A Study of Prevention of Phishing Threats using Visual Cryptography

Sneha M. Shelke, Prof. Prachi A. Joshi
Department of Computer Science and Engineering
Deogiri Institute of Engineering and Management Studies,
Aurangabad (MS), India

Abstract— **Phishing is the criminal and fraudulent act of attempting to acquire sensitive information such as username, passwords, account IDs, and credit card information etc by masquerading as a trustworthy entity in an electronic communication. The information thus acquired may be re-sold or used to cause financial losses. In the Internet, phishing can reach the user in several ways, e.g., through a web browser pop-up, instant messaging or e-mail. Recently a number of phishing attacks are increasing more and more. Hence there is a need for efficient mechanism for the prevention of phishing. Cryptography is one of an efficient mechanisms used to protect personal information. In this paper, anti fishing method based on visual cryptography has been studied.**

Keywords— Phishing, visual cryptography shares

I. INTRODUCTION

Internet is today’s common need and provides the backbone for modern living enabling ordinary people to shop, socialize, financial transaction, access all kinds of information anytime from anywhere and be entertained all thorough their own computers. As people’s reliance on the Internet grows, so the possibility of hacking and other security breaches increases regularly [1]. One such threat is phishing attack which can perform identity theft [1-4].

In the past few years, phishing has become one of the major issues and the number of phishing attacks is increasing more and more [2]. Lot of users become victim to these attacks. Phishing websites are a replica of genuine websites. Phishing website has visual similarity and website pages look exactly like real web pages. Only specialists can identify these types of phishing websites immediately. But all the web users are not specializing in the computer engineering and hence they become victim by providing their personal details to the phishing artist. Phishing is continuously evolving since it is easy to copy an entire website using the HTML source code. By making slight changes in the source code, it is possible to direct the victim to the phishing website. Phisher uses a lot of techniques to lure the unsuspected web user. They send generic greetings to the customers to check their account immediately. They also send threat messages indicating to update their account immediately, otherwise their account will be cancelled. Thus an efficient mechanism is required to identify the phishing websites from the legitimate websites in order to save credential data [5].

In the Internet, phishing can reach the user in several ways, e.g., through a web browser pop-up, instant messaging or e-mail. Usually, the victim is persuaded to perform a mouse click to download and install malicious code or access a fraudulent web site without being aware of it [6].

In email-born phishing attacks, phisher sends emails that mislead their victims into revealing credential information such as account numbers, passwords, or other personal information to the phisher. For example, Fisher send the fake e-mail message to the bank user’s, as if the database of the bank has been crashed due to some technical reasons, so they request you for updation of the personal information. As most phishing emails are nearly identical to the normal emails, it is quite difficult for the average users to distinguish phishing emails from non-phishing once. Moreover, phishing tactics have become more and more complicated and the phishers continually change their ways of perpetrating phishing attacks to defeat the anti-phishing techniques. In some cases, the phishers implant malicious software that controls a computer so that it can participate in future phishing scams [6-8].

II. RELATED WORK

Phishing is a criminal trick of stealing victim's personal sensitive information by luring users to visit a forged web page that designed to mimic a target page's own visual identity. Recently, phishing has become one of the major issue and the number of phishing attacks is increasing more and more [2,5,6,9].

In the past few years, a number of anti-phishing solutions have been proposed that mainly divided into three categories:

1. Server-based schemes, such as shared e-certificate and dynamic security skins. They allow the remote server to provide the client with a unique identity that can be used to verify whether it matches the corresponding local identity, but this requires user awareness and prior knowledge. Automated Challenge Response Method is one such authentication mechanisms [11].

2. Browser-integrated anti-phishing schemes, for instance, phishing websites filter in Internet Explorer, Google Safe Browsing for Firefox. If the requested web page is checked in a blacklist of known phishing sites, the user will be warned. How-ever, the average time that a phishing site stays online is 3.8 days, the longest time is only 30 days, so the disadvantage of the approach is that non blacklisted phishing sites not be recognized[4, 12].

