**International Journal of Computer Engineering & Technology (IJCET)**
Volume 7, Issue 6, November–December 2016, pp. 18–29, Article ID: IJCET_07_06_003
Available online at
http://www.iaeme.com/ijcet/issues.asp?JType=IJCET&VType=7&IType=6
Journal Impact Factor (2016): 9.3590(Calculated by GISI) www.jifactor.com
ISSN Print: 0976-6367 and ISSN Online: 0976–6375
**© IAEME Publication**

# AN EFFICIENT ANTI PHISHING FRAMEWORK BASED ON DYNAMIC CAPTCHA

**N. Chandra Sekhar Reddy**
Professor, HOD Department of CSE, MLR Institute of Technology, Hyderabad, India

**Dr. Purna Chandra Rao**
Professor, Department of CSE, Swamy Vivekananda Institute of Technology, India

**Dr. A. Govardhan**
Professor, Department of CSE, Principal, JNTUH, Hyderabad, India

## ABSTRACT

*Web security has become a serious and challenging issue due to the growth of Internet, due to this drastic growth Cyber-attacks has been increasing day by day. Phishing (attempt to obtain sensitive information such as user names, passwords, and credit card details from unsuspecting victims for identity theft, financial gain and other fraudulent activities) is one of the most popular attack. Hackers design fake websites which appear very identical to the original ones are being hosted to achieve this. In this paper a new approach called "Anti-phishing framework based on visual cryptography "is introduced to solve phishing problems. Using Visual Cryptography, we will be able to use image for authentication. Visual cryptography (VC) schemes hide the secret image into two or more images called shares. Here the shares are shared with the user and database. The secret image will be recovered simply by stacking the shares together without any complex computation. The original image captcha can be revealed without any complex computation only when both shares are simultaneously available; the individual sheet images do not reveal the original image captcha. Once the original image captcha is revealed to the user that can be used as the password. Using this method the website cross verifies its identity and proves that it is a genuine website before the end users.*

**Key words:** Phishing, Image Captcha, Shares, Security, Visual cryptography.

**Cite this Article:** N. Chandra Sekhar Reddy, Dr. Purna Chandra Rao, Dr. A. Govardhan, An Efficient Anti Phishing Framework based on Dynamic Captcha. *International Journal of Computer Engineering and Technology,* 7(6), 2016, pp. 18–29.
http://www.iaeme.com/ijcet/issues.asp?JType=IJCET&VType=7&IType=6

## 1. INTRODUCTION

Now-a-days online transaction has become very common and there are various attacks present behind this. In these types of various attacks, phishing is distinguish as a major security threat and new novel ideas are arising in each and every second so preventive mechanisms should also be so effective. Thus the security in these cases is very high and should not be easily tractable with implementation easiness.

Continuous improvement of design and technology in the middle-ware has made the applications detection very critical. As a result, it has become impossible to be sure whether a computer connected to the internet can be considered trustworthy and secure or not. Phishing scams have become a problem for online banking and e-commerce users.

The question is how to handle applications that require a high level of security.

Phishing is a form of online fraudulent activity that aims to steal sensitive information such as online banking passwords and credit card details from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and well developed. Another definition of phishing is given as "a criminal activity acquiring personal or vital information using social engineering techniques. Phishers attempt to acquire sensitive information, such as passwords, credit card details etc., by falsifying as a trustworthy person / business in an electronic communication". One more comprehensive definition of phishing, states that it is "the act of sending emails to a user falsely claiming to be an legitimate enterprise into an attempt to scam the user into surrendering private information that will be used as identity theft". With this acquired vital information, masquerading as a trustworthy person has also become easier with the use of technology. Identity theft can be described as "a crime in which the impostor obtains key pieces of information such as SSN numbers and driving license numbers and uses them for his or her own gain".

Phishing [1] scams rely upon a mix of technical deceit and social engineering practices. In the majority of cases the phisher must provoke the victim to intentionally perform a series of actions that will provide access to confidential/private information. Email, web-pages, IRC and instant messaging services are most popular communication channels. In all these cases the phishers must use a trusted source (eg, the help desk of their bank, automated support response from their selected online retailer, etc.) to make the victim to believe. To date, the most successful phishing attacks have been initiated by emails – where the phisher impersonates the sending authority (eg. spoofing the source email address and embedding appropriate company logos). So here we introduce a new method which can be used as a safe way against phishing which is named as "A novel approach against phishing using visual cryptography". As the name describes, in this approach we introduced a new website which cross verifies its own identity and proves that it is a genuine website (for bank transaction, E-commerce and online booking system etc.,) to make the both the sides of the system secure as well as an authenticated one. Here the concept of image processing and an improved visual cryptography is used. Image processing is a technique of processing the image input and to get the improved form of the same image and/or characteristics of the input image as output. Visual Cryptography (VC) is a method of encrypting the secret image into shares, so that stacking number of sufficient shares reveals the secret image.

