An Anti-phishing Framework Based on Visual Cryptography

Bushra Siddique[1], Upendra Malekar[2], Mohini Kashyap[3]

[1]Student, Dept. of CSE, Ballarpur Institute of Technology, MS, India
[2]Assistant Professor, Dept. of CSE, Ballarpur Institute of Technology, MS, India
[3]Student, Dept. of CSE, Ballarpur Institute of Technology, MS, India

Abstract - *Due to immense use of internet, online attack has increased. Among that, phishing attack is the most common one. Phishing is an act carried by an individual or a group to access personal information such as credit card details, passwords etc for financial gain and other fraudulent activities. Thus, a new method is proposed named as "An Antipishing framework based on visual cryptography" to solve phishing issues. In this paper, an image based authentication using visual cryptography (VC) is used. The use of visual cryptography is to preserve the privacy of an image captcha by decomposing the original image captcha into two sheets that are stored in separate database servers. The original image captcha can be revealed only when both are simultaneously available. Once the original image captcha is revealed to its user, it can be used as the password. Using this, websites can cross verify it and proves its identity.*

***Key Words*: Image captcha, shares, visual cryptography, security, phishing.**

1. INTRODUCTION

In today's world, online transactions are very common and some leads to various online attacks. In this, the major security threat is the phishing attack and thus innovative ideas are coming with this every second. So, for this the preventive measurement should also be developed in a very effective manner. Therefore, the security for this should not be traceable easily.

Now-a-days, majority of the applications is as secure as underlying system. As a result, it is not possible to be confident that the computer that is connected with the internet is a secure one or not. Phishing attack is also creating problems for e-commerce and online banking users. So, how to tackle with the application that needs high security.

The main goal of the phished is to hack information such as credit card information, passwords etc from the users. Phishing is a form of fraud in which the attacker tries to learn information such as login or account information by masquerading as a reputable entity, IM or other communication channels. Another definition of phishing is given as the criminal activity done using social engineering.

The phishing done on the website is same as the fishing done in a lake, but in this phishing instead of stealing the fish the phisher steals the personal information of the users to commit crime. Thus, to overcome all this factors we are giving a technique to prevent phishing using visual cryptography.

In this technique, a concept called image processing is used. Here, the image is given as an input and it is been processed in image processing thus generating the output as the improved or of the same characteristics of the original image. The concept of image processing is that an image can be spitted into any number of shares such that to get the original image, a particular number of shared must be combined.

2. RELATED WORK

Phishing web pages are fake web pages that are created by phishers to imitate Web pages of real web site. This kind of web page has visual similarities to do fraud with their victims. Email is the most common way for doing this due to its easiness and simplicity. Phishers can send crafted emails to majority of the legitimate and can fool the users using the flaws in SMTP.

To overcome all this, researchers have given different methods such as-

1) Automated challenge Response method [1] is a method which provides authentication mechanisms. This method provides two way authentication and simplicity. This method also prevents man-in-middle attacks.
2) There are also a DNS-based anti-phishing approach [2] technique that contains heuristic detection, blacklists and page similarity assessment. But these techniques to have some cons.

a) In Heuristic based anti phishing technique, it is easy for the hacker to avoid the heuristic characteristics detection.
b) In Blacklist-based technique, we cannot detect the website that are not available in the database of the blacklist
c) In Similarity assessment based technique, it requires much time to calculate the pages. Thus, this is not suitable for detecting the phishing sites.

3) Ren-junn Hwang has proposed a technique which makes use of watermark method [3] to save digital image copyright ownership using visual cryptography. But here, there is the difficulty of finding the pixels having the watermark pattern.
4) Divya James [4] and Mintu Philip [4] have given an anti-phishing framework which uses visual cryptography [5] for detecting the phishing websites. In this, Image captcha validation scheme is used. There are two phases in this paper. One is for registration while other is for login.

3. EXISTING METHODOLOGY

In the existing methodology, from the below diagram we can see that whenever an end user enters the data in the websites then if the site is an actual site then the data is safe otherwise if the site is a phishing site then in this situation the information can be easily captured by the attackers using phishing technique.

