Anti Phishing using Visual Cryptography

Amit Navarkar[1], **D. A. Phalke**[2]

[1]D Y Patil College of Engineering, Akurdi, Pune, India
[2]D Y Patil College of Engineering, Akurdi, Pune, India

Abstract: ***Phishing is done to acquire confidential information such as usernames, passwords, and credit card details by disguising as a legitimate entity in an electronic communication. In this paper we have proposed a new approach named as "Anti-phishing using visual cryptography" to solve the problem of phishing. Here an image-based authentication is performed using Visual Cryptography. The image captcha is decomposed into two shares that are stored in separate database servers (one with user and one with server) such that the original image captcha is revealed only when both the shares are simultaneously stacked. Once the original image captcha is revealed, the user can use it as the password.***

Keywords: Phishing, Visual Cryptography, Image Captcha

1. Introduction

Online transactions are nowadays become very common and it is no more a safe platform for its users. There are various types of attacks, but phishing is identified as a major security threat, so preventive mechanism should also be so effective. The term is a variant of fishing, probably influenced by phreaking, and alludes to "baits" used in hopes that the potential victim will "bite" by clicking a malicious link or opening a malicious attachment, in which case their financial information and passwords may then be stolen. So the security required in these cases should be very high and should not be easily tractable with implementation easiness.

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 can be explained as a criminal activity using social engineering techniques where Phishers attempt to falsely acquire sensitive information by masquerading as a trustworthy person or business in an electronic communication. Another comprehensive definition of phishing, states that it is “the act of sending an email to a user falsely claiming to be an established legitimate enterprise into an attempt to scam the user into surrendering private information that will be used for identity theft”.

Here we have introduced a new method, which can be used as a safe way against phishing, which is named as "Anti-phishing using visual cryptography". In this approach website cross verifies its own identity to the end users and makes the system secure as well as an authenticated one. In this technique the concept of image processing and an improved visual cryptography is used. Visual Cryptography (VC) is a method of encrypting a secret image into shares, such that after stacking a sufficient number of shares the secret image is revealed.

2. Types of Phishing

Numerous different types of phishing attacks have now been identified. Some of the more prevalent are listed below.

2.1 Deceptive Phishing

Messages about the need to verify account information, system failure requiring users to re-enter their information, fictitious account charges, undesirable account changes, new free services requiring quick action, and many other scams are broadcast to a wide group of recipients with the hope that the unwary will respond by clicking a link to or signing onto a bogus site where their confidential information can be collected.

2.2 Malware-Based Phishing

Refers to scams that involve running malicious software on users' PCs. Malware can be introduced as an email attachment, as a downloadable file from a website, or by exploiting known security vulnerabilities--a particular issue for small and medium businesses (SMBs) who are not always able to keep their software applications up to date.

2.3 Key loggers and Screen loggers

These are particular varieties of malware that track keyboard input and send relevant information to the hacker via the Internet. They can embed themselves into users' browsers as small utility programs known as helper objects that run automatically the first line indented about 3.6 mm when the browser is started as well as into system files as device drivers or screen monitors.

2.4 Man-in-the-Middle Phishing

It is harder to detect than many other forms of phishing. In these attacks hackers position themselves between the user and the legitimate website or system. They record the information being entered but continue to pass it on so that users' transactions are not affected. Later they can sell or use the information or credentials collected when the user is not active on the system.

2.5 Search Engine Phishing

This occurs when phishers create websites with attractive sounding offers and have them indexed legitimately with search engines. Users find the sites in the normal course of searching for products or services and are fooled into giving up their information. For example, scammers have set up false banking sites offering lower credit costs or better interest rates than other banks.

2.6 Data Theft

Unsecured PCs often contain subsets of sensitive information stored elsewhere on secured servers. Certainly PCs are used to access such servers and can be more easily compromised. Data theft is a widely used approach to business espionage. By stealing confidential communications, design documents, legal opinions, employee related records, etc. thieves profit from selling to those who may want to embarrass or cause economic damage or to competitors.

