International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-3)

Research Article | **March 2014**

An Enhanced Anti-Phishing Framework Based on Visual Cryptography

Gaurav Palande, Shekhar Jadhav, Ashutosh Malwade, Vishal Divekar, Prof. S. Baj
Department of Computer Engineering,
Dr. D. Y. Patil College of Engineering,
Pune-410506, India

Abstract —

With the evolution in the world of internet, it has become prone to several online attacks and the most common attack is phishing. Phishing is an act of fraudulently acquiring confidential and sensitive information about the user, such as banking password or credit card number, by pretending to be a trustworthy entity. Victims are tricked into providing such information by a combination of spoofing techniques and social engineering. In this paper we have proposed a new technique named as "An Enhanced Anti-Phishing Framework Based on Visual Cryptography". In this paper an image based authentication using Visual Cryptography is implemented. Our proposed methodology uses visual cryptography to preserve the privacy of the randomly chosen image by decomposing the image into two shares. These two shares are for that particular session. The trusted server stores unique keys for the users required for decryption of the share. The original image is obtained at the user end only when both the user and the server under test are registered with the trusted server. Using this method the user can determine whether the site is safe or unsafe to carry out his transaction.

Keywords*— *Phishing, Shares, Visual Cryptography, Encryption, Decryption, Security

I. INTRODUCTION

Phishing is similar to fishing in a lake, but instead of trying to capture fish, phishers attempt to steal your personal information. The act of sending email that falsely claims to be from a legitimate organization or websites such as eBay, Flipkart, or other banking institutions. This is usually combined with a threat or request for information: for example, that an account will close, a balance is due, or information is missing from an account. The email will ask the recipient to supply confidential information, such as bank account details, PINs or passwords; these details are then used by the owners of the website to conduct fraud. Some e-mails will ask that you enter even more information, such as your full name, address, phone number, social security number, and credit card number. However, even if you visit the false website and just enter your username and password, the phisher may be able to gain access to more information by just logging in to you account.

Phishing is a con game that scammers use to collect personal information from unsuspecting users. The false e-mails often look surprisingly legitimate and even the Web pages where you are asked to enter your information may look real.

So here we introduce a new and secure method which can be used to prevent phishing attacks which is named as "An Enhanced Anti-phishing Framework Based on Visual Cryptography". In this method, we provide a provision to the user to check whether the website he is willing to visit is a genuine website or a phishing website. So, by knowing these he can securely perform his further proceedings or transactions. Here, we used the concept of an improved visual cryptography. Visual Cryptography (VC) is used here to divide the image into shares and in order to reveal the original image appropriate number of shares should be combined.

A. *Visual Cryptography*

Visual cryptography schemes were independently introduced by Shamir [4] and Blakley [5], and their original motivation was to safeguard cryptographic keys from loss. These schemes also have been widely employed in the construction of several types of cryptographic protocols [6] and consequently, they have many applications in different areas such as access control, opening a bank vault, opening a safety deposit box, or even launching of missiles. A segment-based visual cryptography suggested by Borchert [7] can be used only to encrypt the messages containing symbols, especially numbers like bank account number, amount etc. The VCS proposed by Wei-Qi Yan et al.,[8] can be applied only for printed text or image. Naor and Shamir introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations.

Most of the previous research work on VC focused on improving two parameters: pixel expansion and contrast [11], [12], [13]. In these cases all participants who hold shares are assumed to be honest, that is, they will not present false or fake shares during the phase of recovering the secret image. Thus, the image shown on the stacking of shares is considered as the real secrete image. But, this may not be true always. So cheating prevention methodologies are introduced by Yan et al.,[14], Horng et al.,[15] and Hu et al.,[16]. But, it is observed in all these methodologies, there is no facility of authentication testing.

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. 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.

