

Visual Secret Sharing For Hacking Prevention

Mrs. Rajashree M Byala,
Asst.Prof,Dept.Information Science Engineering,
East west Institute of Technology,Bangalore,
VTU belguam

Mrs. Ramya Avinash
Mtech in Computer Networks Engineering
East west Institute of Technology,Bangalore,
VTU belguam

Abstract—The various online attacks has been increased with the advent of internet and among them the most popular attack is phishing. An increasingly common form of online theft is the act of tricking computer users into handing over control of their online accounts using, typically, a combination of a forged email and website. In this proposed approach named as “Visual secret sharing for hacking prevention” to solve the problem of phishing. CAPTCHAs (Completely Automated Public Turing tests to tell Computers and Humans Apart) are currently being used to prevent automated bots from registering for email accounts. Visual secret sharing schemes hide the secret image into two or more images which are called shares. The image CAPTCHA privacy is preserved through visual secret sharing by decomposing the original image CAPTCHA into two shares (known as sheets) and these are stored in separate database servers (one with user and one with server) .The identity of the original image CAPTCHA will not be revealed by individual sheet images. Once the original image CAPTCHA is revealed to the user it can be used as the password and this method can be used by website to cross verify its identity and prove that it is a genuine website before the end users.

1. Introduction

Phishing is also known as "brand spoofing". It is pronounced as fishing. The word has its origin from two words “Password harvesting” or “fishing for passwords”. Phishing is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information.

Phishing is a form of online identity theft associated with both social engineering and technical subterfuge. Attackers might send millions of fraudulent e-mail messages that appear to come from Web sites you trust, like your bank or credit card Company, and request that

you provide personal information. As scam artists become more sophisticated, so do their phishing e-mail messages and pop-up windows, they often include official-looking logos from real organizations and other identifying information taken directly from legitimate Web sites. When users unwittingly browse phishing pages and enter their personal information like user name and password their password will get stored in the attackers database and then users are redirected to original sites directly by way of phisher-controlled proxies.

Phishing has thus become a serious threat to information security and Internet privacy [16]. To deceive users into thinking phishing sites are legitimate, fake pages are often designed to look almost the same as the official ones in both layout and content. Phishers might insert an arbitrary advertisement banner that redirects users to another malicious Web site if they click on it.

So, phishing attacks have become a serious threat.If a user finds that the page he visits is a phishing page then he can report it to the APWG [10]. They will add that page in the list of phishing page. First to find whether the page is a phishing page or real page, we’ve developed a image based Authentication using visual cryptography.

Nowadays, the phishing attack has become a bigger problem. It results in stealing One’s personal information like Gmail account and bank password. To avoid phishing attacks many methods are developed, but none of the method is more efficient enough to solve such this kind of problems and still the phishing attacks takes place. The method that we developed here is purely image based.

1.1 A Growing Problems in Phishing

The phish attack volume increased 33% in April to 36,557 attacks, continuing the growth trend from March. Phish attacks had been in general decline from August 2009 to February 2010, but now look set to

return to the seasonal growth trend that has historically peaked in late Summer/early Fall [9].

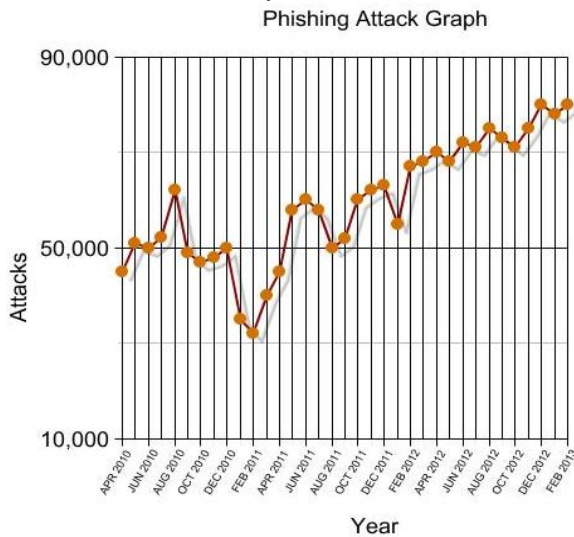


Fig 1: Monthly Phishing Attack

In August 2009, for example, the high point of fast-flux phish attacks Produced 60,678 incidents. As shown in Figure. 1, the monthly attacks from April 2009 to April 2010 averaged 45,605.

1.2 Phishing Attack

Employ visual elements from target site. Most methods of phishing use some form of technical deception designed to make a link in an e-mail (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by phishers [11]. Example: www.gmail.com – original link, www.gmai1.com – Fake link. Here are a few phrases that a phishing page may contain verify your account, businesses should not ask you to send passwords, login names, social security numbers, or other personal information through e-mail.

