International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161
©2014 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

Review Article

# Malicious Website Detection using Visual Cryptography and OTP

Kajal Nanaware[Å], Kirti Kanade[Å], Manisha Bhat[Å*], Reshma Patil[Å] and A.S. Deokar[Å]

[Å]Department of Computer Engineering, Savitribai Phule Pune University, Pune, Maharashtra, India

Accepted 10 Sept 2014, Available online 01 Oct 2014, **Vol.4, No.5 (Oct 2014)**

***Abstract***

*With the advent of internet, various online attacks have been increased and among them, the most popular attack is phishing. Phishing is an attempt by an individual or a group to get personal confidential information such as passwords, credit information from unsuspecting victims for identity theft, financial gain and other fraudulent activities, by pretending to be a trustworthy entity. Victims are tricked into providing such information by a combination of spoofing techniques and social engineering. Fake websites which appear very similar to the original ones are being hosted to achieve this. In this paper we have proposed a new approach named as "Malicious Website Detection using Visual Cryptography and OTP" to solve the problem of phishing. Here an image based authentication using Visual Cryptography is implemented with the combination of OTP (One Time Password). The use of visual cryptography is explored to preserve the privacy of an image captcha by decomposing the original image captcha into two shares. 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, website cross verifies its identity and proves that it is a genuine website before the end users.*

***Keywords:*** *Phishing, visual cryptography, image captcha, shares, OTP.*

## 1. Introduction

Phishing is similar to fishing in a lake, but instead of trying to capture fish, phishers attempt to steal your personal information. It can be an 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 your account.

Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging. Phishing (Ollmann G, 2004) is a continual threat that keeps growing to this day. The risk grows even larger in social media such as Facebook, Twitter, Myspace etc. Hackers commonly use these sites to attack persons using these media sites in their workplace, homes, or public in order to take personal and security information that can affect the user and the company (if in a workplace environment). Phishing (Xiaoqing GU *et al*, 2013) is used to portray trust in the user since you can usually not tell that the site or program being visited/ used is not real, and when this occurs, is when the hacker has the chance to access the personal information such as passwords, usernames, security codes, and credit card numbers among other things.

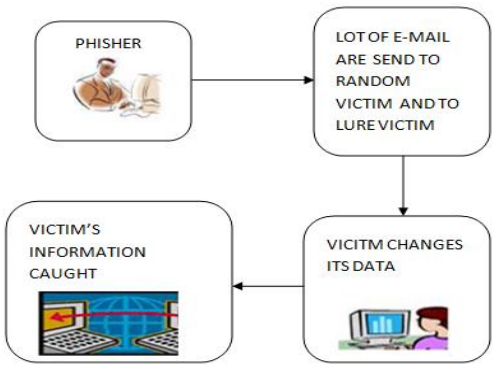


**Fig.1** Phishing Process

So here, we introduce a new method which can be used as a safe way against phishing which is named as "Malicious Website Detection using Visual Cryptography and OTP". As the name describes, in this approach, website cross

*Corresponding author: **Manisha Bhat**

verifies its own identity and proves that it is a genuine website (to use bank transaction, E-commerce and online booking system etc.) before the end users and make the both the sides of the system secure as well as an authenticated one. The concept of OTP is used for the purpose of randomness and time-out session which strengthens the security. This OTP is constructed into an image. 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.

## 2. Visual Cryptography

One of the best known techniques to protect data is cryptography. It is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Naor and Shamir (Naor *et al*, 1994) introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations.

Visual cryptography schemes were independently introduced by Shamir (A. Shamir, 1979) and Blakley (G.R.Blakley, 1970), 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 (A. Menezes *et al*, 1997) 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 (B. Borchert, 2007) 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 (W-Q Yan *et al*, 2004) 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 (C. Blundo *et al*, 1999; P. A. Eisen *et al*, 2002; E. R. Verheul *et al*, 1997). 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 secret image. But, this may not be true always. So, cheating prevention methodologies are introduced by Yan (H.Yan *et al*, 2004), Horng (G.B.Horng *et al*, 2006) and Hu (C. M. Hu *et al*, 2007). But, it is observed in all these methodologies, there is no facility of authentication testing.