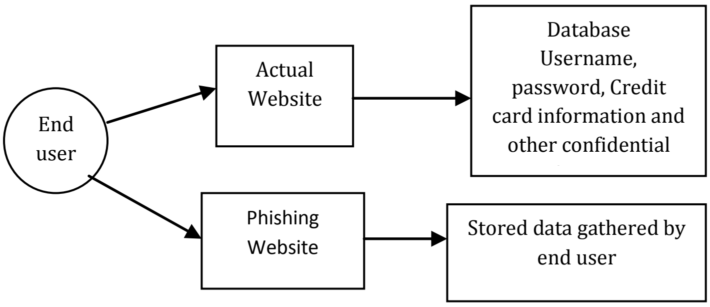

End user
Actual Website
Database Username, password, Credit card information and other confidential
Phishing Website
Stored data gathered by end user

Fig1: Existing Scenario

4. PROPOSED METHODOLOGY

In our proposed work, we are giving the methodology used for detecting the phishing websites. Our methodology is based on anti-phishing image captcha validation scheme using visual cryptography. The use of visual cryptography is to preserve the image captcha privacy. This is done by decomposing the image captcha into two shares such that one is with the user and the other with the server. The original image captcha can be generated only when both the shares are simultaneously present. The individual share cannot reveal the image captcha. Once we get the image captcha we can use it as a password.

This system protects confidential information of users by proving 3 layers of security.

1) First layer verifies whether the website is phishing website or secure website. If the site is phished one then it will not display the image captcha to the users because the image is generated by the stacking of both the shares, present with the user and the server.

2) Second layer checks validation of the image captcha in response to the user. The image captcha is human readable and not to machine users. Thus, by using image captcha mechanism no machine based user can hack the password or other information.

3) As a third layer of security, it prevents intruders attack.

5. MODULES

The modules in our project are: -

1) Registration phase

2) Login phase

A) Registration phase:-

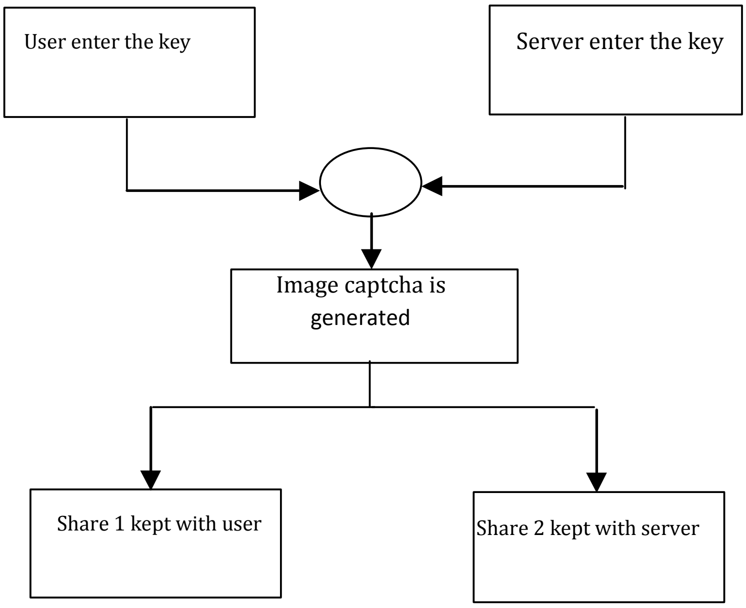
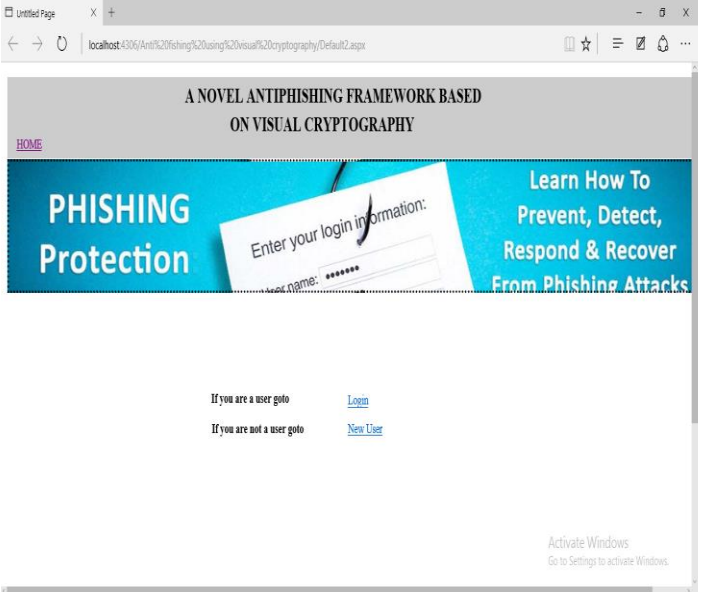


Figure: When user performs registration process for the website

In this phase, a key string (password) is taken by the user during the registration. The password can be the combination of letters and alphabet to give secure environment. The string is then combined with randomly generated string by server and thus forming the image captcha. The image is then split up into two shares i.e. one kept with user and another with server. It is also stored at database.