This paper is organized as follows: Part II deals with the related work using Visual Cryptography and Part III presents the proposed Methodologies. Part IV presents the implementation and Part V deals with Results and Discussions. Part VI contains the conclusion.

## 2. LITERATURE SURVEY

Phishing web pages are forged web pages that are created by malicious people to mimic Web pages of real web sites. Most of these kinds of web pages have high visual similarities to scam their victims. Some of these kinds of web pages look exactly like the real ones. Victims of phishing web pages may expose their bank account, password, credit card number, or other important information to the phishing web page owners. It includes techniques such as tricking customers through email and spam messages, man in the middle attacks, and installation of key loggers and screen captures.

Emails are one of the most common techniques for phishing, due to its simplicity, ease of use and wide reach. Phishers can deliver specially crafted emails to millions of legitimate email addresses very quickly and can fool the recipients utilizing well known flaws in the SMTP. Some of the most common techniques used by phishers include official looking and sounding emails, copying legitimate corporate emails with minor URL changes, obfuscation of target URL information etc. Methods like virus/worm attachments to emails, crafting of ‘personalized’ or unique email messages are also common.

One of the best techniques to protect data is cryptography (data encryption/decryption). It is the art of sending and receiving encrypted messages which can be decrypted only by the end user. Encryption and decryption are computed by using mathematical algorithms in such a way that only intended recipient can decrypt and read the message. Naor and Shamir [2] introduced the visual cryptography scheme (VCS) which is a simple and secure way to allow the secret sharing of images without any cryptographic computations.

A brief survey is presented here in the field of visual cryptography. Visual cryptography schemes were separately proposed by Shamir [3] and Blakley [4], their original intention was to safeguard cryptographic keys from loss. These schemes also have been widely used in the construction of several types of cryptographic protocols [5] .They have used these techniques many applications in different areas such as opening a bank vault, access control, opening a safety deposit box or even launching of missiles. Visual cryptography which is based on segment is suggested by Borchert [6] can be used only to encrypt the messages which are containing symbols, especially numbers like bank account number, amount etc. The VCS proposed by Wei-Qi Yan et al., [7] can be applicable only for printed images or text.

An iterative VC method proposed by Monoth et al., [8] is computationally complex as the encoded shares are further encoded into number of sub-shares iteratively. Likewise a technique proposed by Kim et al., [9] also draw backs due to computational complexity, though it avoids dithering of the pixels. Most of the previous research work on Visual Cryptography focused on improving two parameters: pixel contrast and expansion [10]. In these cases all participants who hold shares are assumed to be trusted user, that is, they will not present false or fake shares during the phase of the secret image recovering. Thus, the image shown on the arranging the shares is considered as the real secrete image. But, this may not be true always. Visual Cryptography Scheme is a cryptographic technique/methodology that allows for the encryption of visual information in which decryption can be performed using only the human visual system.

| **Pixel Name** | **Pixel probability (p)** | **Shares combination for pixel formation** | **Resultant pixel after overlapping** |
|---|---|---|---|
| White □ | P=0.5<br>P=0.5 | □■ □■<br>■□ ■□ | □■<br>■□<br>White Pixel Forms two sub pixels- white and black |
| Black ■ | P=0.5<br>P=0.5 | ■□ □■<br>□■ □■ | ■■<br>■■<br>Black pixel forms two black sub pixels |