3. Related Work

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, 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.

Researchers propose user-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. Challenge-Response module in turn will call the get response application, which is installed in the client machine. Once the challenge-response is validated user credentials are demanded from client and server to precede the transaction validates it.

Automated Challenge-Response Method ensures two way authentication and simplicity. The proposed method also prevents man-in-the middle attacks since the response is obtained from the executable that is called by the browser and third man interruption is impossible. 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 nullify.

Now there is DNS-based anti-phishing approach technique, which mainly includes blacklists, heuristic detection and the page similarity assessment. But they do have some shortcomings.

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 query interface. Internet Explorer7, Netscape Browser8.1, 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. The administrator has verified every URL in the blacklist, the false alarm probability is very low. However, there are a lot of technical disadvantages. Firstly, the phishing websites we found is a very small proportion, so the failed alarm probability is very high. Secondly, generally to say, the life cycle of a phishing website is only a few days. A website might be shut down before we found and verified it is a phishing website.

Heuristic-based anti-phishing technique is to estimate whether a page has some phishing heuristics characteristics. For example, some heuristics characteristics used by the Spoof Guard toolbar include checking the host name, checking the URL for common spoofing techniques, and checking against previously seen images. If you only use the Heuristic-based technique, the accuracy is not enough. Besides, phishers can use some strategies to avoid such detection rules. The user may be deceived by the phishing website because the phishing website imitates a legitimate website. Its pages are often similar with the legitimate sites. Therefore, some researchers proposed a similarity assessment method to detect phishing sites.

A three-factor authentication scheme named Phish-Secure focuses to counter attack phishing. Here as a first factor of authentication, an image similarity detection is done which helps in finding out which page the user tends to visit, then it is checked for Phishing .For this purpose a system captures the image of a webpage in a particular resolution in the required format. This image is termed as Visual image. If the attacker is going to create a Phishing site he is going to use the replica of the original webpage in order to fool the users. Now Phish-Secure gets the Visual image of the visited page and collects the mean RGB value of the image. This is termed as V_RGB. The database with Phish-Secure uses consists of details about the page, which has to be authenticated. The actual mean RGB of various Webpages is stored in the database, which is denoted as A_RGB. Phish-Secure will utilize this information and make a comparison to find out the similarity between the visited page and the page in the database. The similarity is obtained in means of percentage, if the percentage of similarity (PS) is greater than 99 % then Phish-Secure concludes which website the user is tending to visit. Taking the corresponding URL in the database carries this out and checking is done in order to find whether the site is Phishing or not.

As a second factor of authentication Phish-Secure grabs the destination IP in Layer 3 which gives information about to which IP address the user is getting connected, this is referred as V_IP. If an attacker's web server IP address has already been found guilty the particular IP is blacklisted. Phish-Secure check this Blacklist with the V_IP and will warn the user. On the other hand if the V_IP is not found in Blacklist, further verification is done in the following step.

Here in this step Phish-Secure grabs the actual list of IP address of the provider which he tends to connect. This is because any provider may have multiple servers for the purpose of load balancing and the user may be connected to his location accordingly. In order to avoid any confusion Phish-Secure gets the list of IP address, which is referred to as actual IP and is checked with the V_IP (i.e.) the IP address to which the user is getting connected. If these two IP address are same Phish-Secure identifies the particular site as genuine and returns a message as authenticated. On the other hand if there is a mismatch in the above verification Phish-Secure identifies the site as Phishing and warns the user. In addition to this the V_IP is added to the black list so that in future if the attacker uses the same web server and tries to attack, Phish-Secure detects the site as Phishing in the second step.

These popular technologies have several drawbacks:

3.1 Blacklist-based technique with low false alarm probability, but it cannot detect the websites that are not in the blacklist database. Because the life cycle of phishing websites is too short and the establishment of blacklist has a long lag time, the accuracy of blacklist is not too high.