There are basic terms provided before defining VCS model.

1**)** Secret image: The private image that we want to hide.

2**)** Hosts: These are facing image that are used hide the original image using GEVCS

3**)** Sheets: The original image encrypted in to n sheets

4) Target: The original image is reconstructed by combining the sheets.

Visual Cryptography Scheme is a cryptographic technique that allows for the encryption of visual information such that the 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. No additional information is required to create this kind of access structure.
- (2,n) Threshold VCS 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.
- (n,n) Threshold VCS scheme:-This scheme encrypts the secret image to n shares such that when all n of the shares are combined, then only the secret image will be revealed. The user will be prompted for n, the number of participants.
- (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. The user will be prompted for k, the Threshold and n, the number of participants.

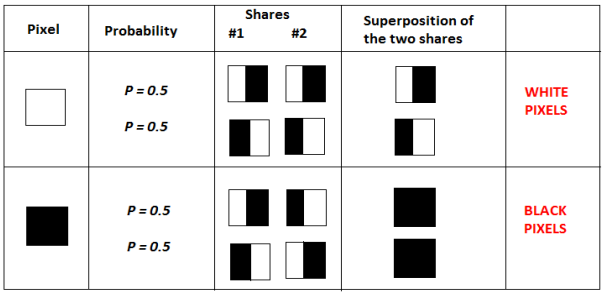


**Fig. 2**Illustration of a 2-out-of-2 VCS scheme with 2 sub pixel construction

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Fig. 2 denotes the shares of a white pixel and a black pixel. Note that the choice of shares for a white and a 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.

## 3. OTP (One Time Password)

A one-time password (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages

to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. On the downside, OTPs need to be delivered to the user as and when generated.

OTP (Himika Parmar *et al*, 2012) generation algorithms typically make use of pseudo-randomness or randomness. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details. Various approaches for the generation of OTPs are listed below:

- Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time).
- Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order)
- Using a mathematical algorithm where the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and/or a counter.

There are also different ways to make the user aware of the next OTP to use. Some systems use special electronic security tokens that the user carries and that generate OTPs and show them using a small display. Other systems consist of software that runs on the user's mobile phone. Yet other systems generate OTPs on the server-side and send them to the user using an out-of-band channel such as SMS messaging or e-mails. Our technology uses the e-mail approach.

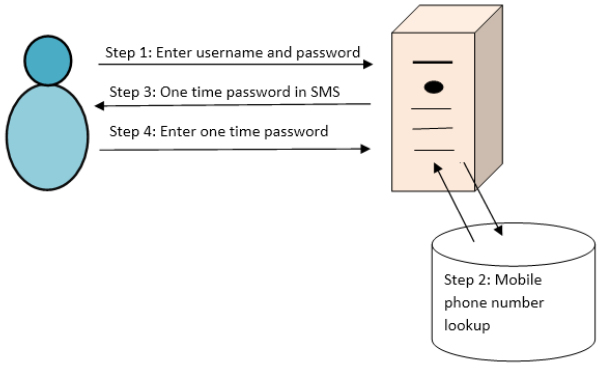


**Fig. 3** Two phase-two factor OTP generation


**Fig. 4** One time password example.

## 4. Current Methodology

In the current scenario as shown in the Fig. 5, 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.

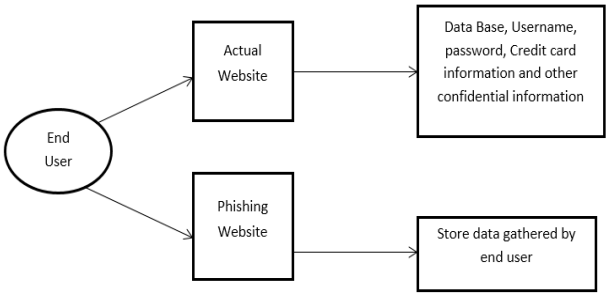


**Fig. 5** Current Scenario

## 5. 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 Fig. 6. As per our methodology, first of all, the user gets registered with the trusted server (mostly, a bank server). The user gets his UID at the time of registration. Once the user is successfully registered with the trusted server, he can login through the client application. For the verification, he sends his UID to the merchant server. The merchant server sends the server ID, server key and UID to the bank server. The bank server validates these items respectively. If the given information is registered under the bank server i.e if the details provided by the merchant server are valid, then the bank server generates an OTP. This OTP is constructed into an image.