**Figure 1** Illustration of a 2-out-of-2 VCS scheme with 2 sub pixel construction.

## 3. PROPOSED METHODOLOGY

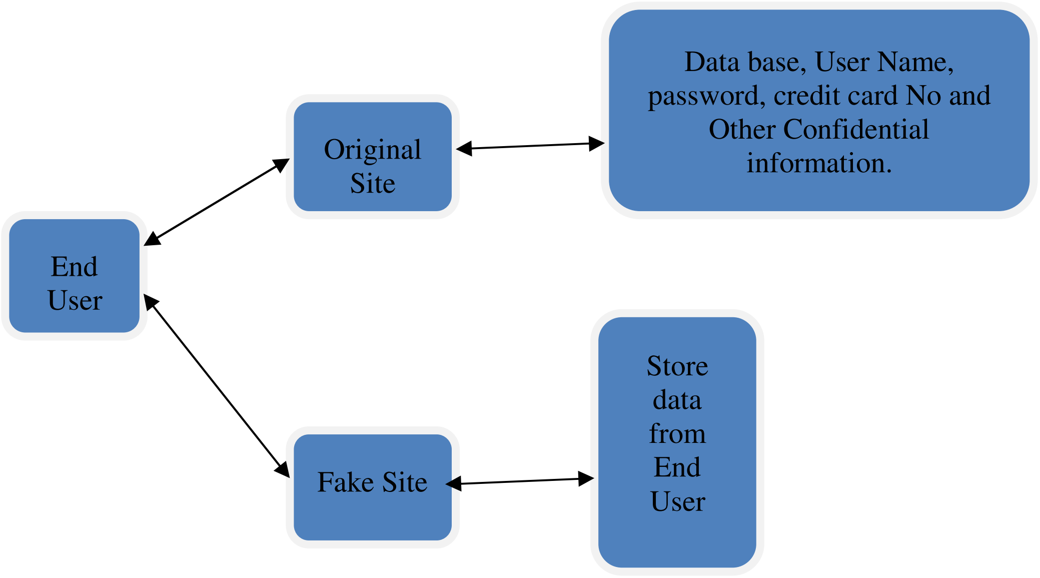

Data base, User Name, password, credit card No and Other Confidential information.
Original Site
End User
Store data from End User
Fake Site

**Figure 2** Current scenario

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 payment gateway or money transfer) by logging into his secure mail account or bank account, the person enters information like credit card no, username, password etc. on the login page. But quite often, this information can be captured by hackers using phishing techniques (a phishing website can collect the login details the user enters and redirect him/her to the actual site). There is no such information that cannot be directly obtained from the user at the time of his login input.

For phishing prevention and detection, we are proposing a new methodology to detect the fake website. Our methodology is based on Image Captcha validation scheme for anti phishing using visual cryptography. It prevents confidential information and password from the phishing websites.

The proposed approach can be divided into two phases:

i. Registration Phase

ii. Login Phase

### 3.1. Registration Phase

In the first (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 shares 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 the key string when it is needed. Registration process is depicted in Fig.3.

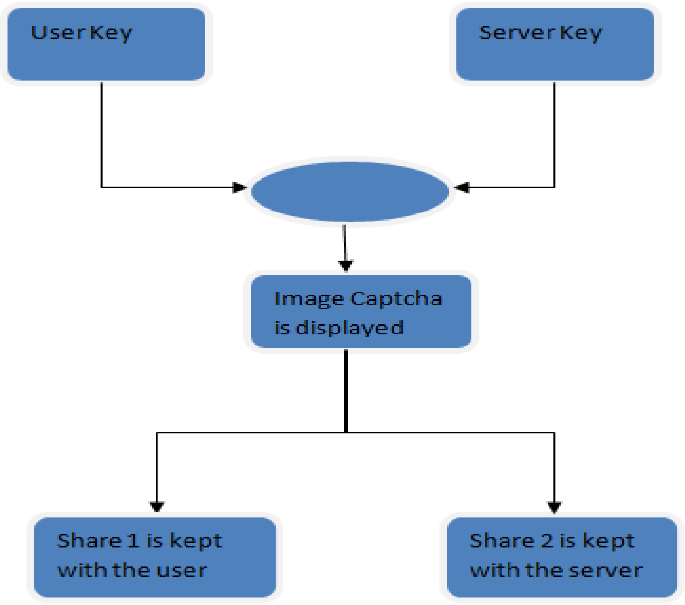

User Key
Server Key
Image Captcha is displayed
Share 1 is kept with the user
Share 2 is kept with the server