The screenshot for this phase are:-

1) The initial page is the home page where the users have two options i.e. if they are already registered then directly they login otherwise they have to first perform the registration.


Untitled Page
localhost:4306/Anti%20fishing%20using%20visual%20cryptography/Default2.aspx
PHISHING Protection
Enter your login information:
User name:
Learn How To Prevent, Detect, Respond & Recover From Phishing Attacks
Activate Windows
Go to Settings to activate Windows.

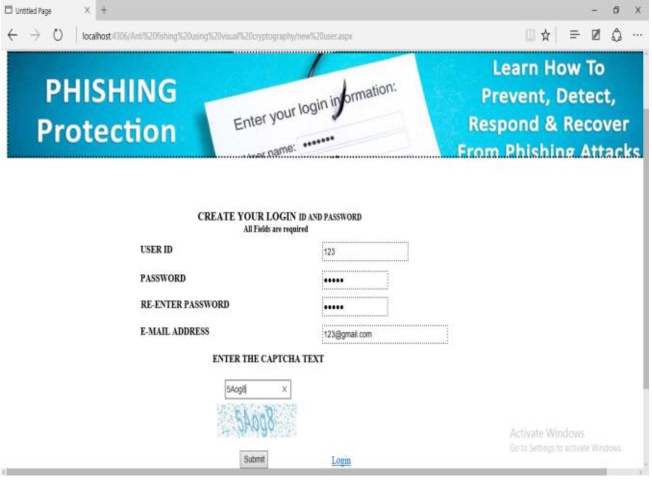
A NOVEL ANTIPHISHING FRAMEWORK BASED ON VISUAL CRYPTOGRAPHY

HOME

If you are a user goto Login

If you are not a user goto New User

2) Now if the user clicks the new user button then the registration page is getting opened.


Untitled Page
localhost:4306/Anti%20fishing%20using%20visual%20cryptography/new%20user.aspx
PHISHING Protection
Enter your login information:
User name:
Learn How To Prevent, Detect, Respond & Recover From Phishing Attacks
Activate Windows
Go to Settings to activate Windows.

CREATE YOUR LOGIN ID AND PASSWORD
All Fields are required

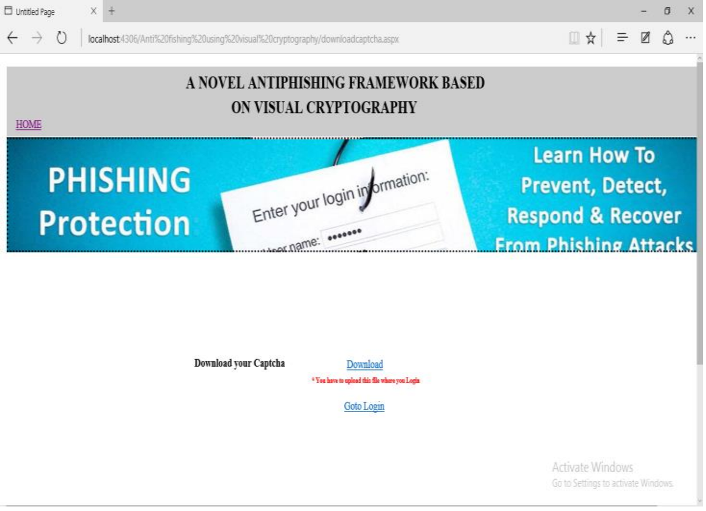
USER ID: 123
PASSWORD: •••••
RE-ENTER PASSWORD: •••••
E-MAIL ADDRESS: 123@gmail.com

ENTER THE CAPTCHA TEXT
5Aog8
5Aog8

Submit Login

Here the image captcha is divided into two shares

3) Now the user share can be downloaded.


Untitled Page
localhost:4306/Anti%20fishing%20using%20visual%20cryptography/downloadcaptcha.aspx
PHISHING Protection
Enter your login information:
User name:
Learn How To Prevent, Detect, Respond & Recover From Phishing Attacks
Activate Windows
Go to Settings to activate Windows.

A NOVEL ANTIPHISHING FRAMEWORK BASED ON VISUAL CRYPTOGRAPHY

HOME

Download your Captcha Download
* You have to upload this file where you Login

Goto Login

Here the registration phase gets completed.