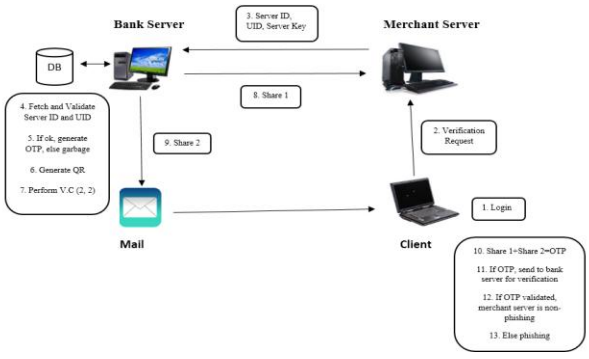


**Fig. 6** Proposed Methodology

Then (2,2) Threshold VCS scheme is applied on the image. Share 1 is sent to the merchant server and share 2 is

sent to the user via e-mail. Merchant server sends share 1 to the user for the verification process. At the user side, share 1 and share 2 are merged together to get the image. From this image, user can get the OTP. The user then enters this OTP and validates it with the bank server through the merchant server. If the OTP is valid, the merchant server is authenticated one. Otherwise, the merchant server is a phishing.

## Conclusion

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 "Malicious Website Detection using Visual Cryptography and OTP", we can easily identify the phishing websites. Our proposed technique provides more security as a random OTP is chosen for a particular session and the visual cryptography is done on the authenticated server side. 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

Divya James and Mintu Philip (2012), A Novel Anti Phishing framework based on Visual Cryptography, *IJDPS, 3*

Ollmann G (2004), The Phishing Guide-Understanding & Preventing Phishing Attacks, *NGS Software Insight Security Research*.

Xiaoqing GU, Hongyuan WANG and Tongguang NI (2013), An Efficient Approach to Detecting Phishing Web, *Journal of Computational Information Systems*, 9:14, 5553–5560.

M. Naor and A. Shamir (1994), Visual cryptography, *Proc. EUROCRYPT*, pp. 1–12.

A. Shamir (1979), How to Share a Secret, *Communication ACM*, 22, 612-613.

G. R. Blakley (1970), Safeguarding Cryptographic Keys, *Proceedings of AFIPS Conference*, 48, 313-317.

A. Menezes, P. Van Oorschot and S. Vanstone (1997), Handbook of Applied Cryptography, *CRC Press, Boca Raton, FL*, June 03-06, 208-223.

B. Borchert (2007), Segment Based Visual Cryptography, *WSI Press, Germany*.

W-Q Yan, D. Jin and M. S. Kanakanahalli, (2004), Visual Cryptography for Print and Scan Applications, *IEEE Transactions, ISCAS*, pp.572-575.

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

P. A. Eisen and D. R. Stinson (2002), Threshold Visual Cryptography with specified Whiteness-Levels of Reconstructed Pixels, *Designs, Codes, Cryptography*, vol. 25, pp. 15-61.

E. R. Verheul and H. C. A. Van Tilborg (1997), Constructions and Properties of k out of n Visual Secret Sharing Schemes, *Designs, Codes, Cryptography*, vol. 11, no. 2, pp. 179-196.

H. Yan, Z. Gan and K. Chen (2004), A Cheater Detectable Visual Cryptography Scheme, *Journal of Shanghai Jiaotong University*, vol. 38.

G. B. Horng, T. G. Chen and D. S. Tsai (2006), Cheating in Visual Cryptography, *Designs, Codes, Cryptography*, vol. 38, no. 2, pp. 219-236.

C. M. Hu and W. G. Tzeng (2007), Cheating Prevention in Visual Cryptography,. *IEEE Transaction on Image Processing*, vol. 16, no. 1, pp. 36-45.

Himika Parmar, Nancy Nainan and Sumaiya Thaseen (2012), Generation of Secure One-Time Password Based On Image Authentication, *CS & IT-CSCP*, 07, 195-206.