**Figure 3** User registration process

### 3.2. 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 Figure 4.

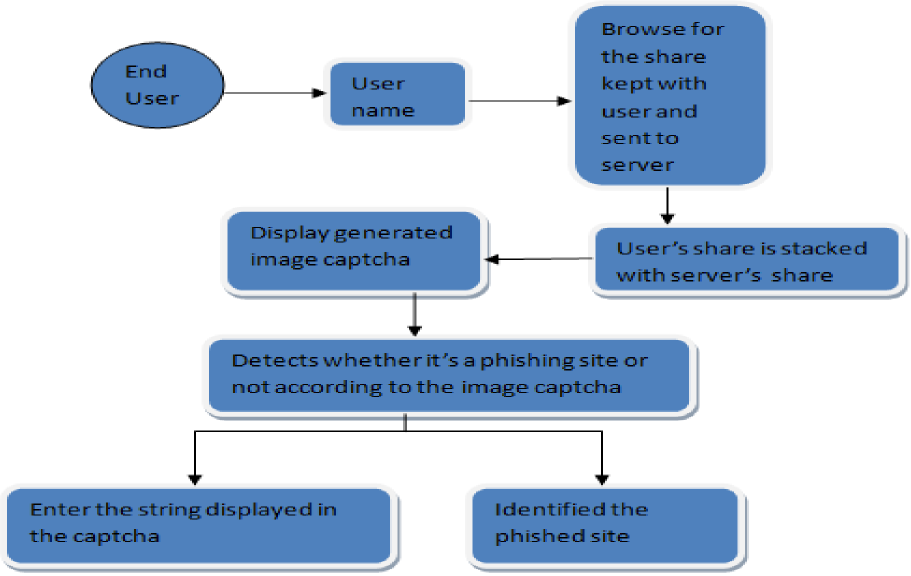

End User
User name
Browse for the share kept with user and sent to server
User's share is stacked with server's share
Display generated image captcha
Detects whether it's a phishing site or not according to the image captcha
Enter the string displayed in the captcha
Identified the phished site

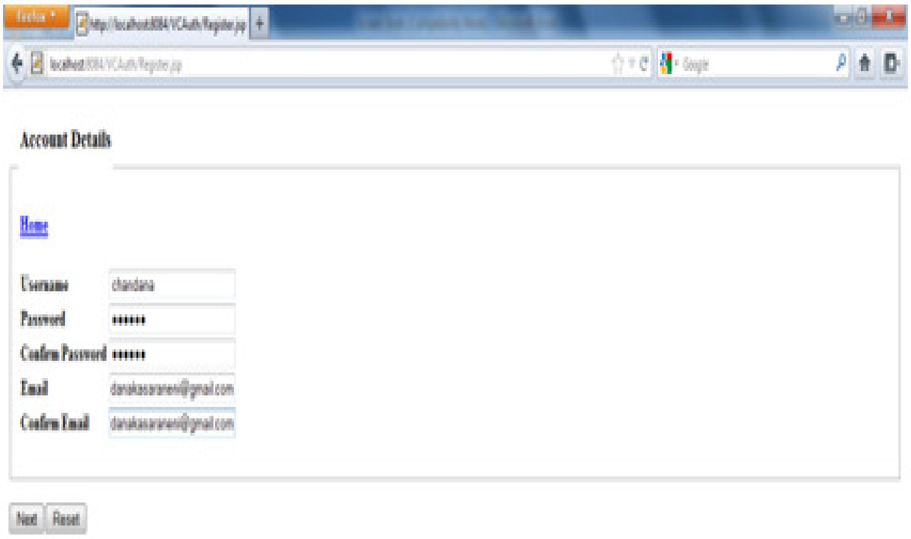
**Figure 4** when user attempts to log in into site

## 4. IMPLEMENTATION & ANALYSIS

In the registration phase creation of shares from the image captcha is the most important part where one share is kept with the server and other share is kept with the user. For login, the user needs to enter a valid username in the given field. Then he has to browse his share to process. An image captcha is generated by combining the user's share and with the share in the server. Now the user has to enter the text from the image captcha in the mandatory input field for logging into the website. The entire process is depicted in the screenshots. The proposed strategy is implemented using Matlab.

### 4.1. Registration Phase

The Registration page consists of Username, Password, Confirmation of Password, email & Confirmation of Email. Password and Confirm password should be same. Email and Confirm email also should be same to register. Username should be in string format. Password may be anything like string or number or combination of both. Registration screenshot is shown in Figure 5.



