International Journal of Computer Science and Engineering Communications- IJCSEC. Vol.2 Issue.4, July 2014. ISSN: 2347–8586

Visual Cryptography Scheme to Predict Phishing Sites

Dr. D.C. Joy Winnie Wise[#1], Mr. H. Jeyamohan[#2] ,A. Sreenivasan[*3], K.P.Vijaiy[*3]

[#1]*Professor, HOD Dept of CSE, Alpha College of Engg, Chennai, T.N, India.*

[#2]*Assistant Professor, Dept of CSE, Alpha College of Engg, Chennai, T.N, India.*

[*3]*U.G Students, B.E CSE, Alpha College of Engg, Chennai, T.N, India.*

[1]vijaiy.kp@gmail.com, [2]sreeni2025@gmail.com

Abstract - Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information etc from unsuspecting victims for identity theft, financial gain and other fraudulent activities. In this paper we have proposed a new approach named as "A Novel Antiphishing framework based on visual cryptography" to solve the problem of phishing. Here an image based authentication using Visual Cryptography (vc) is used. The use of visual cryptography is explored to preserve the privacy of image captcha by decomposing the original image captcha into two shares that are stored in separate database servers 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.

Keywords – Vc, Passwords, Privacy

I. INTRODUCTION

VISUAL cryptography (VC), which was proposed by Naor and Shamir, allows the encryption of secret information in image form [1]. Following their work, much research was done on visual secret sharing schemes (VSSs) [2]. From the point of view of access structures, the existing VC schemes (VCSs) can be divided into two categories: threshold access structure (also known as k-out-of-n VCSs or (k, n)-VCSs) [3]–[5] and general access structure (GAS) [6]–[12]. Naor and Shamir focused on how to generate n shares such that the secret image is revealed by at least k shares ($2 \leq k \leq n$).mobile devices have mobile databases in order to achieve stable data processing.

Ateniese et al. (hereinafter Ateniese) [6] proposed the GAS concept and also developed a VC-based solution for some GASs. Using the GAS enables dealers to define reasonable combinations of shares as decryption conditions rather than to specify the number of shares. For example, if there are four participants (one president, one vice president, and two managers) sharing a secret, the president may expect to decrypt the secret with any single colleague who holds one of the other shares, whereas the vice president is allowed to obtain the secret only with two managers. The two managers are restricted from accessing the secret. Given these flexibilities, we also can set the number of shares as the decrypting condition. Clearly, (n, n)- and (k, n)-VCSs are special cases of the GAS.

The pixel-expansion problem is a major drawback with most VCSs that use the VC-based approach. The pixelexpansion problem affects the practicability of a VC scheme because it increases the storage and/or transmission costs. Moreover, the pixel-expansion problem usually introduces the side effect that the recovered secret images have less contrast. The contrast of the recovered images decreases in proportion to 1/m, whereas the shares are expanded by a factor of m times..

As a result, the decrease in contrast limits the application of these VC schemes. To address the pixel expansion problem, Adhikari et al. also proposed construction methods for VCSs for GASs; their approach aims to reduce the pixel expansion factor for (k, n)-VCSs [10]. Hsu et al. (hereinafter Hsu) used the probability concept to construct a VCS for GAS [7], [8]. However, Hsu's method does not guarantee enough blackness in some access structures, such that recovered images cannot be recognized by the naked eyes. Liu et al. proposed a deterministic construction method for GASs to balance the drawbacks of display quality and pixel expansion [9].

The developer should use a particular library that is provided by the vender of mobile database or modify existing mobile applications for synchronization process. Because of these flexible restrictions, the extensibility, adaptability and flexibility of mobile business systems are markedly decrease. This problem must be solved in order to build efficient mobile business systems because upcoming mobile environments will have heterogeneous characteristics in which diverse mobile devices, mobile databases, and

RDBMS exist. This paper suggests new SAMD (Synchronization Algorithms based on Message Digest) in order to resolve the problems mentioned above. SAMD resolves synchronization problems using only standard SQL queries as certified by the ISO (International Organization for Standardization). This is followed by a possible synchronization of any data combination regardless of the kind of server-side database or mobile database.
The SAMD therefore would provide extensibility, adaptability and flexibility.

