quite similar to the concept of phishing on internet, where the internet refers to the lake while the valuable personal information about an individual corresponds to the fish. Nowadays, online attacks are becoming viral because of increase in the number of online transactions. Phishing has become a con game that scammers use to collect the personal information from suspecting users. The act of sending spoofed emails that falsely claims to be from a genuine organization or websites such as PayPal, Flipkart, or other banking institutions[6]. The email will ask the recipient to provide confidential information, such as bank account details, PINs or passwords; these details are then used by the owners of the website to accomplish fraud.

Today, most applications are only as secure as their underlying system. In account of the design and technology of middleware has upgraded gradually and ceaselessly, their detection has become a challenging problem[4]. And thus consequently, it is nearly impracticable to consider the trustworthiness and security of a computer that is linked to the internet. E-banking and e-commerce users are facing the issues of phishing scams, so the need of the hour is to find the appropriate way of handling applications that gives high level security.

Fig. 1Phishing Process

An attacker who tries to trick internet users to provide confidential information such as banking passwords and credit card information is a malicious activity and is termed as phishing [7]. At random, the URL of bogus websites are sent to large number of users via instant messages or electronic mails. Unsuspected users are asked to input their personal information on the hoax website to which they were directed whenever they click on the link. Phishing process is done in following four steps. Firstly, the phisher set up a hoax website which looks exactly like the legitimate one. In second step, to convince the victims to visit their websites, phisher then sends them a large amount of spoofed e-mails that consists the link of the fake websites. In next step, the victim clicks on the link and visits the fake website and put confidential information there. Lastly, the personal information of the victim is stolen by the phisher which are then used to perform deceitful activities such as money transferring from victim account. This is shown in figure 1.

Generally, while using social engineering techniques, phishing is scrutinized as an illegal and criminal activity. By subterfuging as a trustworthy person or business in an electronic communication, phisher attempts to unfairly attain the sensitive information such as passwords and credit card details of the user. In our paper, we present a methodology that can be used as a safe way against phishing by using the concept of visual cryptography. In the next two sections, we introduced the concept of visual cryptography and current methodology which are being used now days to get prevention from phishing. In section 4, we describe our proposed methodology that can be used efficiently to prevent phishing in a more secure manner. In section 5, we draw a detail conclusion.

II. RELATED WORK

Several methods have been introduced and approaches have been proposed to defend against phishing which mainly comprises techniques like blacklists, heuristic detection and the page similarity assessment [4]. These all are mainly DNS based anti-phishing approaches that still consists of some flaws. Those websites that are not present in the blacklist database remains undetected in blacklist based detection technique. This is because the life cycle of phishing websites is too short and the inception of blacklist has a long lag time, making this technique not highly precised.Heuristic-based anti-phishing techniqueis used to approximate whether a page has some phishing heuristics characteristics. But in this technique phisher can easily evade the heuristic characteristic detection by using some proficient technical ways.Similarity assessment based is a time-consuming technique. The speed of calculating the visual similarity between pages is too slow and low accuracy rate relying upon many factors, such as the text, images, and similarity measurement techniques making this technique unacceptable for detection of phishing website on client machine. Many related methods concerning the theory and the applications of visual cryptography have been proposed by researcher. An extended visual cryptography scheme, coloured visual cryptography scheme has been studied by researchers [7]. Most of the previous research work on VC focused on improving two parameters: pixel expansion [3] [8] and contrast [7] [11]. Text Graphics Character CAPTCHA [11], Colour images based visual cryptography has been studied [5]. Recently, number of applications of visual cryptography, such as authentication, human identification, copyright protection, watermarking, mobile ticket validation, visual signature checking, biometrics etc. has been introduced [7]. The major drawback of this scheme is that visually impaired people cannot make use of this technique [9].

III. VISUAL CRYPTOGRAPHY

Cryptography is a technique of achieving security by encoding data to make them non-readable in such a way that only intended users with appropriate keys can decrypt the data and no other third party can misuse the data. In other words, it is a method of shielding confidential information. The term visual cryptography was pioneered by Moni Naor and Adi Shamir in 1994 [2][3]. They analyzed and concluded that the visual cryptography consists of two vitalcharacteristics. The first characteristic is its perfection in keeping a message secret and the second one is the method used for decryption of the message which required neither the computer aided processes nor complex decryption algorithms. It merelyuses human visual system to discover the confidential information from the stacked images of variousconsent set of shares.