3.2 Heuristic-based anti-phishing technique, with a high probability of false and failed alarm, and it is easy for the attacker to use technical means to avoid the heuristic characteristics detection.

3.3 Assessment based technique is time-consuming. It needs too long time to calculate a pair of pages, so using the method to detect phishing websites on the client terminal is not suitable. And there is low accuracy rate for this method depends on many factors, such as the text, images, and similarity measurement technique. However, this technique (in particular, image similarity identification technique) is not perfect enough yet.

Thus there are various methods present in online manipulations for making the systems safe from these types of attacks. But we can see that they have its own problems, which make it again unsafe. So a system based on visual cryptography that can perform as a new method can overcome these problems effectively.

4. Visual Cryptography

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a technical operation that does not require a computer. One of the best-known techniques has been credited to Moni Naor and Adi Shamir [2], who developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n-1 shares revealed no information about the original image. Each share was printed on a separate transparency, and overlaying the shares performed decryption. When all n shares were overlaid, the original image would appear. Using a similar idea, transparencies can be used to implement a one-time pad encryption, where one transparency is a shared random pad, and another transparency acts as the cipher text.

VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. We can achieve this by one of the following access structure schemes.

1)(2, 2)- Threshold VCS scheme- This is the simplest threshold scheme that takes a secret message and encrypts it in two different shares that reveal the secret image when they are overlaid.
2)(n, n) -Threshold VCS scheme-This scheme encrypts the secret image into n shares such that when all n of the shares are combined will the secret image be revealed.
3)(k, n) Threshold VCS scheme- This scheme encrypts the secret image into n shares such that when any group of at least k shares are overlaid the secret image will be revealed.

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Figure.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 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.

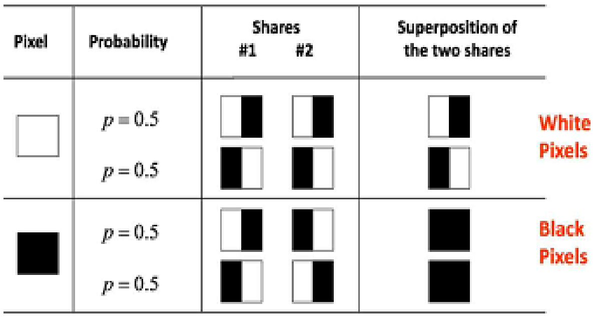


Figure 1: Illustration of a 2-out-of-2 VCS scheme with 2-subpixel construction

5. Current System

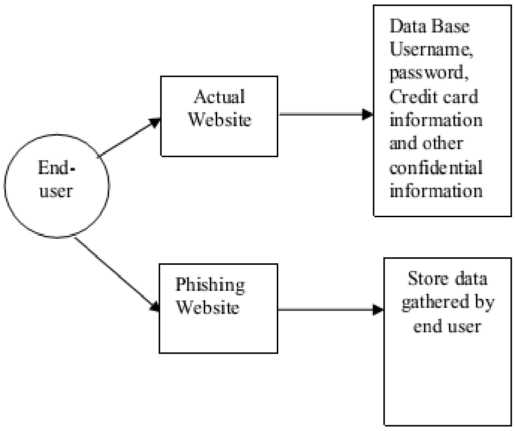

End-user
Actual Website
Data Base Username, password, Credit card information and other confidential information
Phishing Website
Store data gathered by end user

Figure 2: Current scenario

In the current scenario, as shown in the Figure 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 number 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.