II. BACKGROUND AND RELATED WORKS

A. Background of General Access Structures

Suppose P = {1, . . . ,n} is a set of n participants, and 2P denotes the power set of P. The quantity Qual denotes the set of subsets of P from which we wish to share the secret; thus, Qual ∈ 2P. Each set in Qual is said to be a qualified set, and each set not in Qual is called a forbidden set (denoted as Forb). Obviously, Qual ∪ Forb = 2P and Qual ∩ Forb = ∅. Based on these definitions, a VCS for an access structure (Qual, Forb) on P can yield n shares. When we stack together the shares associated with the participants in any set X ∈ Qual, we can recover the secret image, but any X ∈ Forb has no information on the stacked image.
To overcome above problem we have introduced the algorithm SAMD (Synchronization Algorithms based on Message Digest) SAMD resolves synchronization problems using only standard SQL queries as certified by the ISO (International Organization for Standardization). The mobile SAMD therefore would provide extensibility, adaptability and flexibility. The SAMD makes the images at the table of the server-side database and the mobile database using a message digest algorithm; then the images, and the message digest values, are saved in the message digest tables on both sides.

B. Review of VCSs for GASs

1) Ateniese's Approach: In 1996, Ateniese first proposed a VC-based approach for VCSs for GASs. They mapped a VCS access structure to a graph and found both the lower and upper bounds on the size of the shares (i.e., the pixel-expansion factor) from the graph. They gave minimum pixel-expansion factors as well as basis matrices for VCSs for strong access structures for a maximum of four participants [6]. MacPherson extended Ateniese's model to include greyscale images and derive new results on the minimum possible pixel expansion for all possible GASs on at most four participants. However, a method for constructing the grey-scale VCSs for GASs remains an open problem [11]. As with other conventional VC-based approaches, the above-mentioned VCS approach for GASs also suffers from the pixel-expansion problem. There also are other drawbacks with Ateniese's approach. For example, black secret pixels cannot be completely recovered, the aspect ratio of the recovered image cannot be maintained, and this approach needs a sophisticated codebook design.

2) Hsu's Approach: In 2006, Hsu, for the first time, reported the formulation of an unexpanded VCS for a GAS problem as an optimization model [7], [8]. Their method adopts a set of n × 1 column vectors to share a secret pixel to encrypt n participants, thus eliminating the drawbacks of pixel expansion. Based on the model, a probability matrix can be found and used to encrypt a secret for a specific access structure. Hsu's objective is to maximize contrast values for all qualified recovered images subject to the security constraint. They use the goal-programming technique and also develop a geneticbased algorithm to solve the optimization problem [7], [8]. Hsu's approaches have better maximum and average contrast values for recovered images than Ateniese's results in some cases. However, Hsu's method still has problems. First, the approach is probabilistic, which leads to poor visual quality for the recovered secret images when the blackness of the images is low. Second, Hsu's objective cannot guarantee an acceptable contrast level for recovered images in the worstcase [8].

3) Lee's Approach: Lee proposed the formulation of a SIVCS for strong general access structures, (Qual, Forb), based on the probabilistic (n, n)–VCSs [12]. Lee's approach is to find the quantity of basis shares and a construction set for a given access structure. The basis shares that were yielded by the probabilistic (n, n)–VCSs are used to synthesize the shares of (Qual, Forb)-VCS according to the construction set.

III. THE PROPOSED MODEL

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. In Visual Cryptography (VC) an image is decomposed into shares and in order to reveal the original image appropriate number of shares should be combined.

VCS 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.

2. (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 be revealed.

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

IV. DESIGN AND IMPLEMENTATION

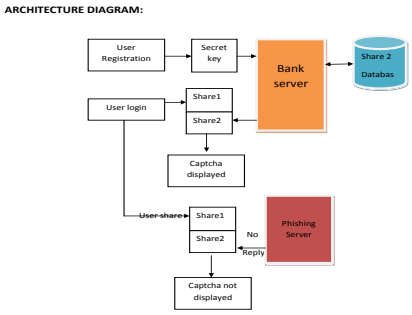

Fig .1 Architecture Diagram

Above Fig represents a model of visual cryptography scheme.

A.Registration with secret code

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 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 phasehe 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.

B.Image captcha Generation:

A key string is converted into image using java classes BufferedImage and Graphics2D. The image dimension is 260*60.Text color is red and the backround color is white.Text font is set by Font class in java.After image generation it will be write into the userkey folder in the server using ImageIO class. Grayscal conversion:The captcha image first convert into grayscal using luminance method.