In visual cryptography, an image is decomposed into n shares so that only authorized user with all genuine n sharescould decrypt the secret image, while someone with n-1 shares could not able to unveil any information about the original image. The decryption of the images is performed by overlapping all the n shares, when each share is printed separately (serving the purpose of secret key) and hence revealing the original image .Unlike other cryptographic techniques which uses complex algorithms a novel approach to visual cryptography make use of the straight forward algorithms and also provides information security . Visual cryptography posses some characteristics such as perfection in security, decryption of image without the aid of a computing device and robustness against lossy compressions and distortion due to its binary attribute [6]. Hence, the overall visual cryptographic process can be summarized as [3]:

A. Visual Cryptographic Schemes

Visual Cryptographic Scheme is the cryptographic way which allows us to encrypt the visual information in such a way that the encrypted messages can be decrypted by employing human visual system.This can be achieved by one of the following structure scheme [5]:

1. (2, 2) Threshold Visual Cryptography scheme: In this scheme, a confidential image is encrypted into two distinct shares that unveil the confidential information when both shares are overlapped. No additional information is required. This is the simplest threshold scheme.
2. (2,n) Threshold Visual Cryptography scheme: The secret image in this scheme is encrypted into n shares in such a way that when any of the two such shares are overlaid the confidential information in form of image is revealed.
3. (n, n) Threshold visual cryptography scheme: This scheme works on the rule that after the encryption of a confidential image into n shares, the confidential image is revealed when all the n shares are combined.
4. (k, n) Threshold visual cryptography scheme: When any group of at least k shares are overlaid after the confidential image is encrypted into n shares, the original image is revealed. In this scheme stacking fewer than k shares does not reveal any information about the confidential image [8].

In the case of (2, 2) VCS, the pixels are encrypted into (sub pixels) shares from the original image pixels P. The VCS model works on the principle of basis matrices. The whole (2, 2) VCS model can be outlined by two basis matrices: one for black pixel and one for white pixel. Basis matrix for (2, 2) VCS is:

B0 = 1 0 B1 = 1 0
1 0 0 1

Fig. 2 denotes the share of a white pixel and a black pixel. Value of the original pixel P can be determined, after the overlapping of two shares. 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.

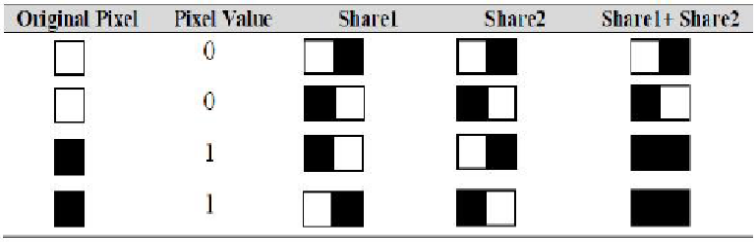


Fig 2. Illustrating (2, 2) VCS scheme with 2 sub pixel construction [8]

IV. CURRENT METHODOLOGY

In the current scenario, as shown in Figure 3, when the end user wants to access his secret information online (in the form of money transfer or payment gateway) by logging into his bank account or secure mail account, the person enters his usual information on login the page like username, password, credit card no. etc. But quite often, this information can be captured by phisher using phishing techniques. As the phished website would ask for all the confidential information at the login and store it in its separate database [4].