Account Details

Home

Username chandana

Password ••••••

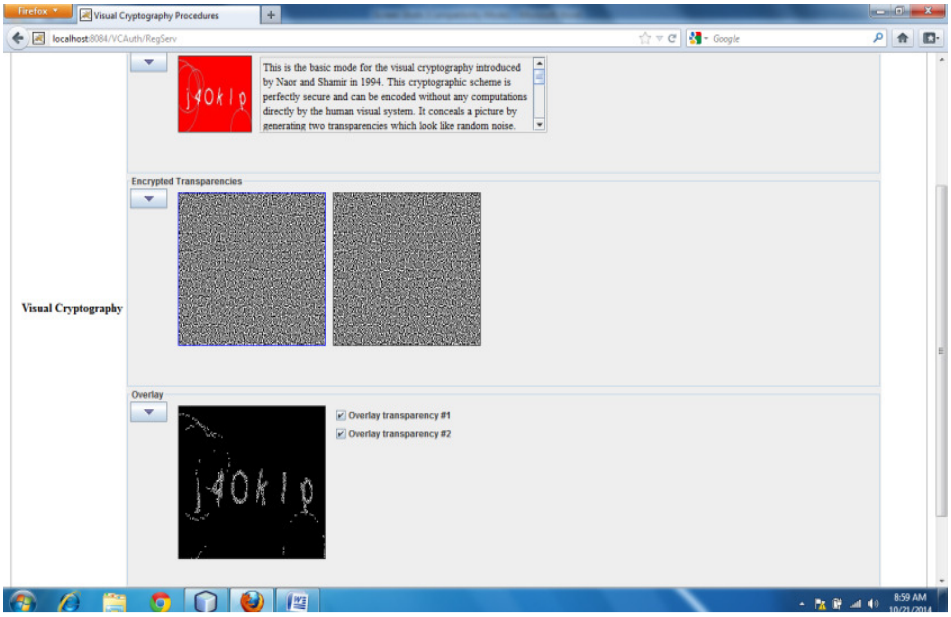
Confirm Password ••••••

Email danakasaraneni@gmail.com

Confirm Email danakasaraneni@gmail.com

**Figure 5** Registration Screen Shot

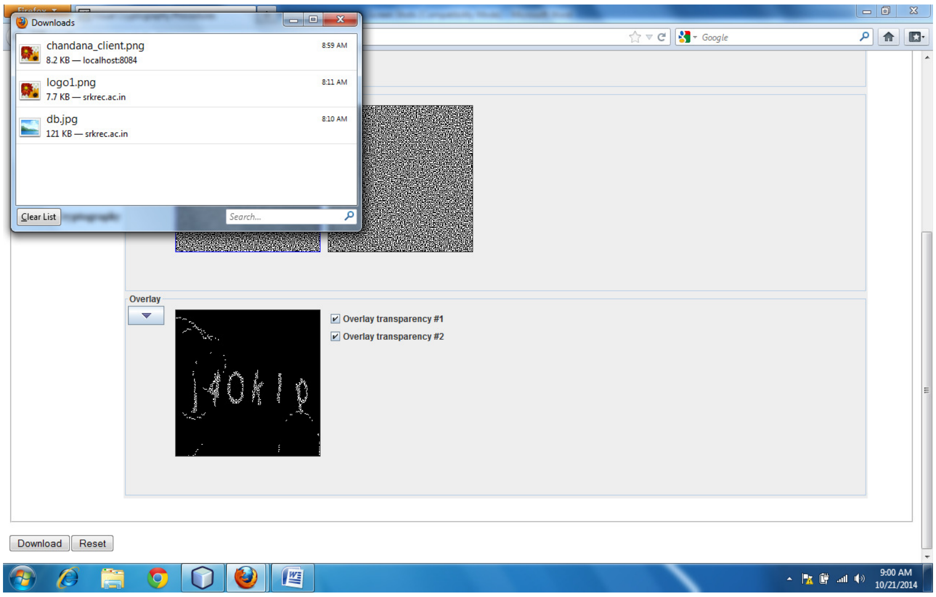
At the registration phase, a key string (password) is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to provide more secure environment. This string is concatenated with randomly generated string in the server and an image CAPTCHA is generated. CAPTCHA can be a combination of alphabets and numbers to provide more secure environment. The CAPTCHA can be generated by shuffling the numbers, capital alphabets and small alphabets. If the CAPTCHA is like in this format it is more secure. The image CAPTCHA is divided into two shares such that one of the shares 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 the key string when it is needed. Generated captcha, encrypted shares and overlapping of the shares. This is shown in Figure 6.


Firefox
Visual Cryptography Procedures
localhost:8084/VCAuth/RegServ
Google
j40klp
Visual Cryptography
Encrypted Transparencies
Overlay
☑ Overlay transparency #1
☑ Overlay transparency #2
8:59 AM
10/21/2014

This is the basic mode for the visual cryptography introduced by Naor and Shamir in 1994. This cryptographic scheme is perfectly secure and can be encoded without any computations directly by the human visual system. It conceals a picture by generating two transparencies which look like random noise.