B) Login phase:-

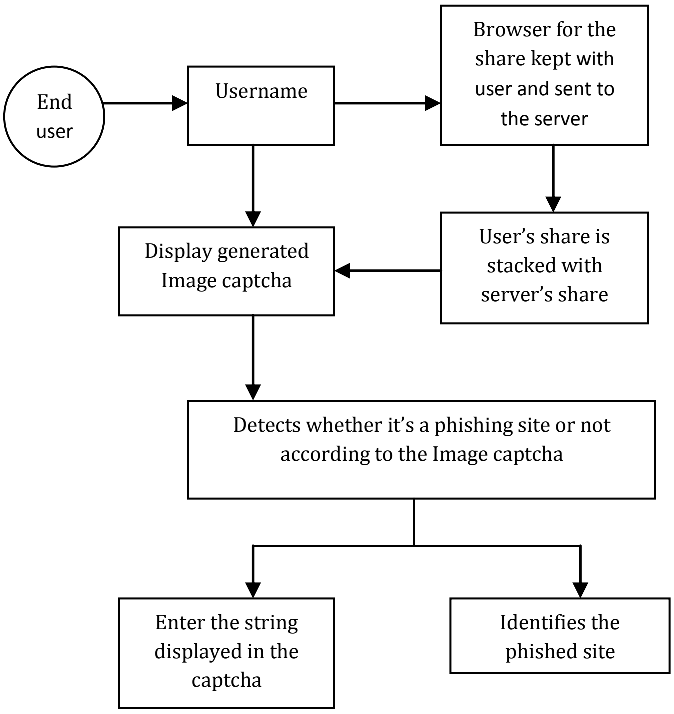
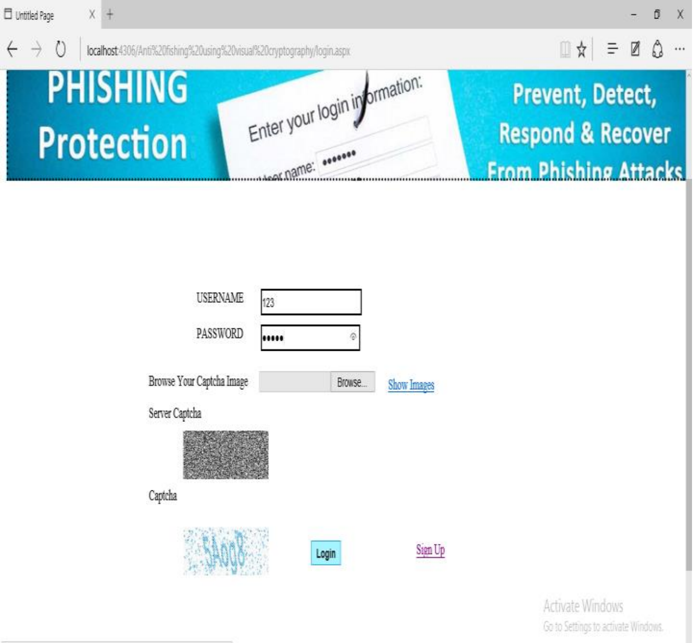

End user
Username
Browser for the share kept with user and sent to the server
Display generated Image captcha
User's share is stacked with server's share
Detects whether it's a phishing site or not according to the Image captcha
Enter the string displayed in the captcha
Identifies the phished site

Fig 3: When user attempts to log in into site

In the login phase, the user is first asked for the username or the user id. Now the user has to enter the share kept with him. Now this share is forwarded to the server where the users share and the share stored at the database is concatenated to produce captcha image. Now the image captcha is displayed to the user and here the end user check whether the given image captcha matches with the captcha created at the during registration phase. The end user is now required to enter the text displayed in the image captcha and this will be considered as a password and using this user can log in into the secured website. Using the username and image captcha generated by stacking two shares one can verify whether the website is secured website or not and can also verify whether the user is a human user or not.

The screenshot for this phase is given as:-

1) Here, first the user enters the username. Then the user browses for the share kept with him. After this we have to click on show image to check whether the same image captcha is generated or not. If he finds the generated captcha is similar to one seen at registration phase then he can easily put the password and can successfully login.


Untitled Page
localhost:4306/Anti%20fishing%20using%20visual%20cryptography/login.aspx
PHISHING Protection
Enter your login information:
Prevent, Detect, Respond & Recover From Phishing Attacks
Browse...
Show Images
Login
Sign Up
Activate Windows
Go to Settings to activate Windows.