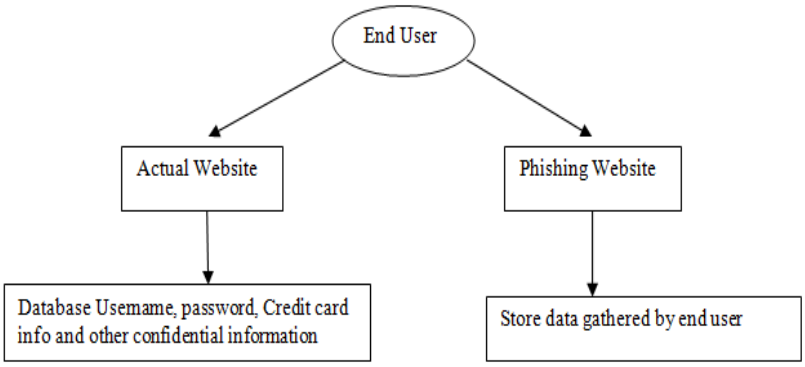


Fig 3. Current Scenario

V. PROPOSED METHODOLOGY

Methodology used in our paper is based on the Anti-Phishing image captcha validation scheme using visual cryptography. It prevents passwords and other confidential information from the phishing websites.The approach is divided into two phases:

i. Registration Phase
ii. Login Phase

A. Registration Phase

In the registration phase, a key string i.e. a password is asked from the user at the time of registration for the secure website. The key string can be alphanumeric string providing more secure environment. This alphanumeric string is concatenated with arbitrarily generated string in the server and an image captcha [11] is generated. The generated image captcha is partitioned into two shares such that one of the shares is kept safe with user and the other share is kept in the server. And for the later verification during login phase the user's share and the original image captcha is sent to the user. The generated image captcha is also stored in the actual database of any confidential website as confidential data. Even after registration, the user can change the key string when it is needed. The complete procedure of registration phase is shown in figure 4.

B. LoginPage

When the user logs in by entering his secret information for using his account, then first the user is asked to enter his username (i.e. 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 construct the image captcha. The image captcha is displayed to the user. The displayed image captcha is matched here with the captcha created at the time of registration. The text displayed in the image captcha is required to be entered by the end user and this can serve the purpose of password and using this, the user can log in into the website. By means of username and image captcha generated by stacking two shares,one can substantiate whether the website is genuine/secure website or a phishing website and can also authenticate whether the user is a human user or not. Figure5 is used to illustrate the login phase.

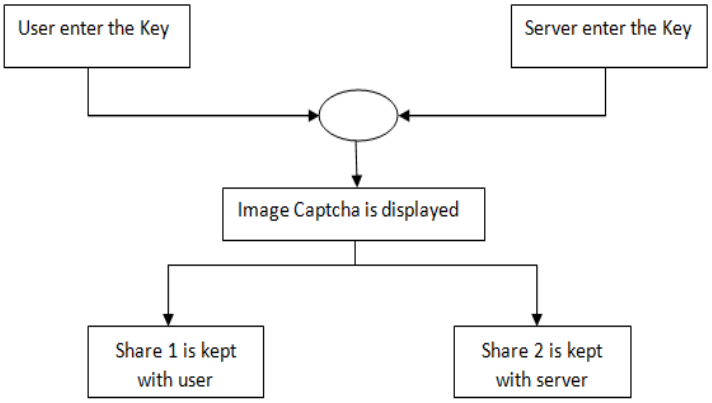


Fig. 4 Registration process for a website performed by theuser

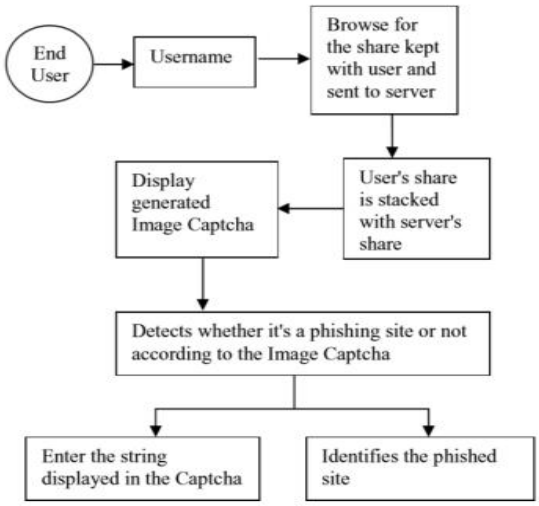
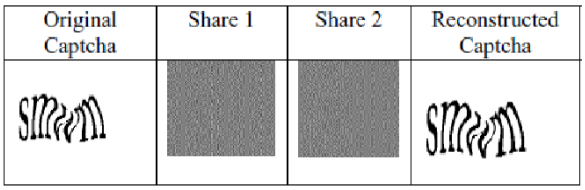