3. Anomaly-based phishing web detection, which examines the anomalies in web pages to detect phishing pages and it is independent of any phishing solutions and have been attracted many attentions. Many anti phishing methods based on phishing webpage detection, which is basis of preventing phishing attack have been proposed recently [3].

However anti-phishing solutions have several drawback, Blacklist-based technique with low false alarm probability, but it cannot detect the websites that are not in the blacklist database. Because the life cycle of phishing websites is found minimum 3.8 days and maximum 30 days and the establishment of blacklist has a long lag time, the accuracy of blacklist is not too high. Heuristic-based anti-phishing technique, with a high probability of false and failed alarm, and it is easy for the attacker to use technical means to avoid the heuristic characteristics detection.

Assessment based technique is time-consuming. It needs too long time to calculate a pair of pages, so using the method to detect phishing websites on the client terminal is not suitable. And there is low accuracy rate for this method depends on many factors, such as the text, images, and similarity measurement technique. However, this technique (in particular, image similarity identification technique) is not perfect enough yet [3,4,12].

III. VISUAL CRYPTOGRAPHY

Cryptography is an essential tool to protect the data that transmits between users by encrypting the data so that only intended users with appropriate keys can decrypt the data . It uses human visual system hence need not required a computer. Therefore, visual cryptography is a very convenient way to protect secrets when computers or other decryption devices are not available. Cryptography is the most commonly used mechanism in protecting data. A survey conducted by Computer Security Institute in 2007 revealed that 71% of companies utilized encryption for their data in transit [3, 7].

Visual cryptography is first proposed by Nior and Shamir to protect secrets [13]. They analyzed that the visual cryptography has two important features. The first feature is its perfect secrecy and the second is its decryption method which requires neither complex decryption algorithms nor the aid of computers. It uses only human visual system to identify the secret from the stacked image of some authorized set of shares. Therefore, visual cryptography is a very convenient way to protect secrets when computers or other decryption devices are not available. The simple decryption method is the reason that attracts many researchers to make further detailed inquiries in this research area.

Many related methods concerning the theory and the applications of visual cryptography have been proposed by researcher. An extended visual cryptography scheme, colored visual cryptography scheme has been studied by researchers. Most of the previous research work on VC focused on improving two parameters: pixel expansion and contrast [9, 14-16]. Text Graphics Character CAPTCHA [12], Color images based visual cryptography [17] have been studied.

Recently, more and more applications of visual cryptography, such as authentication, human identification, copyright protection, watermarking, mobile ticket validation, visual signature checking etc. are introduced [18, 19].

The most of the constructions of visual cryptography schemes are realized using two n × m matrices, S^0 and S^1, called basis matrices. The general method for the construction of basis matrices is discussed below.

A. Basis Matrices

Any black-and-white visual cryptography scheme can be described using two n x m Boolean matrices S^0 and S^1, called basis matrices, to describe the sub pixels in the shares. The basis matrix S^0 is used if the pixel in the original image is white, and the basis matrix S^1 is used if the pixel in the original image is black. The use of the basis matrices S^0 and S^1 can have small memory requirements (it keeps only the basis matrices S^0 and S^1), and it is efficient (to choose a matrix in C_0 or C_1) because it only generates a permutation of the columns of S^0 or S^1. The basis matrices of (2,2) VCS model are

$$S^0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{1}$$

Here, element 1 means the presence of a black pixel in the share image generated from this matrix and element 0 means the presence of white pixel. Hence we could conclude that, Visual Cryptography scheme represented in computer using n x m Basis matrices. Basis matrices are binary n x m used to encrypt each pixel in the secret image, where n is the number of participants in the scheme and m is the pixel expansion. The following algorithm is used to implement a VCS using basis matrices:

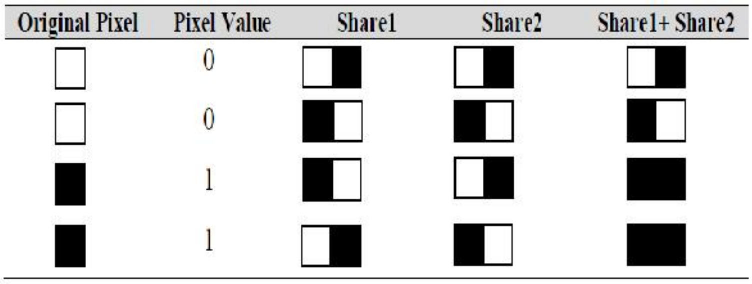
B. Various Visual Cryptography Schemes (VCS)

The general construction of various visual cryptography schemes is as follows

1. (2, 2) Threshold visual cryptography scheme: In this scheme, 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 visual cryptography 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 visual cryptography scheme: This scheme encrypts the secret image to n shares such that when all n of the shares are combined the secret image is revealed. The user will be prompted for n, the number of participants.
4. (k, n) Threshold visual cryptography scheme: This scheme says n shares will be produced to encrypt an image, and k shares must be stacked to decrypt the image. If the number of shares stacked is less than k, the original image is not revealed.

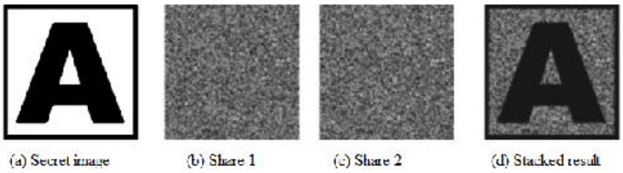
Let us consider a binary secret image S containing exactly m pixels. The dealer creates two shares (binary images), S1 and S2, consisting of exactly two pixels for each pixel in the secret image as shown in Table 1. If the pixel in S is white, the dealer randomly chooses one row from the first two rows of Table 1. Similarly, if the pixel in S is black, the dealer randomly chooses one row from the last two rows of Table 1.

TABLE I. PIXEL PATTERNFOR (2,2) VCS WITH 2-SUBPIXEL LAYOUT



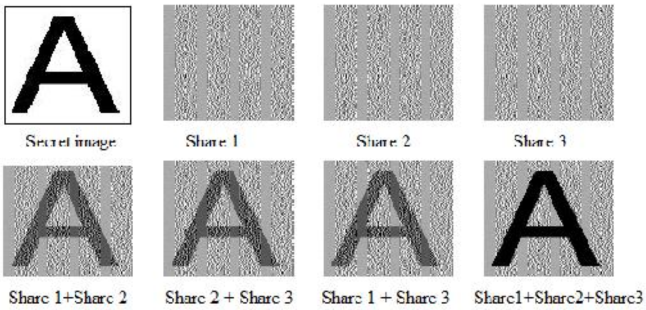
Original Pixel	Pixel Value	Share1	Share2	Share1+ Share2
□	0	□■	□■	□■
□	0	■□	■□	■□
■	1	■□	□■	■■
■	1	□■	■□	■■

To analyze the security of the 2-out-of-2 VCS, the dealer randomly chooses one of the two pixel patterns (black or white) from the Table 2.1 for the shares S1 and S2. The pixel selection is random so that the shares S1 and S2 consist of equal number of black and white pixels. Therefore, by inspecting a single share, one cannot identify the secret pixel as black or white. This method provides perfect security. The two participants can recover the secret pixel by superimposing the two shared subpixels. If the superimposition results in two black subpixels, the original pixel was black; if the superimposition creates one black and one white subpixel, it indicates that the original pixel was white. In visual cryptography, the white pixel is representing by 0 and the black pixel by 1. Implementation of (2,2) and (2,3) VCS is given below.



