A PROBABILISTIC MODEL OF VISUAL CRYPTOGRAPHY SCHEME FOR ANTI-PHISHING

V. Naresh[1], K. Pavithran[2], Mr. V. Muthu[3]

[1,2,3] Student, Department of Computer Science Anand Institute of Higher Technology Chennai, India
[3]Asst. Professor, Department of Computer Science Anand Institute of Higher Technology Chennai, India

---

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. The first defense should be strengthening the authentication mechanism in a web application. A simple username and password based authentication is not sufficient for web sites providing critical financial transactions In this paper we have proposed a new approach for phishing websites classification to solve the problem of phishing. Phishing websites comprise a variety of cues within its content-parts as well as the browser-based security indicators provided along with the website. The use of images 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. Several solutions have been proposed to tackle phishing.*

***Keywords*— Phishing, fraudulent activities, image captcha, authentication, critical financial transactions, security indicators.**

1. INTRODUCTION

Online transactions are nowadays become very common and there are various attacks present behind this. In these types of various attacks, phishing is identified as a major security threat and new innovative ideas are arising with this in each second so preventive mechanism should also be so effective. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. Phishing scams are also becoming a problem for online banking and e-commerce users. The question is how to handle applications that require a high level of security. Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication. 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 to shares, such that stacking a sufficient number of shares reveals the secret image.

2. RELATED WORKS

[1] A novel chaotic image cipher using a single-round modified permutation– diffusion pattern (ICMPD) was proposed. Unlike traditional permutation–diffusion structure, the permutation of ICMPD is operated on bit level instead of pixel level and its diffusion stage is operated on masked pixels, which are obtained by carrying out the classical affine cipher, instead of plain pixels. Following a divide-and-conquer strategy, this paper reports that ICMPD can be compromised by a chosen-plaintext attack efficiently and the involved data complexity is linear to the size of the plain-image.

[2] In permutation-only image ciphers, the entries of the image matrix are scrambled using a permutation mapping matrix which is built by a pseudo-random number generator (PRNG). The literature on the cryptanalysis of image ciphers indicates that permutation-only image ciphers are insecure against cipher text-only attacks and/or known/chosen plaintext attacks. However, previous studies have not been able to ensure the correct retrieval of the complete plaintext elements. In this paper, we re-visited the previous works on cryptanalysis of permutation-only image encryption schemes and made the cryptanalysis work on chosen-plaintext attacks complete and more efficient. We proved that in all permutation-only image ciphers, regardless of the cipher structure, the correct permutation mapping is recovered completely by a chosen-plaintext attack.

[3] Motivated by the cascade structure in electronic circuits, this paper introduces a general chaotic framework called the cascade chaotic system (CCS). Using two 1-D chaotic maps as seed maps, CCS is able to generate a huge number of new chaotic maps. Examples and evaluations show the CCS's robustness. Compared with corresponding seed maps, newly generated chaotic maps are more unpredictable and have better chaotic performance, more parameters, and complex chaotic properties. To investigate applications of CCS, we introduce a pseudo-random number generator (PRNG) and a data encryption system using a chaotic map generated by CCS.

[4] We investigate the potential application of a famous quantum computation model, i.e., quantum walks (QW) in image encryption. It is found that QW can serve as an

excellent key generator thanks to its inherent nonlinear chaotic dynamic behavior. Furthermore, we construct a novel QW-based image encryption algorithm. Simulations and performance comparisons show that the proposal is secure enough for image encryption and outperforms prior works. It also opens the door towards introducing quantum computation into image encryption and promotes the convergence between quantum computation and image processing.

[5] In the bit-level permutation, we divide each pixel into 8 bits, and arrange the positions of each bit by the generalized Arnold map in row and column direction. Hence, a significant diffusion effect is happened in the bit-level permutation. In the pixel-level diffusion procedure, we apply affine cipher to change the gray value and the histogram distribution of the permutated image. Various types of security analyses demonstrate that the proposed scheme is competitive with that ordinary permutation–diffusion type image cipher and proper for practical image encryption.

[6] The new (*n, k, p*)-Gray code has potential applications in digital communications and signal/image process in systems. This paper focuses on three illustrative applications of the (*n, k, p*)-Gray code, namely, image bit-plane decomposition, image denoising, and encryption. The computer simulations demonstrate that the (*n, k, p*)-Gray code shows better performance than other traditional Gray codes for these applications in image systems.

3. PROPOSED SYSTEM

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.

(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.

(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.

(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. 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.

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website. Our methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography.