Luminosity:

The graylevel will be calculated as

Luminosity = 0.21 × R + 0.72 × G + 0.07 × B

C. Shares Creation(VCS):

The image captcha is divided into two shares such that one of the share 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.

D.Login Phase:

In the Login phase first the user is prompted for the 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.

E.Testing share:

The entire process is depicted in 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.

V. CONCLUSION & FUTURE WORK

In this study, we propose a weak visual cryptography scheme for GASs using the optimization technique.

A part of implementation results for access structure 10, (a) the secret image (320 × 320 pixels, 192DPI), (b) the recovered image for set {2, 3, 5} (Model A, contrast $\alpha = 1/10$, blackness $\beta = 4/5$), (c) the recovered image for set {2, 3, 5} (Model B, $\alpha = 1/10$, $\beta = 9/10$), (d) the recovered image for set {1, 3, 4, 5} (Model C, $\alpha = 1/12$, $\beta = 1$). The proposed model for SIVCSs eliminates the disadvantages of the pixel-expansion problem from which conventional VC scenarios suffer. Our method guarantees the blackness of black
secret pixels for VCSs and improves the display quality of the worst-case image. The experimental results show that our approach performs better than those previously proposed in terms of the display quality of the recovered image, which includes the controllable blackness for black secret pixels and maintenance of the same aspect ratio as that of the original secret image.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology*, vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.
[2] J. Weir and W. Yan, "A comprehensive study of visual cryptography," in *Transactions on Data Hiding and Multimedia Security V* (LNCS), vol. 6010. New York, NY, USA: Springer-Verlag, 2010, pp. 70–105.
[3] C. N. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognit. Lett.*, vol. 25, no. 4, pp. 481–494, 2004.
[4] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Trans. Fundam.*, vol. E82-A, no. 10, pp. 2172–2177, 1999.
[5] P. L. Chiu and K. H. Lee, "A simulated annealing algorithm for general threshold visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 992–1001, Sep. 2011.
[6] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Inf. Comput.*, vol. 129, no. 2, pp. 86–106, 1996.
[7] C. S. Hsu and Y. C. Hou, "Goal-programming-assisted visual cryptography method with unexpanded shadow images for general access structures," *Opt. Eng.*, vol. 45, no. 9, pp. 097001-1–097001-10, 2006.
[8] C. S. Hsu, S. F. Tu, and Y. C. Hou, "An optimization model for visual cryptography schemes with unexpanded shares," in *Foundations of Intelligent Systems* (LNAI), vol. 4203. New York, NY, USA: Springer- Verlag, 2006, pp. 58–67.
[9] F. Liu, C. Wu, and X. Lin, "Step construction of visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 27–38, Mar. 2010.
[10] A. Adhikari, T. K. Dutta, and B. Roy, "A new black and white visual cryptographic scheme for general access structures," in *Progress in Cryptology* (LNCS), vol. 3348. New York, NY, USA: Springer-Verlag, 2004, pp. 399–413.
[11] L. A. MacPherson, "Grey level visual cryptography for general access structures," M.S. thesis, School of Comput. Sci., Univ. Waterloo, Waterloo, ON, Canada, 2002.
[12] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 219–229, Feb. 2012.
[13] F. Liu, C. K. Wu, and X. J. Lin, "A new definition of the contrast of visual cryptography scheme," *Inf. Process. Lett.*, vol. 110, no. 7, pp. 241–246, 2010.
[14] C. Blundo and A. De Santis, "Visual cryptography schemes with perfect reconstruction of black pixels," *Comput. Graph.*, vol. 22, no. 4, pp. 449–455, 1998.
[15] T. Hofmeister, M. Krause, and H. U. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," *Theoretical Comput. Sci.*, vol. 240, no. 2, pp. 471–485, 2000.
[16] H. Koga, "A general formula of the *(t, n)*-threshold visual secret sharing scheme," in *Advances in Cryptology, Asiacrypt*. New York, NY, USA: Springer-Verlag, 2002, pp. 328–345.
[17] Y. W. Chow, W. Susilo, and D. S.Wong, "Enhancing the perceived visual quality of a size invariant visual cryptography scheme," in *Information and Communications Security* (LNCS), vol. 7618. New York, NY, USA: Springer-Verlag, 2012, pp. 10–21.
[18] H. B. Zhang, X. F. Wang, W. H. Cao, and Y. P. Huang, "Visual cryptography for general access structure using pixel-block aware encoding," *J. Comput.*, vol. 3, no. 12, pp. 68–75, 2008.