(a) Secret image (b) Share 1 (c) Share 2 (d) Stacked result

Fig. 1. Implementation of a (2, 2) VCS



Secret image Share 1 Share 2 Share 3

Share 1+Share 2 Share 2 + Share 3 Share 1 + Share 3 Share1+Share2+Share3

Fig. 2. Implementation of a (2, 3) VCS

IV. CONCLUSION

Nowadays phishing has become one of the major issue and the number of phishing attacks is increasing more and more. Personal information is acquired in an electronic communication to cause financial losses. Lot of users becomes victim to these attacks. Hence s strong antifishing mechanism is required. In this paper anti fishing solution based on visual cryptography has been studied. From the literature it is observed that cryptography is an essential tool to protect the data. Visual cryptography is a very convenient way to protect secrets. The developments and proposals by different authors in visual cryptography schemes are reviewed. The visual cryptography scheme is very useful in providing mutual authentication. The different perspectives on visual cryptography such as types of access structures, types of shares of secret images are discussed in this paper.

REFERENCES

[1] Liang H., & Xue Y., Understanding security behaviors in personal computer usage: A threat avoidance perspective. Association for Information Systems, 11(7), 2010, 394–413.

[2] Nalin Asanka Gamagedara Arachchilage, Steve Love, Security awareness of computer users: A phishing threat avoidance Perspective, Computers in Human Behavior 38 (2014) 304–312

[3] Yuancheng Lia et al., “A semi-supervised learning approach for detection of phishing web pages”, Optik, 124 (2013) 6027– 6033

[4] Anti-Phishing Working Group (APWG), Phishing activity trends report for the month of June, 2007 http://www.antiphishing.org/

[5] Isredza Rahmi A. Hamid, Jemal H. Abawajy, “An approach for profiling phishing activities” computers & security 45 (2014) 27 -41

[6] Cleber K. Olivo, Altair O. Santin, Luiz S. Oliveiraba “Obtaining the threat model for e-mail phishing”, Applied Soft Computing 13 (2013) 4841–4848Julian Jang- Jaccard ,

[7] Surya Nepal, “A survey of emerging threats in cyber security” Journal of Computer and System Sciences 80 (2014) 973–993

[8] Won Kim, Ok-Ran Jeong, ChulyunKim, Jungmin So The dark side of the Internet: Attacks, costs and responses, Information Systems 36 (2011) 675–705

[9] Carlo Blundo, Stelvio Cimato, Alfredo De Santis, Visual cryptography schemes with optimal pixel expansion, Theoretical Computer Science 369 (2006) 169 – 182

[10] Santhana Lakshmi V, Vijaya MS, Efficient prediction of phishing websites using supervised learning algorithms, Procedia Engineering 30 (2012) 798 – 805

[11] Thiyagarajan, P., Venkatesan, V. P., Aghila, G., "Anti-Phishing Technique using Automated Challenge Response Method'", in Proceedings of IEEE- International Conference on Communications and Computational Intelligience, 2010.

[12] Divya James, Mintu Philip, A novel anti phishing framework based on visual cryptography, International Journal of Distributed and Parallel System, Vol.3, No.1, 2012, 207-217

[13] M. Naor and A. Shamir, Visual Cryptography, Advances in Cryptology-Eurocrypt’94, LNCS 950, pp. 1-12, 1995.

[14] C. Blundo and A. De Santis, .On the contrast in Visual Cryptography Schemes, in Journal on Cryptography, vol. 12, 1999, pp. 261-289.

[15] 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.

[16] 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.

[17] Y.C. Hou, C.Y. Chang, F. Lin, Visual cryptography for color images based on color decomposition, Proceedings of the Fifth Conference on Information Management, Taipei, November 1999, pp. 584–591.

[18] Chen-Chang Wang, Shen-Chuan Tai and Chong-Shou Yu, Repeating Image Watermarking Technique by the Visual Cryptography, IEICE Trans. Fundamentals, E83–A(8) : 1589– 1598, 2000.

[19] Yan,W.Q., Jin, D., Kankanhalli, M.S.: Visual cryptography for print and scan applications.In: Proceedings of International Symposium on Circuits and Systems, Vancouver, Canada, pp. 572–575, 2004.

[20] http://www.phishing.org

[21] https://www.us-cert.gov/report-phishing