6. Proposed Method

The proposed approach can be divided into two phases:

a. Registration Phase
b. Login Phase

6.1 Registration Phase

In the registration phase, a key string (password) is asked to be entered by the user at the time of registration for the secure website. The key string can be a combination of both alphabets and numbers to provide more secure environment for the users. This string entered by the user is concatenated with randomly generated string by the server and an image captcha is generated [3][4]. The image captcha is divided into two shares such that one of the shares is given to the user and the other share is kept in the server. The user's share and the original image captcha are 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. Registration process is depicted in Fig.3

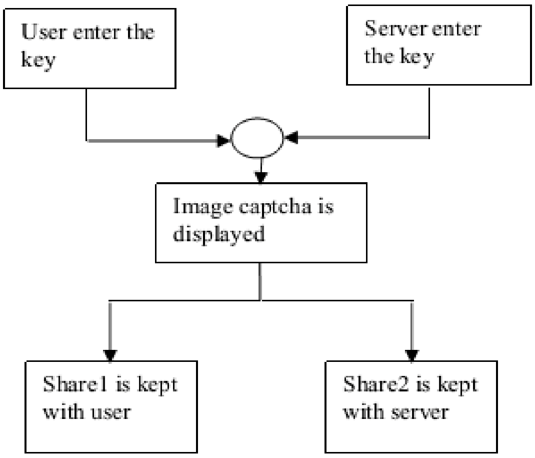


Figure 3: When user performs registration process for the website

6.2 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 generated image captcha is displayed to the user. Here the end user can check whether the displayed image captcha matches with the captcha given to him 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.

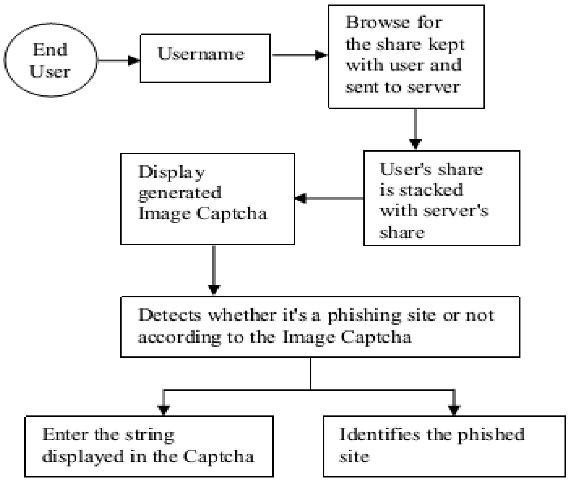

End User
Username
Browse for the share kept with user and sent to server
User's share is stacked with server's share
Display generated Image Captcha
Detects whether it's a phishing site or not according to the Image Captcha
Enter the string displayed in the Captcha
Identifies the phished site

Figure 4: when user attempts to log in into 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

7. Implementation and Analysis

The proposed methodology is implemented using Matlab. The sequence of encryption process (Block transformation, Rotation, and Sub pixel dividence) [5] is depicted in the Fig 5.

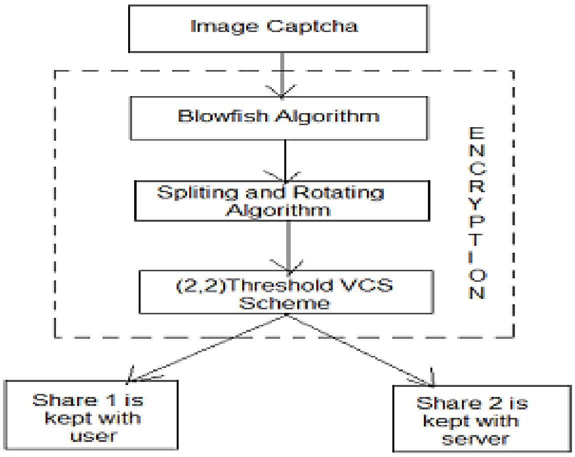


Image Captcha
Blowfish Algorithm
Spliting and Rotating Algorithm
(2,2)Threshold VCS Scheme
ENCRYPTION
Share 1 is kept with user
Share 2 is kept with server

