International Journal of Current Engineering and Technology ISSN 2277 – 4106

Available at http://inpressco.com/category/ijcet

Research Article

Online Polling System Based on Visual Cryptography

Jayalaxmi M[a*] and V.R.Udupi[b]

[a]Computer Science Engg, VTU University, Belgaum
[b]G.I.T(E&C,Hod), Belgaum

Abstract

Now a days only few people go for voting because of their tight schedule. There are many reasons, few may be everyone has to go to voting center, we have to stand in a long queue, many may be tired because of their tight schedule. So we have developed online voting system. But this system has some disadvantage. Phishing attackers directly get the passwords from the user and they enter into the relevant web sites with correct password. Consider an online polling system for corporate companies, polling is happening once in a year to elect the president or secretary or key directors of the company. At present system all the votes are has to assemble at one place on polling day and put their vote. In this approach we are making use of a new scheme which is known as Visual cryptography. In this scheme we are making use of visual information for security. Here we are dividing original image into two shares which are stored in separate database. Whenever these two shares are stacked with each other we get the original image. Once we get the original image it can be used as password. This system is very useful and safe for online remote voting. This system is web based application so that it can be accessed by any authorized person anywhere in the world through internet.

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

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 mechanisms should also be so effective. Thus the security in these cases be very high and should not be easily tractable with implementation easiness. Today, most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, their detection is a difficult problem.

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. One definition of phishing is given as it is a criminal activity using social engineering techniques. Visual Cryptography (VC) is a method of encrypting a secret image into shares, such that stacking a sufficient number of shares reveals the secret image. This paper is organized as follows: Section II deals with the related work using Visual Cryptography and Section III & IV presents the current and proposed Methodologies. Section V presents the implementation and Section VI deals with Results. Section VII contains the conclusion.

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 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 Scheme is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. In the case of (2, 2) VCS, each pixel P in the original imageis encrypted into two sub pixels called shares. Fig.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 shares provide 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 subpixel.

*Corresponding author: **Jayalaxmi M**

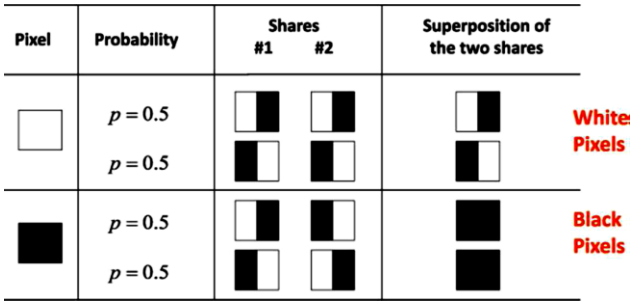

Fig. 1 Illustration of a 2-out-of-2 VCS scheme with 2 subpixel construction.

3. 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.

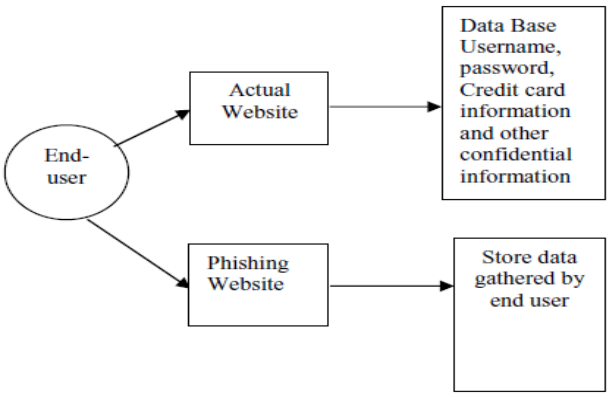

Fig.2 Current scenario

4. Proposed methodology

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. The proposed approach can be divided into two phases

A. Registration Phase
B. Login Phase

A. *Registration Phase*

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 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. After the registration, the user can change thekey string when it is needed. Registration process is depicted in Fig.3.

