ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Detecting Phishing Websites Based on Visual Cryptography

Ambre Reshma[1], Fugare Saroj[2], Revagade Ranjana[3] ,Wakchuare Priyanka[4] , Deshmukh S.C. [5]

***Abstract*—Most of the time people using internet for online transactions from one place to another place. The security in this case should be very high and should not be easily traceable to attacker. Attacker may attack on system online or offline. In this types of various attacks, phishing (meaning is- knowing users details through fake sites) is identified as a major security threat and each second new ideas comes into place to attack users account online, soprevention mechanism should be very strong. In Phishing process individual or a group of thefts used to steal person's confidential information such as passwords, credit card information, banking details etc.for making frauds. In this project, new approach is defined named as "A Novel Anti-phishing framework based on visual cryptography" to solve phishing based problems. In project, an image based authentication using Visual Cryptography (VC) is used. The privacy of image captcha is preserve by the use of visual cryptography by extracting the original image captcha into two shares that are stored in separate database servers such that the original image captcha can be identified only when both are simultaneously available.**

***Keywords*— Phishing, Visual Cryptography, Image Captcha, Shares, Security.**

I. INTRODUCTION

Most online applications use various types of securities. Since, the design and technology of has improved rapidly, hacking and cracking techniques also improved in same range. As a result, it is nearly impossible to make sure whether a computer that is connected to the internet canbe trustworthy and secure. Phishing scams is become a problem for online banking and e-commerce users. Big question is how to prevent e transaction applications online from Phishes. Phishes means the online theft that aims to steal sensitive information such as online Banking passwords and credit card information from users. Another meaning of phishing states that it is "the act of sending an email to a user claiming that they have won $100000000 prize something or of any kind of fake advertising mails, so that to get users after clicking on it may indirectly give his personal information to fraud users(theft)".

So in our project we introduce a new concept which can be used as a safe way against phishing which is named as "A novel approach against Anti-phishing using visual cryptography". In this methodology, website we can check side by side verifies its own identity and proves that it is a true website before the end users and makes sure that both user and server sides are authenticated one. The technique of both image processing and an improved visual cryptography is used in our project. Image Processing is a technique of processing an input image and to get the output as either improved form of the same image. In Visual Cryptography (VC)an image captcha is decomposed into shares and stores separately in server database, so after login by user, that image captcha should get match with its content behind image. After both user and server side captcha's get matched, the user can log in into the website very securely.

II. RELATED WORKS

Phishing web pages are forged web pages that are created by malicious people to mimic Web pages of original web sites. M These types of web pages have high visual similarities to scam their casualty's. Such types of web pages stare absolutely like the actual a solitary. Casualties of fraud web pages may expose their personal account, secure word, positive identification number, or other data to the phishing web page holders. It includes methods such as defraud the customers through email and unsolicited mail, fitting of key loggers. Electronic mails are mostly use techniques for phishing, due to its simplicity, ease of use and wide reach. Phishes can deliver specially crafted emails to millions of legitimate email addresses very quickly and can fool the recipients utilising well

ISSN: 2321-9653

known imperfection in the Synchronous Mail Transfer Protocol. Methods like adenovirus extension to electronic mails, crafting of 'personalised' or unique email messages are also often. Investigator proposes customer-based mechanisms to authenticate the server. Automated Challenge Response Method is one such authentication mechanisms includes challenge generation module from server which in turn interacts with Challenge-Response interface in client and request for response from user. Here instead of getting response from get-response executable it is better to update the get-response executable automatically from bank server when the responses are about to negate. Now there are Domain Name System based anti-phishing resemble technique which mainly includes blacklists, heuristic detection, the page similarity assessment. But they do have some short comings. Blacklist is a DNS based anti-phishing approach technique now most commonly used by the browser. Anti Phishing Work Group, Google and other organizations have provided an open blacklist enquiry interface. Internet Explorer 7, Netscape Browser 8.1, Google Safe Browsing (a feature of the Google Toolbar for Firefox) are important browsers which use blacklists to protect users when they are navigating through phishing sites. Because administrator has verified every URL in the blacklist, the fault reminder possibility is very low. Although, there are a plenty of technical drawbacks. Initially, the fraud websites we found is a very minor percentage, so the failed reminder possibility is very big. Furthermore, commonly to say, the life revolution of a fraud website is not many days. A website might be shut down before we found and verified it is a fraud website. Heuristic-based anti-phishing technique is to estimate whether a page has some phishing fact-finding features. For example, some fraud-finding features used by the Spoof Guard [3] toolbar include checking the host name, checking the Uniform Resource Locator for common spoofing techniques, and checking against before watch images. While you only use the Heuristic-based technique, the perfection is not sufficient. Alongside, frailer can use some policies to circumvent such detection rules. The user may be defraud by the fraud website because the phishing website imitates a legitimate website. Its pages are often similar with the legitimate sites. For example, CANTINA is a content similarity based approach to detect phishing websites [6]. These favored technologies have several downsides:

1. Blacklist-based technique with low false reminder possibility, but it cannot diagnose the websites that are not in the blacklist database. Because the life revolution of fraud websites is too short and the establishment of blacklist has a lengthy delay time, the correctness of blacklist is low.
2. Heuristic-based anti-phishing technique, with a high possibility of false and failed reminder, and it is not difficult for the attacker to use technical means to avoid the heuristic features diagnose.
3. Similarity assessment based technique is time-swallowing. It needs too more time to deliberate a couple of pages, so using the method to diagnose fraud websites on the client terminal is not fitting. And there is low correctness rate for this method depends on many factors, such as the word, photographs, and equivalence measurement technique. However, this technique is not perfect enough yet.

1. 0ne time password: - If user forgot his/her password then user create new password using OLTP technique.
2. Using visual cryptography scheme we divide image into six shares because of these when any share get crash or lost from other, we recover the original image.

III. PHASES OF SYSTEM

A. *Registration Phase:*

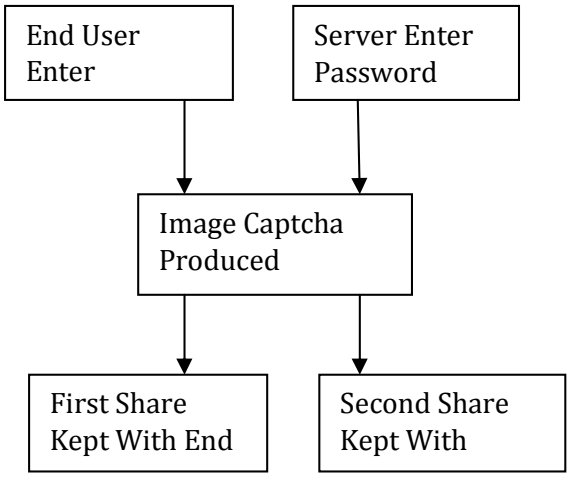


Fig 1: Registration Phase

In registration phase, user enter password at the time of registration for secure website. The password is combination of numbers and alphabets. The password joining with the randomly generated password in the server side and image captcha produced. The image captcha distinct into two shares one share kept with user & other share kept with server. The user's share & initial image

ISSN: 2321-9653

Captcha is sent to the user during login phases. The image captcha stocked in the real database of secure websites. After registration user can modify the password when it is needed [6].

B. *Login Phase*

In this phase's user id then user entered share which is kept with him. User Share send to the server the user share and server share are combined together. The image captcha seen to the user .Here user can test seen image Captcha match with Captcha created at the time of registration. User enters the text seen in the image captcha this text can used for password purpose and user can login to website.Using user id Image captcha produced by combining two shares one can verify whether the website is secure website [6].

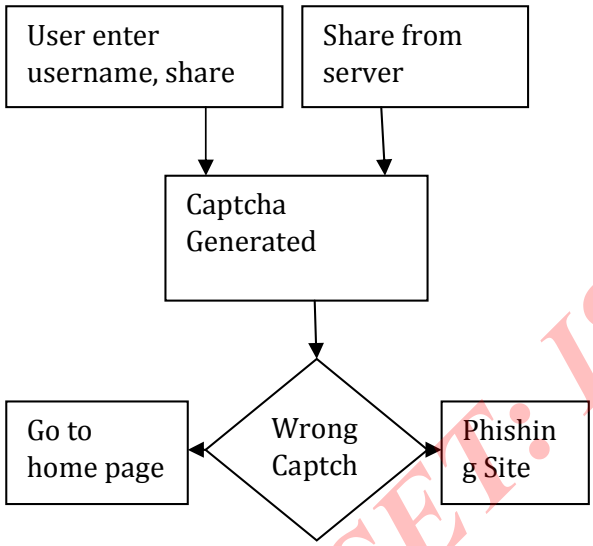


Fig 2: Login Phase

IV. VISUAL CRYPTOGRAPHY SCHEME

VC scheme is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual structure. We can accomplish this information by following scheme.