USERNAME 123

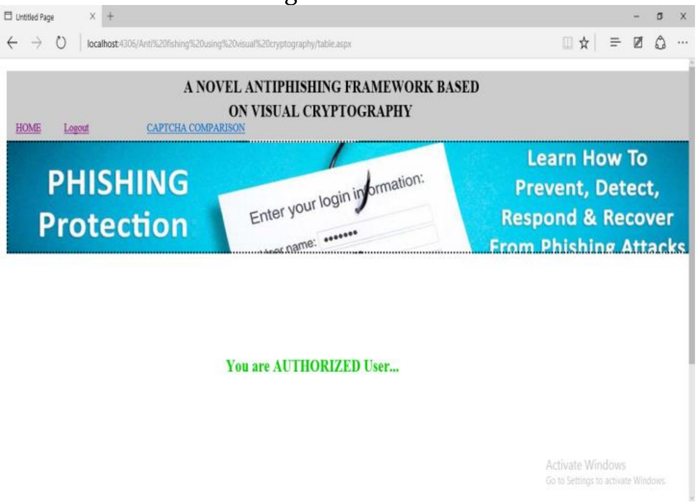
PASSWORD •••••

Browse Your Captcha Image

Server Captcha

Captcha

2) If the complete data is correct then the user can see the screen stating that he is an authorized user.


Untitled Page
localhost:4306/Anti%20fishing%20using%20visual%20cryptography/table.aspx
HOME
Logout
CAPTCHA COMPARISON
PHISHING Protection
Enter your login information:
Learn How To Prevent, Detect, Respond & Recover From Phishing Attacks
Activate Windows
Go to Settings to activate Windows.

A NOVEL ANTIPHISHING FRAMEWORK BASED ON VISUAL CRYPTOGRAPHY

You are AUTHORIZED User...

6. Implementation & Analysis

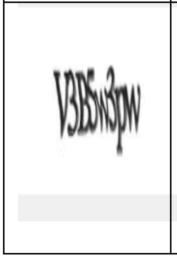
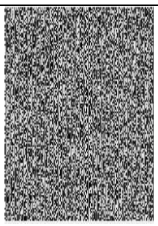
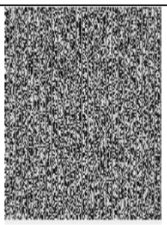
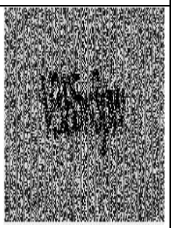
The proposed methodology is implemented using Asp.net and the following figure shows the result obtain by creation and stacking of shares.

The entire process is shown in the form of cases.

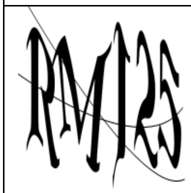
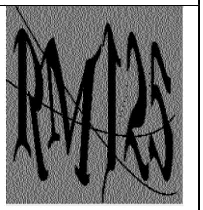
Case1 and Case 2 show the creation and stacking of shares of two image captcha's resulting in original captcha.

In Case3 share1 of first image captcha is combined with share2 of second captcha resulting in unrecognizable form of captcha.

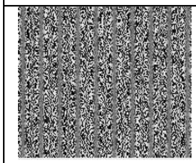
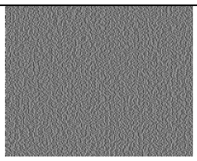
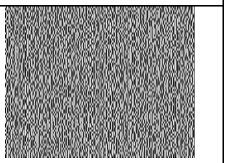
Case.1

Original Captcha	Share1	Share2	Reconstructed captcha
			

Case.2

Original Captcha	Share1	Share2	Reconstructed Captcha
			

Case.3

Share1 of case1	Share2 of case2	Reconstructed Captcha
		

It is seen that both original and reconstructed image captcha's are related with high degree of correlation.

7. CONCLUSION

Phishing attacks are very common in day-to-day life because it is done globally and very easily it can store the user's confidential information. This data can be used by attackers. . Phishing websites as well as human users can be easily identified using our proposed "An Anti-phishing framework based on Visual Cryptography". The proposed methodology protects confidential information of users using 3 layers of security.The proposed methodology can be used to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market etc.

REFERENCES

[1]. Thiyagarajan, P.; Venkatesan, V.P.; Aghila, G.; "Anti-Phishing Technique using Automated Challenge Response Method'", in Proceedings of IEEE- International Conference on Communications and Computational Intelligience, 2010.

[2]. Sun Bin.; Wen Qiaoyan.; Liang Xiaoying.; "A DNS based Anti-Phishing Approach," in Proceedings of IEEE- Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010.

[3]. Ren-Junn Hwang,"A digital image copyright protection scheme based on visual cryptography", Tamkang Journal of science and engineering, Vol.3, No. 2, pp. 97-106(2000).

[4]. Divya James, Mintu Philip, "A novel Anti-phishing framework based on visual cryptography", IEEE 2012.

[5]. M.Naor and A.Shamir,"Visual cryptography", in Proc. EUROCRYPT, 1994, pp.1-12. IJDPS Vol.3, No.1, 2012.