Figure 5: Image Captcha Encryption

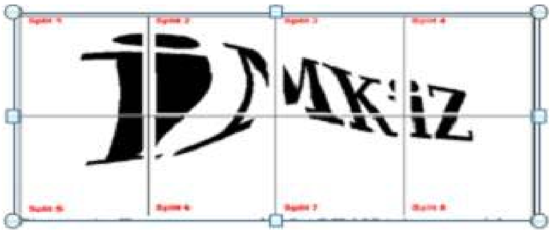


Figure 6: Captcha under blowfish algorithm

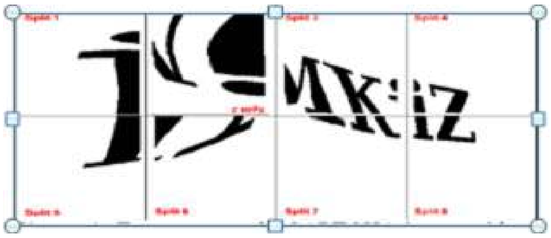


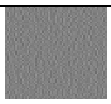
Figure 7: Captcha under splitting and rotating algorithm

Figure 8 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 login into the website.

The entire process is depicted in Fig 6 as different cases. Case 1 illustrates the creation and stacking of shares of two-image captcha's resulting in original captcha. In Case 2 share1 of first image captcha is combined with share2 of second captcha resulting in unrecognizable form of captcha.

Case 1:

Original Captcha	Share 1	Share 2	Reconstructed Captcha
			

Case 2:

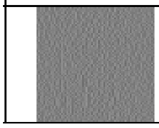
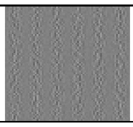
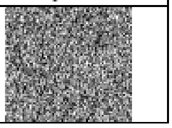
Share 1 of Case1	Share 2 of Case2	Reconstructed Captcha
		

Figure 8: Creation and stacking of shares

8. Results and Discussions

When the image captcha is processed under Blowfish Algorithm, Splitting and Rotating Algorithm and Visual Cryptography (2, 2) scheme the sequence of splitted image captcha, rotated image captcha and the final image captcha shares with difficulty is produced.

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 Figure 9.

Also when two different shares are stacked their corresponding correlation co-efficient is obtained as -0.0073.This shows that there will be zero degree of correlation between original and output images for two different shares. When the two image captcha shares are available then the original image captcha is revealed using the decryption method.

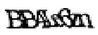
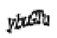
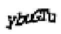
Original Captcha	Reconstructed Captcha	Correlation Coefficient
		0.9679
		0.9598
		0.9627
		0.9578
		0.9657

Figure 9: Correlation coefficient

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. Phished websites as well as human users can be easily identified using the proposed "Anti-phishing using Visual Cryptography". The proposed method maintains confidential information of users using 3 layers of security.

First layer verifies whether the website is a genuine/secure website or a phishing website. If the website is a phishing website, then in that situation, the phishing website can't display the image captcha for that specific user 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.

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

[1] Divya James and Mintu Philip, "A Novel Anti Phishing Framework Based On Visual Cryptography".

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

[3] CAPTCHA:Using Hard AI Problems For Security Luis von Ahn1, Manuel Blum1, Nicholas J. Hopper1, and John Langford.

[4] A Text-Graphics Character CAPTCHA for Password Authentication Matthew Dailey Chanathip Namprempre.

[5] Mrs. A.Angel Freeda, M.Sindhuja, K.Sujitha, "Image Captcha Based Authentication Using Visual Cryptography".

Author Profile

Amit Navarkar pursuing the Bachelor's degree in Engineering from the D Y Patil College of engineering of the University of Pune, Maharashtra, India

Mrs. D. A. Phalke has completed her Masters degree in Computer Engineering from University of Pune and currently working as an Assistant Professor in Computer Department at D Y Patil College of Engineering, Akurdi, Pune, having the total 12 years of teaching experience.