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 overlap. No extra information is needed to create this kind of access structure.

2. (2,i) Threshold VCS scheme-This scheme encrypts the secret image into i shares such that when any two(or more) of the shares are overlaid the secret image is disclosed. The user will be prompted for i, the number of participants.

3. (i,i) Threshold VCS scheme-This scheme encrypts the secret image to i shares such that when all i of the shares are combined will the secret image be disclosed. The user will be prompted for i, the number of participants.

4.(k,i) Threshold VCS scheme- This scheme encrypts the secret image to i shares such that when any group of at least k shares are overlaid the secret image will be disclosed. The user will be prompted for k, the Threshold,, and i, the number of participants.

In that case (2, 2) VCS, each pixel P in the real image is encrypted into two sub pixels called shares. Figure show the shares of a white pixel and a black pixel. Neither share provides any clue about the original pixel since different pixels in the genuine image will be encrypted using independent random choices. When the two shares are superimposed, the value of the real pixel value of p found. The p black pixel then we gets two black sub pixels and if p is white pixel, we get black sub pixel and another is white sub pixel [6].

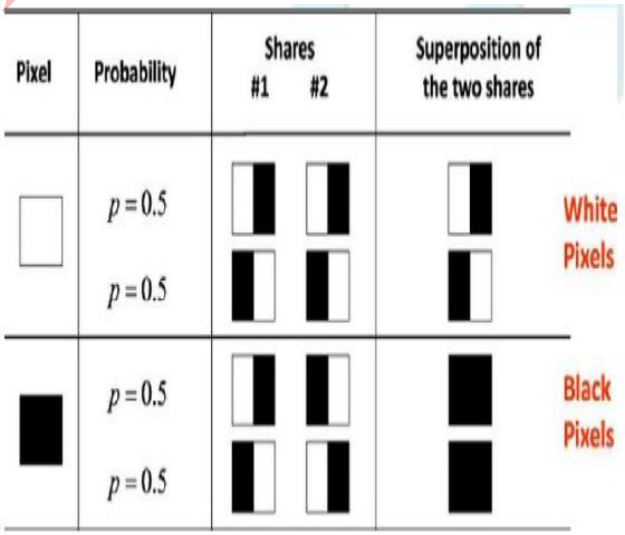


Fig. 3: VCS scheme with 2 sub pixel construction.

