Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 3, March-2018

Implementing Secure Authentication For The Detection Of Web Server-Compromise Risks Using Visual Cryptography Scheme

S.Venkatha Lakshmi [*1], Prithiba Selvaraj [*2], J.Thirupura Sundari [*3], S.Poornima [*4]

Department of computer science, Panimalar Institute of technology

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 proposed system 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.*

I. INTRODUCTION

The recent years increase in the popularity of the Internet and multimedia communication has resulted in the fast development of information exchange and consumer electronics applications. However, it has also led to an increase in the demand of secure and real-time transmission of these data. Whereas, one of the viral risk factor is webserver-compromises.

Each month many thousands of websites are compromised by criminals and repurposed to host phishing websites, distribute malware, and peddle counterfeit goods. Despite the substantial harm imposed, the number of infected websites has remained stubbornly high. While many agree that the current level of Internet security is unacceptably low, there is no consensus on what countermeasures should be adopted to improve security or where limited resources should be focused. This majorly affects the real-time websites for transmission of data

II. LITERATURE SURVEY

A. Title: Chosen-Plaintext Attack Of An Image Encryption Scheme based On Modified Permutation–Diffusion Structure

Author Yuansheng Liu[1], Leo Yu Zhang[1], Jia Wang[1], Yushu Zhan[1], Kwok-wo Wong[1]

Abstract: 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.

B. Title: On The Security Of Permutation-Only Image encryption Schemes

Author Alireza Jolfaei[2], Xin-Wen Wu[2] and Vallipuram Muthukkumarasamy[2]

Abstract: In permutation-only image ciphers, the entries of the image matrix are scrambled using a permutation mapping matrix which is b uilt 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.

C. Title: Cascade Chaotic System With Applications
Author: Yicong Zhou[3],Zhongyun Hua[3], Chi-Man Pun[3] and C. L. Philip Chen[3]

Abstract 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.

D. Title: Novel Image Encryption Based On quantum Walks
Author: Yu-Guang Yang[4], Qing-Xiang Pan[4], Si-Jia Sun[4] and Peng Xu[4]

Abstract 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 in here nt-nonlinear chaotic dynamic behaviour. 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.

E. Title: An Image Encryption Scheme Using Generalized Arnold Map And Affine-cipher
Author: Md. Anisur Rahman1[5] , Alimul Haque Khan[5] , Dr. Tofayel Ahmed , Md. Mohsin Sajjad[5]

Abstract 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.

F. Title: (n, k, p)-Gray Code For Image Systems
Author: : Yicong Zhou[6], Karen Panetta[6], Sos Agaian[6], and C. L. Philip Chen[6]

Abstract The (*n, k, p*)-Gray code, which includes several commonly used codes such as the binary-reflected, ternary, and (*n, k*)-Gray codes. The new (*n, k, p*)-Gray code has potential applications in digital communications and signal/image processing systems. This paper focuses on three illustrative applications of the (*n, k, p*)-Gray code, namely, image bit-plane decomposition, image de-noising, 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.

G. Title: Colour Image Encryption Based On The Affine Transform And Gyrator Transform
Author: Hang Chen[7], Xiaoping Du[7] , Zhengjun Liu[7] , Chengwei Yang[7]

Abstract The RGB components of the colour image are converted into the real part and the imaginary part of a complex function by employing the affine transform. Subsequently the complex function is encoded and transformed in gyrator domain. The gyrator transform is performed twice to enhance the security of this encryption algorithm. The parameters in the affine transform and the gyrator transform are regarded as the key in the encryption algorithm. Some numerical simulations are made to test the validity and capability of the proposed colour encryption algorithm.

H. Title: A Novel Image Encryption Scheme Based On Improved Hyper Chaotic Sequences
Author: Congxu Zhu[8]

Abstract The hyper chaotic sequences are modified to generate chaotic key stream that is more suitable for image encryption. Secondly, the final encryption key stream is generated by correlating the chaotic key stream and plaintext

which result in both key sensitivity and plaintext sensitivity. The scheme can achieve high key sensitivity and high plaintext sensitivity through only two rounds diffusion operation. The performance test and security analysis has been performed using the histograms, correlation coefficients, information entropy, peak signal-to-noise ratio, key sensitivity analysis, differential analysis, key space analysis, and decryption quality and speed analysis.

I. Title: Breaking Row-Column Shuffle Based Image Cipher
Author: Weihai Li[9], Yupeng Yan[9], Nenghai Yu[9]

Abstract A redundancy based cipher-only attack is proposed to break row-column shuffle based image encryption algorithms, which are considered to be safe under cipher-only attack before although it is well known that they are fragile under known plaintext attack. This attack is carried out on the shuffle operations itself by analyzing the redundancy remained in cipher image, and doesn't care how the shuffle tables are generated. So, no matter how the shuffling tables are generated, this attack is valid. Experimental results show high quality deciphered images from one single cipher image, and that demonstrate the validity of our attack method.

J. Title: Colour Image Encryption Using Spatial Bit-Level Permutation And High-Dimension chaotic System
Author: Hongjun Liu[10], Xingyuan Wang[10]

Abstract Convert the plain color image of size (M×N) into a grayscale image of size (M×3N), then transform it into a binary matrix, and permute the matrix at bit-level by the scrambling mapping generated by piecewise linear chaotic map (PWLCM). Secondly, use Chen system to confuse and diffuse the red, green and blue components simultaneously. Experiment results and security analysis not only show that the scheme can achieve good encryption result, but also that the key space is large enough to resist against common attack.

III. PROPOSED WORK

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**.**

This can be achieved by the following access structure scheme.

(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.