It prevents password and other confidential information from the phishing websites. URL address on the address bar of your internet browser begins with "https"; the letter's' at the end of "https" means 'secured'.

Look for the padlock symbol either in the address bar or the status bar (mostly in the address bar) but not within the web page display area. Verify the security certificate by clicking on the padlock.

4. BLOCK DIAGRAM

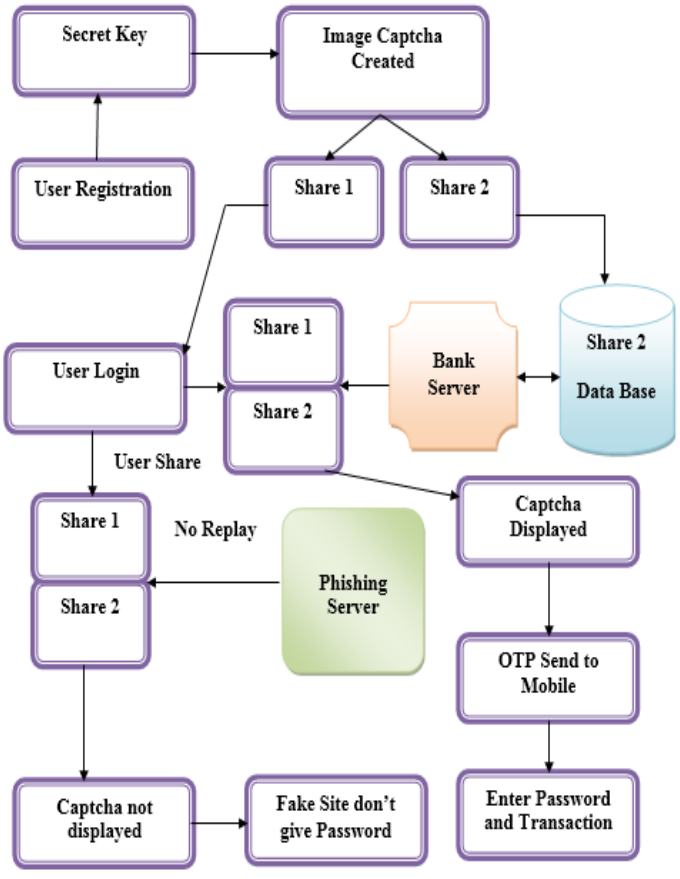

Figure 1: Architecture Diagram

5. 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. 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. The proposed methodology is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market.

6. FUTURE ENHANCEMENT

In future we can increase the security by adding many algorithms to encrypt the image. Encryption Phase contains many algorithms like Blowfish, Splitting and Rotating algorithm and (2,2) Visual Cryptography Scheme. First the "Blowfish Algorithm" is applied to the original image captcha then the image captcha is divided into many blocks and rearranged. After the image captcha blocks are rearranged, the "Splitting and Rotating Algorithm" is applied to the image captcha, and then the rearranged blocks are rotated. Then the rearranged and rotated blocks are combined. Then (2, 2) VCS scheme is applied to the combined blocks. This scheme is used to divide the encrypted image captcha into two shares based on white and black pixels. When the two sub pixels are identical blocks it considers as a white pixel. Likewise when the two sub pixels are different the original pixel is considered as black pixel. This VCS scheme adds more complication to the image captcha.

REFERENCE:

1. Y. Liu, L. Y. Zhang, J. Wang, Y. Zhang, and K.-W. Wong, "Chosen plaintext attack of an image encryption scheme based on modified permutation–diffusion structure," Nonlin. Dyn., vol. 84, no. 4, pp. 2241–2250, 2016.

2. A. Jolfaei, X.-W. Wu, and V. Muthukkumarasamy, "On the security of permutation-only image encryption schemes" IEEE Trans. Inf. Forensics Security, vol. 11, no. 2, pp. 235–246, Feb. 2016.

3. Y. Zhou, Z. Hua, C.-M. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," IEEE Trans. Cybern., vol. 45, no. 9, pp. 2001–2012, Sep. 2015.

4. Y.-G. Yang, Q.-X. Pan, S.-J. Sun, and P. Xu, "Novel image encryption based on quantum walks," Sci. Rep., vol. 5, no. 7, 2015, Art. no. 7784.

5. H. Zhu, C. Zhao, X. Zhang, and L. Yang, "An image encryption scheme using generalized Arnold map and affine cipher," Optik Int. J. Light Electron Opt., vol. 125, no. 22, pp. 6672–6677, 2014.

6. H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," Opt. Commun., vol. 284, nos. 16–17, pp. 3895–3903, 2011.