V. OUR APPROACH TO DETECTING PHISHING WEBSITE

ISSN: 2321-9653

Architecture

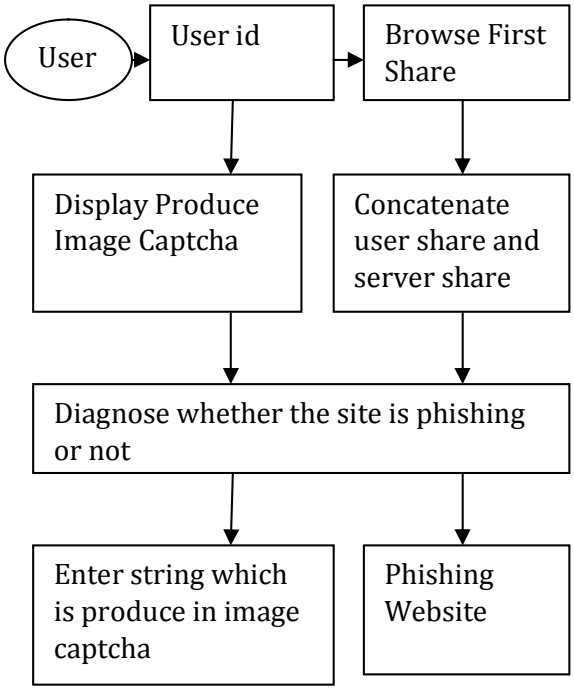


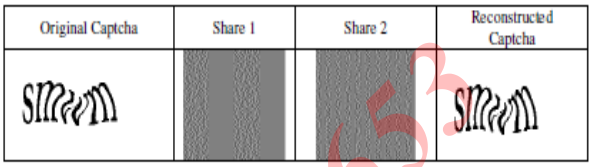
Fig 4: User log into website

In this methodology, end user enter user name user id and user browse for the share which is kept with user and send to the server. User's share is stacked with server share and image captcha generated. Detect whether websites is phishing site or not according to image captcha. If image captcha matches with captcha generated at time of registration then user is human user and user enter the string displayed image captcha. Else Image captcha is not matches with captcha generated then at time of registration indentify phishing site[6].

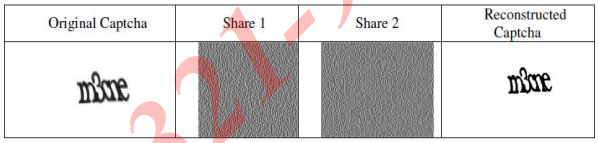
VI. IMPLEMENTATION & ANALYSIS

In the registration phase the weightiest portion is the make of shares from the image captcha .where one share is kept with the user and other share can be kept with the server side. For login phase, the user needs to enter a correct username in the given text field. Then he has to browse his share and process. At the server side the user's share is joined 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 login into the website. The entire process is depicted in Figure.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 is combined with share2 of second captcha resulting in unrecognizable form of Captcha [6].

Case 1:



Case 2:



Case 3:

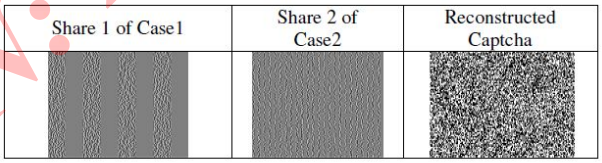


Figure 4: Creation and concatenation of shares

It is observed that both original and reconstructed image captcha's are related with high degree of correlation. The correlation coefficient of original captcha and reconstructed captcha are shown in Table 1.Also when two different shares are stacked their corresponding correlation coefficient is obtained as -0.0073.This shows that there will be zero degree of correlation between original and output images for two different shares [6].

Original Captcha	Reconstructed Captcha	Correlation Coefficient
		0.9679
		0.9598
		0.9627
		0.9578
		0.9657

VII. FUTURE WORK

1. This technology is not only use in banking sector but also use in military sector for detecting phishing websites
2. We will divide user confidential information onto the five servers so it provides more security.
3. If user forgot his/her password so to create new password we use new method such as one time password.
4. We use new technique such as admin authentication

VIII. CONCLUSION

Our methodology "Antiphishing framework based on visual cryptography" preserves secure information of users using three layers of security. First layer verifies whether website is secure website or not. In second layer check validated image captcha .Only human user acquire the website can read image Captcha. In third layer of security to prevent attacks from unauthorized user in user account.

REFERENCES

[1] Mrs.A.Angel Freda, M.Sindhuja, K.Sujitha, IJREAT, Image Captcha based Authentication using visual cryptography vol.1, pp.2320-8791, April-May, 2013.

[2] Anthony Y. Fu, Liu Wenyin, "Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Moverâ Distance (EMD)",IEEE Transactions on Dependable and Secure Computing, vol.3, pp.301-311, October/December 2006.

[3] JungMin Kang, DoHoon Lee,IEEE, "Advanced White List Approach for Preventing Access to Phishing Sites", pp.491-496, 2007.

[4] Wenyin Liu, Xiaotie Deng, Guanglin Huang, and Anthony Y. Fu,IEEE Internet Computing "An Antiphishing Strategy Based on Visual Similarity Assessment", vol.10, p 58-65, March/April 2006..

[5] Haijun Zhang, Gang Liu, and TommyW. S. Chow, IEEE Trans. "Neural Netw, Textual and Visual Content-Based Anti-Phishing: A Bayesian Approach", IEEE Trans. Neural Netw., vol.22, no. 10, pp.15321546, Oct.2011.

[6] Divya James1 and Mintu Phillip2,"A novel anti phishing framework based on visual cryptography", vol.3, no...1. pp.1264-3459, January.