**Figure 6** Captcha generation process

The client share of the CAPTCHA is downloaded for future purpose is shown in screen shot (Figure 7) below.



chandana_client.png 8:59 AM
8.2 KB — localhost:8084

logo1.png 8:11 AM
7.7 KB — srkrec.ac.in

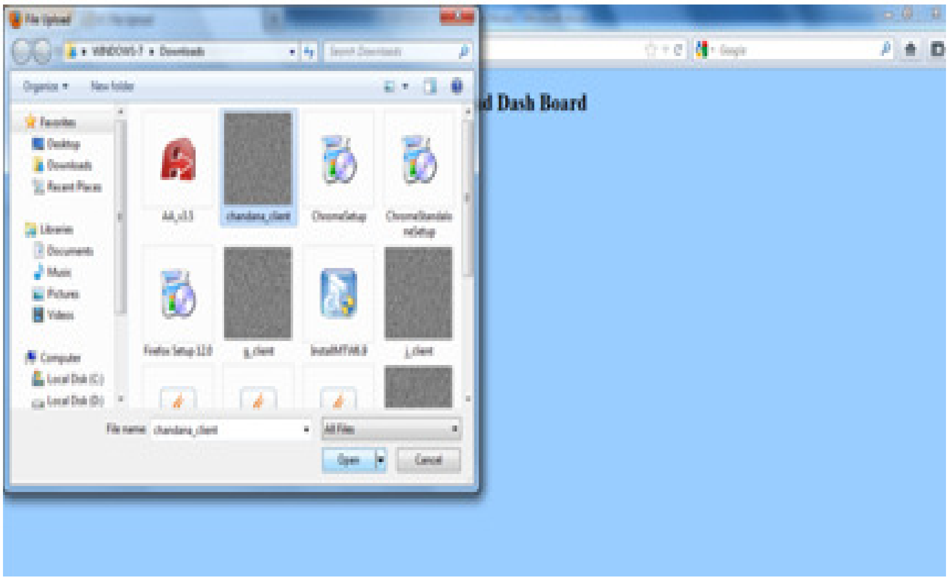
db.jpg 8:10 AM
121 KB — srkrec.ac.in

**Figure 7** Downloaded Captcha

## 4.2. Login Phase

At the time of Login Phase, 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 client share of the CAPTCHA will be uploaded to login. After selecting the file then click open button and then click upload button to upload the client share below is the screen shot for client uploading the downloaded file. Below is the screen shot (Figure 8) for user uploading the downloaded CAPTCHA.



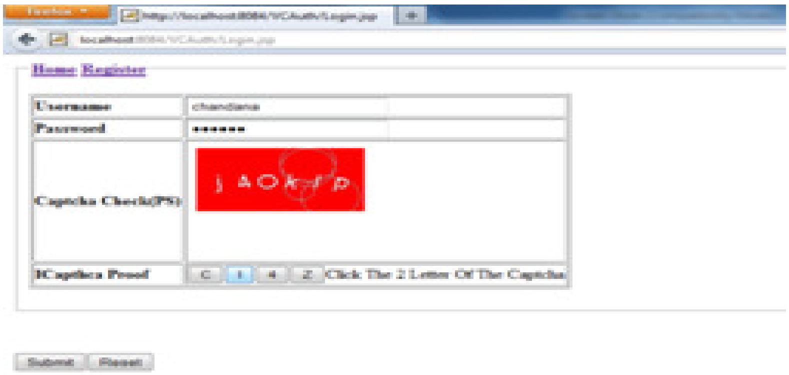
File name: chandana_client

All Files

**Figure 8** Uploading the downloaded Captcha

After entering into the Login Page the user must enter Username, Password & must click on the corresponding characters. This input sequence continues until one click has been performed for each character of the CAPTCHA image.