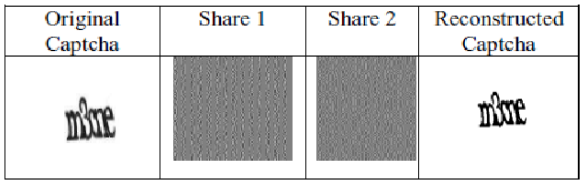
Fig. 5 When user attempt to log in into site

In order to login to the website the entire process is depicted in figure 6 as different cases.Case1 and Case 2illustrate the creation and stacking of two shares.

Case 1.



Case 2.



Case 3.

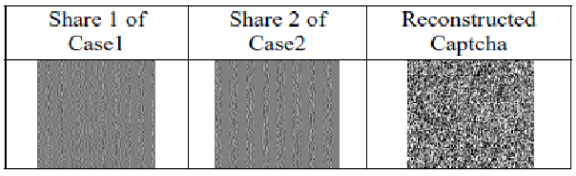


Fig 6. Creation and Stacking of Shares [5]

The image generated in reconstructed column in both cases 1 and 2 is the image constructed after the creation and heaping of shares of two original image captcha's. In Case3, share1 of first image captcha (Case 1) is combined with share 2 of second captcha (Case 2) resulting in an unrecognizable form of captcha.

VI. CONCLUSION

Phishing attacks have become so common because it attacks globally and capture the users' confidential and concealed information. This information is used for phishing processes and purposes. The method discussed in our paper can easily be used to identify phished websites. The methodology preserves confidential information of users using three layers of security. First layer make sure whether the website is a genuine website or a phishing website. If the website is a phishing websitethen in that condition, the phishing website can't display the image captcha for that particular user (who wishes to log in into the website) due to the fact that the image captcha is generated by the stacking of two shares, one which with the user and the other share with the actual database of the website. Next layer cross validates image captcha analogous to the user. The image captcha works on the fact that it 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 legitimate or not. So with the help of image captcha technique, no machine based user can decode the password or other confidential information of the users.Lastly, in third layer of security it prevents encroachers' attacks on the user's account. This method provides additional security interms of not permitting the encroacher log in into the account even when the user knows the username or some other confidential information of a particular user. The methodology is useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market.

REFERENCES

[1] Ollmann G., The Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research.

[2] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12**.**

[3] Dimple Kapoor1 , Swati Keshari , Saurabh Kumar Gaur, "An Overview of Visual Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, February 2014 ISSN: 2277 128X.

[4] Divya James, Mintu Philip , "A novel Anti-Phishing Framework Based on Visual Cryptography",IEEE, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012.

[5] Wenyin Liu, Xiaotie Deng, Guanglin Huang, and Anthony Y. Fu, "An Antiphishing Strategy Based on Visual Similarity Assessment", IEEE Internet Computing, v 10, n 2, p 58-65, March/April 2006.

[6] W-Q Yan, D. Jin and M. S. Kanakanahalli, .Visual Cryptography for Print and Scan Applications. IEEE Transactions, ISCAS-2004, pp.572-575.

[7] Sneha M. Shelke, Prof. Prachi A. Joshi, "A Study of Prevention of Phishing Threats using Visual Cryptography", (IJIRSE) International Journal of Innovative Research in Science & Engineering ISSN (Online) 2347-3207.

[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] Deepti Chaudhary, Rashmi Welekar, "Secure Authentication Using Visual Cryptography", International Journal Of Computer Science And Applications Vol. 8, No.1, Jan- Mar 2015 ISSN: 0974- 1011.

[10] Sridevi Thota, Naga VenkataSubbaRao Dupaguntla, Amrutha Kamal Gummadi, "Secured Bank Authentication using Image Processing and Visual Cryptography", International journal of Systems and Technologies , Double Blind Peer Reviewed Journal Vol 6, Issue 2, 2013, pp 32-40 ISSN 0974 – 2107.

[11] A Text-Graphics Character CAPTCHA for Password Authentication Matthew Dailey Chanathip Namprempre.