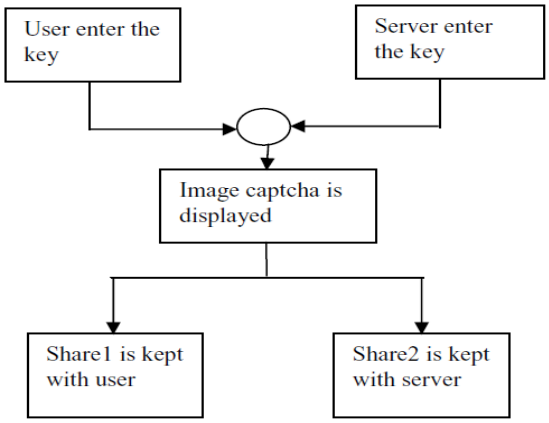

Fig.3 When user performs registration process for the website

B. Login Phase

When the user logs in by entering his confidential information for using his account, then first the user is asked to enter his 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. This phase is depicted in Fig.4.

4. Implementation & analysis

The proposed methodology is implemented using Matlab. Fig 5, Shows the result of creation and stacking of shares. In the registration phase the most important part is the creation of shares from the image captcha where one share is kept with the user and other share can be kept with the server. For login, the user needs to enter a valid username

in the given field. Then he has to browse his share and process. At the server side the user's share is combined with the share in the server and an image captcha is generated. The user has to enter the text from the image captcha in the required field in order to log in into the website. The entire process is depicted in Fig.5 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.

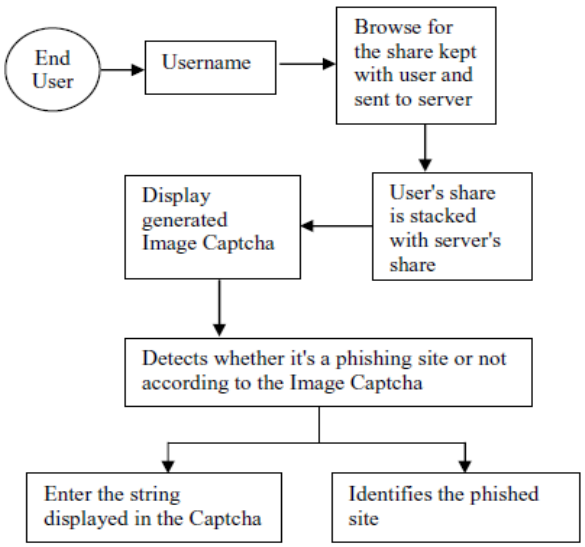

Fig.4 When user attempts to log in into site

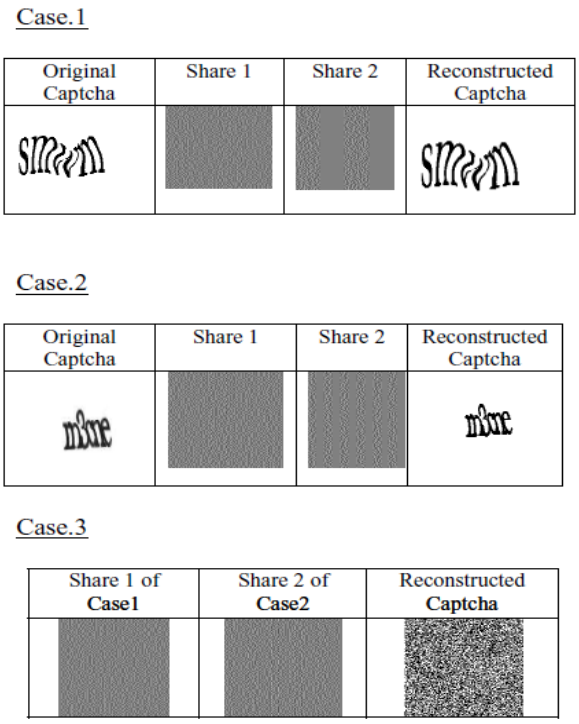

Fig.5 Creation and stacking of shares

6. Result

This system is very useful and safe for online remote voting. This system is web based application so that it can be accessed by any authorized person anywhere in the world through internet.

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 using 3 layers of security. 1st layer 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. Second layer cross validates image Captcha corresponding to the user. The image Captcha is readable by human users alone and not by machine users. Only human users accessing the website can read the image Captcha and ensure that the site as well as the user is permitted one or not. So, using image Captcha technique, no machine based user can crack the password or other confidential information of the users.And as a third layer of security it prevents intruders' attacks on the user's account. This method provides additional security in terms of not letting the intruder log in into the account even when the user knows the username of a particular user. The proposed methodology is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market.

References

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

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

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

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

A. Menezes, P. Van Oorschot and S. Vanstone (1997), .Handbook of Applied Cryptography,. *CRC Press, Boca Raton*, FL, 1997.