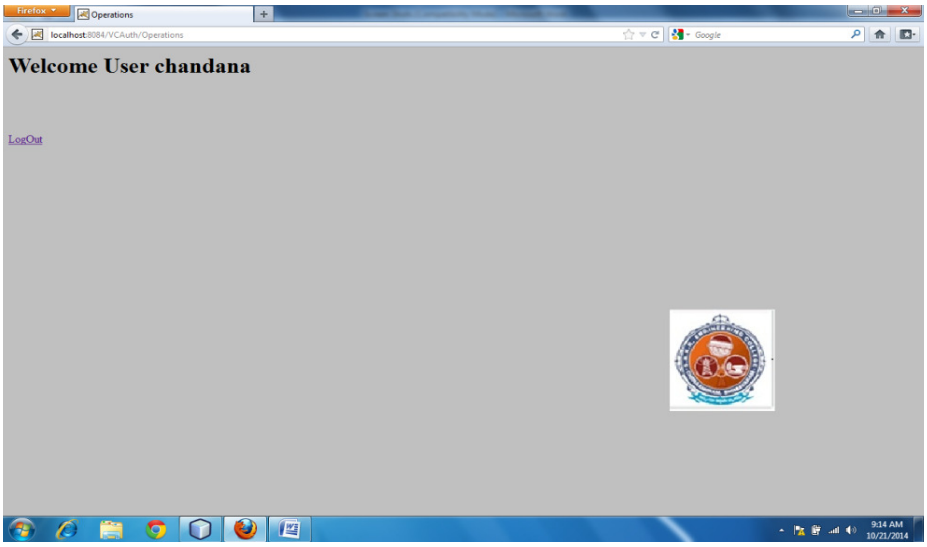
Client has to click the first letter of the CAPTCHA which is displayed on the screen. On successful clicking client side Ajax script will send request to the server which is ping command. Then server will send reply to client as pong command. The second challenge for the 2nd letter will be displayed on the screen this process will keep on continuing until captcha length as shown in Figure 9.


Firefox
http://localhost:8084/VCAuth/Login.jsp
localhost:8084/VCAuth/Login.jsp
Home Register
j A O k f p
Submit
Reset

| | |
|---|---|
| Username | chandana |
| Password | •••••• |
| Captcha Check(PS) | |
| ICaptcha Proof | C 1 4 Z Click The 2 Letter Of The Captcha |

**Figure 9** Captcha Approval Process

When the input sequence is complete, the correct index sequence is then compared with the user clicked index sequence. If there is a match, the CAPTCHA has been correctly decoded by the user. User successful login is shown in Fig. 10.



Welcome User chandana

LogOut

**Figure 10** User authentication

# 5. RESULTS AND DISCUSSIONS

## 5.1. Creating Image Captcha

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 shares 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 the key string when it is needed which is shown in figure 11.

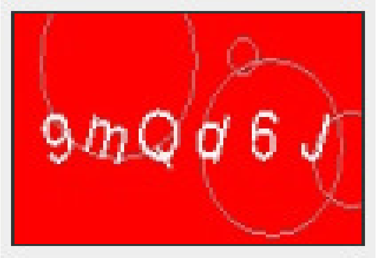


**Figure 11** Original CAPTCHA

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. Figure 12 show the two generated shares. Fig 13 show resultant captcha generated by superimposing the two shares.

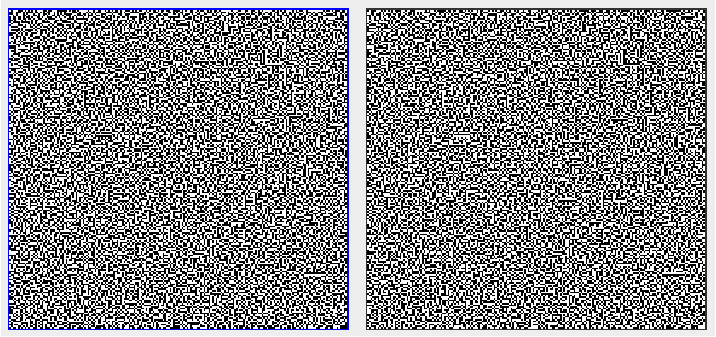


**Figure 12** Overlaying Share 1 & Share 2

## 5.2. Captcha Solving Test

In CAPTCHA solving test, the user is required to solve one CAPTCHA to solve one CAPTCHA test. This test begins with by clicking on the CAPTCHA image. After clicking on the CAPTCHA image some buttons with characters are appeared below the CAPTCHA image. Here, first the user must click on the button corresponding to character-1 of the CAPTCHA image and follow the same certain sequences until all the characters in the CAPTCHA image are completed in order to successfully solve this CAPTCHA test. The idea behind this CAPTCHA test is that here we stored the per character response time. If the user is login to the website for the first time then the per character response time is stored at the server side.

**Table 1** Time sequences of different logins of the user

| Login number | Existing system time(sec) | Proposed system time(sec) |
|---|---|---|
| 1 | 1.2 | 1 |
| 2 | 2.5 | 1 |
| 3 | 2 | 1.8 |
| 4 | 3 | 2.8 |

Next time the user is login to that website then at that time the verification process is done here i.e here the current user per character response time is compared with the previously stored per character response time which is stored at the server. If it is matches, then finally the user can successfully log in into that website and can securely perform further proceedings. If it is not matches then the user has to login again in order to access the website. Time sequences of different logins of the user are shown in the Table 9.1.