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

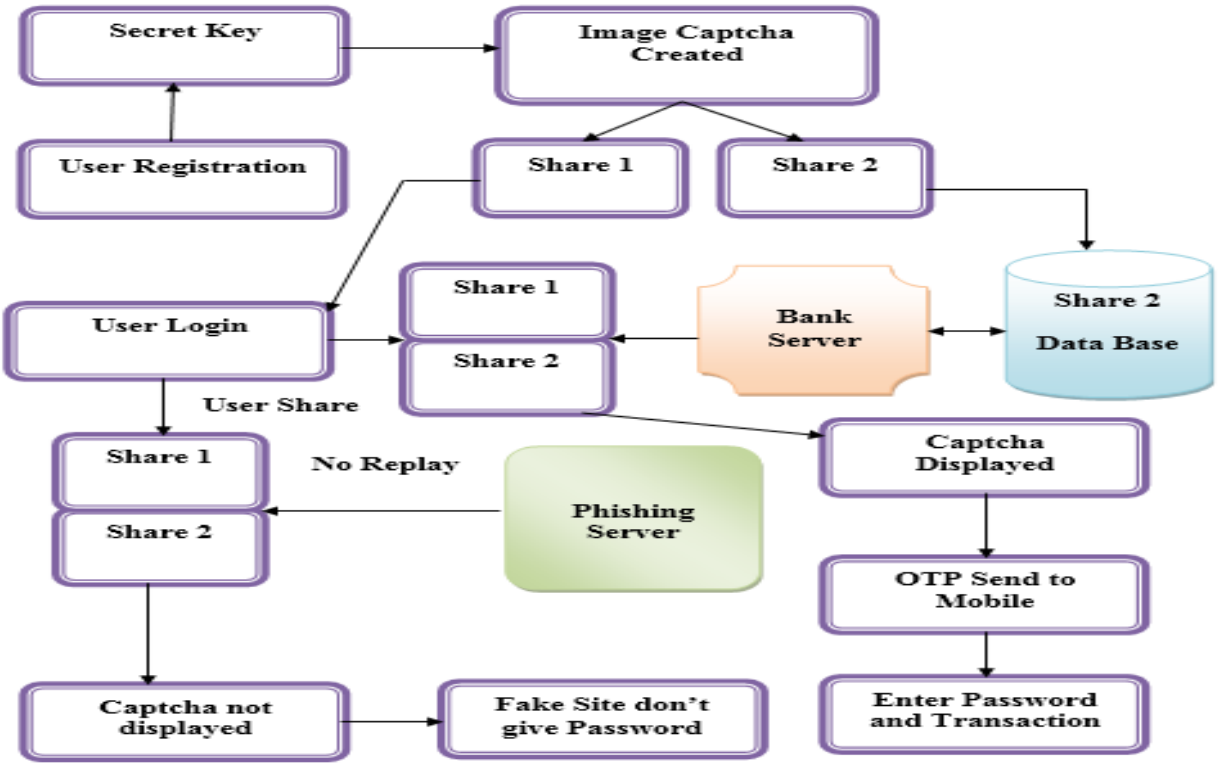

Figure 1.Block diagram

IV. CONCLUSION

This project is effectively useful in reducing the fraudulence in the real time web applications by strengthen authentication and it also detects phishing websites efficiently. This scheme improves the practical usability of valid webservers and highly reduces the webserver-compromise risks

V. REFERENCES

[1] Yuansheng Liu, Leo Yu Zhang, Jia Wang, Yushu Zhang, Kwok-wo Wong "Chosen-Plaintext Attack Of An Image Encryption Scheme based On Modified Permutation–Diffusion Structure" Springer Science+Business Media Dordrecht 2016.

[2] Alireza Jolfaei, Xin-Wen Wu and Vallipuram Muthukkumarasamy "On The Security Of Permutation-Only Image encryption Schemes" IEEE Transactions on Information Forensics And Security,2015.

[3] Yicong Zhou, Zhongyun Hua, Chi-Man Pun and C. L. Philip Chen "Cascade Chaotic System With Applications" IEEE Transactions On Cybernetics,2014.

[4] Yu-Guang Yang, Qing-Xiang Pan, Si-Jia Sun and Peng Xu "Novel Image Encryption Based Onquantum Walks" College of Computer Science and Technology, Beijing University of Technology, Beijing 100124.

[5] Md. Anisur Rahman1, Alimul Haque Khan, Dr. Tofayel Ahmed, Md. Mohsin Sajjad "An Image Encryption Scheme Using Generalized Arnold Map And Affine-cipher" Department of Mathematics and Computer Science, Indiana State University, Terre Haute, IN 47809, USA.

[6] Yicong Zhou, Karen Panetta, Sos Agaian, and C. L. Philip Chen "(n, k, p)-Gray Code For Image Systems" IEEE Transactions On Cybernetics, Vol. 43, No. 2, April2013.

[7] Hang Chen, Xiaoping Du , Zhengjun Liu , Chengwei Yang "Colour Image Encryption Based On The Affine Transform And Gyrator Transform" Department of Automation Measurement and Control, Harbin Institute of Technology, Harbin 150001, China, Elesvier 2013.

[8] Congxu Zhu "A Novel Image Encryption Scheme Based On Improved Hyper Chaotic Sequences" School of Information Science and Engineering, Central South University, Changsha, 410083, China, Elsevier 2011.

[9] Weihai Li, Yupeng Yan, Nenghai Yu "Breaking Row-Column Shuffle Based Image Cipher " Department of Electronic Engineering and Information Science University of Science and Technology of China

[10] Hongjun Liu, Xingyuan Wang "Colour Image Encryption Using Spatial Bit-Level Permutation And High-Dimension chaotic System" Faculty of Electronic Information and Electrical Engineering, Dalian 116024,China, Elsevier B.V 2011.