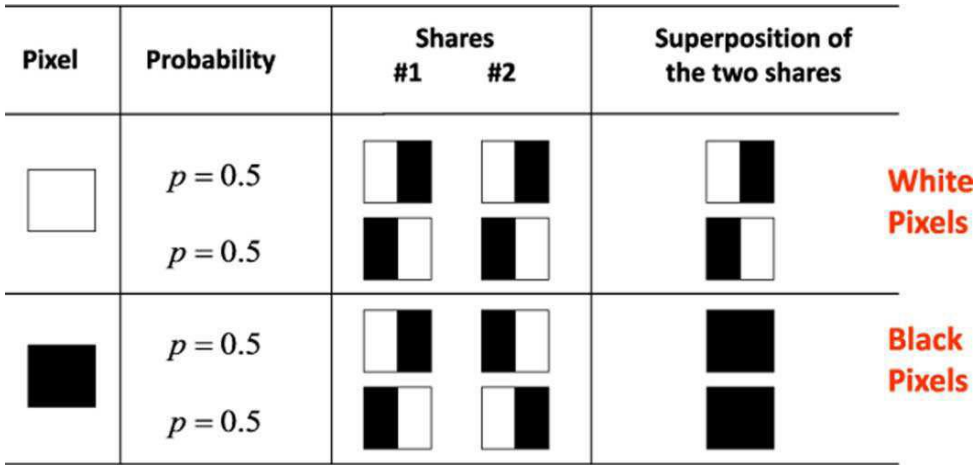

Fig.1 Illustration of 2-out-of-2 VCS scheme with 2 sub pixel construction

II. CURRENT METHODOLOGY

In the current scenario as shown in the Fig. 2, when the end user wants to access his confidential information online (in the form of money transfer or payment gateway) by logging into his bank account or secure mail account, the person enters information like username, password, credit card no. etc. on the login page. But quite often, this information can be captured by attackers using phishing techniques (for instance, a phishing website can collect the login information the user enters and redirect him to the original site). There is no such information that cannot be directly obtained from the user at the time of his login input.

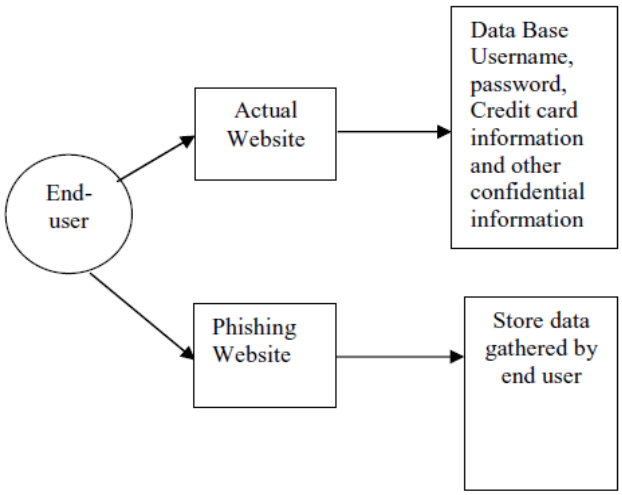

Fig.2 Current Scenario

III. PROPOSED METHODOLOGY

For the purpose of detecting and preventing phishing, we are proposing new methodology to identify a phishing website. Our proposed anti-phishing framework is as shown in the figure 3. As per our methodology first of all the user gets registered with the trusted server. At the time of registration a unique key is generated by the administrator application. This unique key is stored in the database at the trusted server. Once the user is successfully registered with the trusted server he then can login through the client application using the username and password. For a particular session the user can select a random image for the purpose of verifying the server under test. Using the client application the user performs cryptography over the randomly chosen image to generate two shares. After encryption one of the shares is forwarded to the server under test. The server under test then forwards this share along with its server name and password to get the share decrypted from the trusted server. The trusted server then decrypts the share using the unique key stored in its database. The trusted server sends the decrypted share to the server under test if and only if the server under test is registered with the trusted server. The server under test on receiving the decrypted version of the share sends it to the client. The client after receiving decrypted share from server under test performs decryptography to obtain the original image. If original image is obtained then the server under test is a legitimate server otherwise close the session. Original image is obtained if and only if both user and the server under test are registered with the trusted server. If either of the user or server under test is not registered with the trusted server then an improper image is obtained.