In our proposed method, we are using here CAPTCHA solving test in order to defend against image based attacks and the third party human based attacks. Because, some researchers proposed that the current existing CAPTCHA can be attacked by using various well-known techniques and within submission time it can be known to the attackers. So, our newly proposed systems used visual cryptographic schemes and newly designed CAPTCHA scheme in order to counter the phishing websites and the phishing attacks. The graph for the time duration in existing system and proposed system is shown in the following Figure 8.

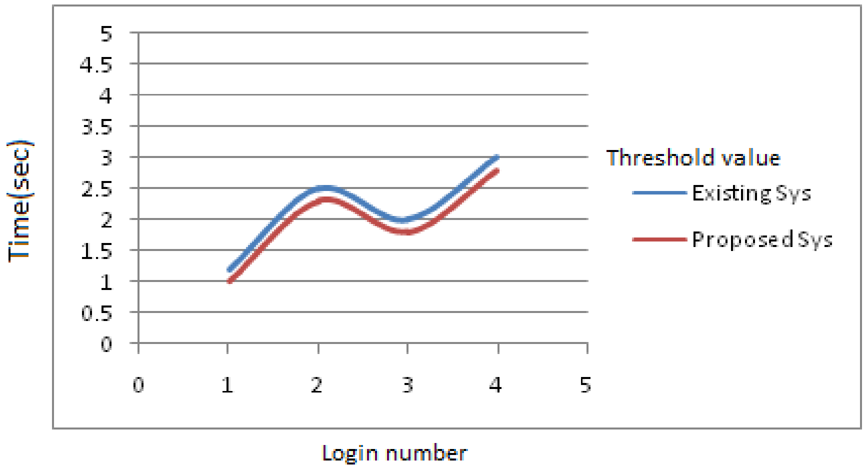


**Figure 8** Time duration in existing system and proposed system

## 6. CONCLUSION

Currently phishing attacks are so common because attackers can attack globally and capture and store the users' confidential information. This information is used for phishing process. Phishing websites as well as human users can be easily identified using our proposed methodology "Anti-phishing framework based on Dynamic captcha". The proposed methodology preserves important information of users using 3 layers of security. 1st layer verifies whether the website is a genuine website or not. If the website is a not genuine website (a fake one just similar to secure website but not the secure website), then in that situation, the fake 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 generation of image captcha is by the stacking of two shares, one with the user and the other with the actual server of the website.

Second layer cross verifies the image Captcha corresponding to the user. The image Captcha generated is readable by human users alone 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, by using image Captcha technique, no machine based user can crack the confidential information or passwords of the users. The third layer of security it prevents intruders' attacks on the user's account. This method provides extra security by not letting the intruders to log in into the account even when though attacker knows the username of a particular user. The proposed strategy is also useful to prevent the attacks of Fake/phishing websites on banking portal, financial web portal, online shopping market.

## REFERENCE

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

[2] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT,1994, pp. 1–12.

[3] A. Shamir, .How to Share a Secret. Communication ACM, vol. 22, 1979, pp. 612-613.

[4] G. R. Blakley, .Safeguarding Cryptographic Keys. Proceedings of AFIPS Conference, vol. 48, 1970, pp. 313-317.

[5] A. Menezes, P. Van Oorschot and S. Vanstone, .Handbook of Applied Cryptography. CRC Press, Boca Raton, FL, 1997.

[6] B. Borchert, .Segment Based Visual Cryptography, WSI Press, Germany, 2007.

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

[8] T. Monoth and A. P. Babu, .Recursive Visual Cryptography Using Random Basis Column Pixel Expansion, in Proceedings of IEEE International Conference on Information Technology, 2007, pp. 41-43.

[9] 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.

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

[11] Getaneh Berie Tarekegn and Yirga Yayeh Munaye, Big Data: Security Issues, Challenges and Future Scope, *International Journal of Computer Engineering and Technology (IJCET),* 7(4), 2016, pp. 12–24.

[12] Dr. R. Mala and K. Karthikeyan . Artificial Neural Cryptography Datagram Hiding Techniques For Computer Security Objects Register , *International Journal of Computer Engineering and Technology (IJCET),* 7(2), 2016, pp. 36 – 43.