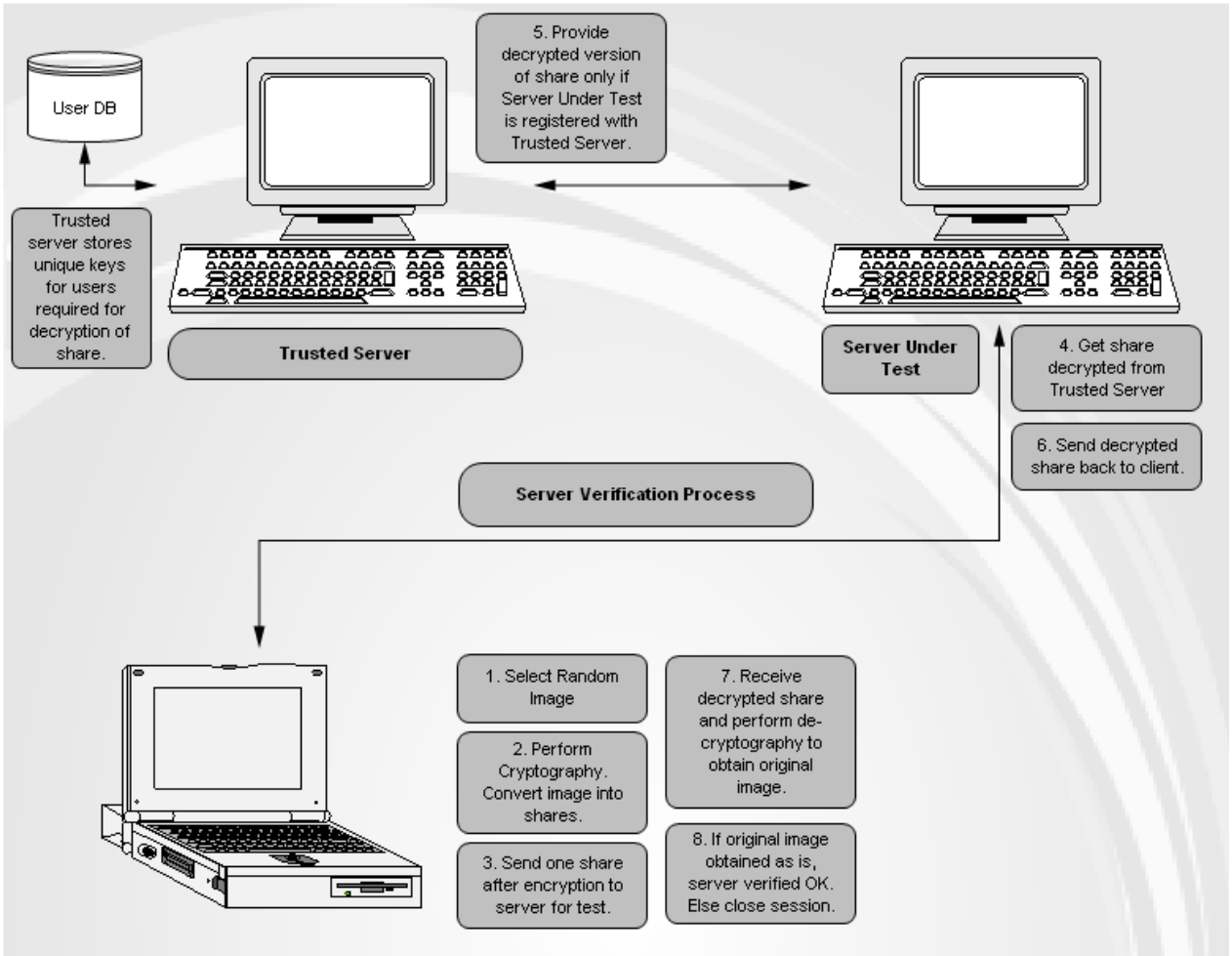

Fig.3 Proposed Methodology

IV. CONCLUSIONS

Nowadays due to increase in number of online transactions phishing attacks are becoming common to acquire the user's confidential information. The attackers use this information in the phishing attacks. With our proposed methodology "An Enhanced Anti-Phishing Framework Based on Visual Cryptography" we can easily identify the phishing websites. Our proposed technique provides more security as a random image is chosen for a particular session and both the encryption and decryption is done with the unique key that is generated at the time of user registration. Since the generated shares are valid for a particular session and are not stored on either side i.e. server or user there is no chance of the share getting stolen by any other user. Hence it provides much better security.

REFERENCES

[1] Divya James.; Mintu Philip.;"A Novel Anti Phishing framework based on Visual Cryptography", in Proceedings of Power, Signals, Controls and Computation (EPSCICON), 2012.
[2] Ollmann G., The Phishing Guide Understanding & Preventing Phishing Attacks, NGS Software Insight Security Research.
[3] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT,1994, pp. 1–12.
[4] A. Shamir, .How to Share a Secret,. Communication ACM, vol. 22, 1979, pp. 612-613.
[5] G. R. Blakley, .Safeguarding Cryptographic Keys,. Proceedings of AFIPS Conference, vol. 48, 1970, pp. 313-317.
[6] A. Menezes, P. Van Oorschot and S. Vanstone, .Handbook of Applied Cryptography,. CRC Press, Boca Raton, FL, 1997.
[7] B. Borchert, .Segment Based Visual Cryptography,. WSI Press, Germany, 2007.
[8] W-Q Yan, D. Jin and M. S. Kanakanahalli, .Visual Cryptography for Print and Scan Applications,. IEEE Transactions, ISCAS-2004, pp.572-575.
[9] T. Monoth and A. P. Babu, .Recursive Visual Cryptography Using Random Basis Column Pixel Expansion,. in Proceedings of IEEEInternational Conference on Information Technology, 2007, pp. 41-43.
[10] H. J. Kim, V. Sachnev, S. J. Choi and S. Xiang, .An Innocuous Visual Cryptography Scheme,. in Proceedings of IEEE-8th International Workshop on Image Analysis for Multimedia Interactive Services, 2007.
[11] C. Blundo and A. De Santis, .On the contrast in Visual Cryptography Schemes,. in Journal on Cryptography, vol. 12, 1999, pp. 261-289.
[12] 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.
[13] 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.
[14] H. Yan, Z. Gan and K. Chen, .A Cheater Detectable Visual Cryptography Scheme,. *Journal of Shanghai Jiaotong University*, vol. 38, no. 1,2004.
[15] G. B. Horng, T. G. Chen and D. S. Tsai, .Cheating in Visual Cryptography,. *Designs, Codes, Cryptography*, vol. 38, no. 2, 2006, pp. 219-236.
[16] 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.