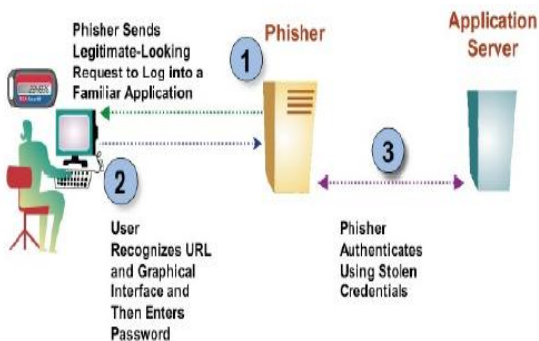


Fig 2: Phishing Attack

From the Figure.2, if you receive an e-mail from anyone asking you to update your credit card information, do not respond, this is a phishing scam. If you don't respond within 48 hours, your account will be closed. These messages convey a sense of urgency so that you will respond immediately without thinking. In the Figure.3, the phishing e-mail might even claim that your response is required because your account might have been compromised [3].

In general, phishing attacks are performed with the following four steps:

- 1) A fake web site which looks exactly like the legitimate Web site is set up by phisher
- 2) Phisher then send link to the fake web site in large amount of spoofed e-mails to target users in the name of legitimate companies and organizations, trying to convince the potential victims to visit their web sites.
- 3) Victims visit the fake web site by clicking on the link and input its useful information there.
- 4) Phishers then steal the personal information and perform their fraud such as transferring money from the victims' account.

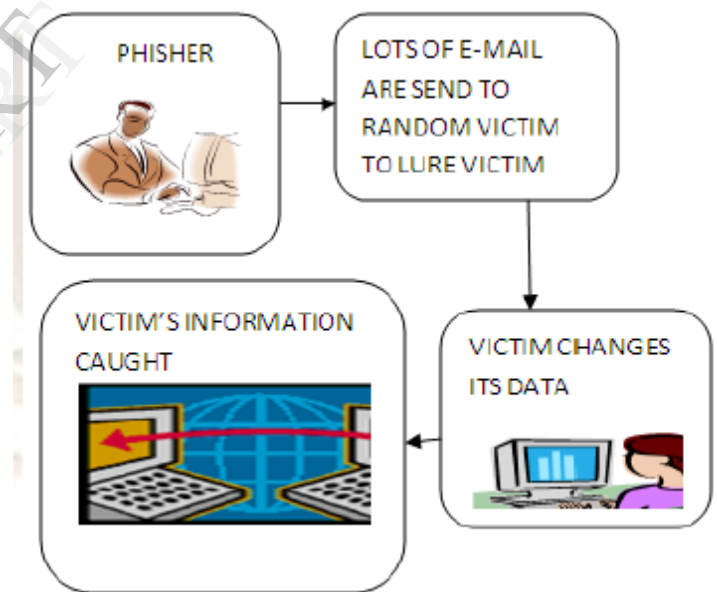


Fig 3: Process of phishing

There are thousands of fake phishing websites established online every day, luring a number of customers. According to a phishing activity trend report published by Anti-phishing working group on 23 dec 2011, a lot of phishing attacks were done in first half of year 2011 as can be seen from fig 1. The number of unique phishing reports submitted to APWG in 2011 reached a high of 26,402 in March, dropping to the half year low of 20,908 in April.

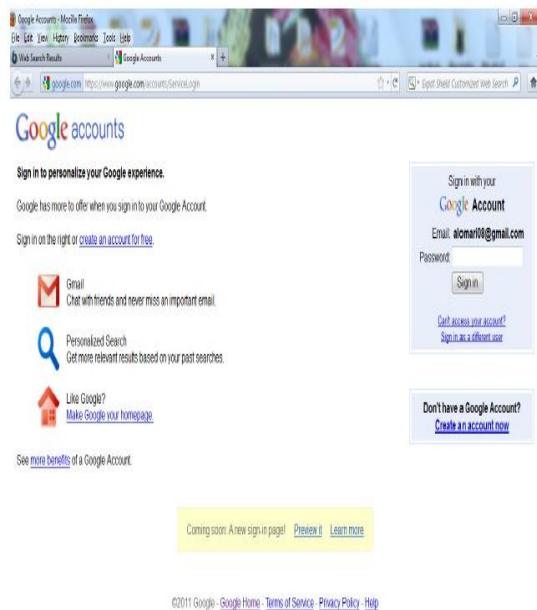


Fig 4: Phishing page

The use of image and video applications has increased dramatically in recent years. When communication bandwidth or storage is limited, data is often compressed. Especially when wireless network is used, low bit rate compression algorithms are needed because of limited bandwidth.

On the other hand, encryption operation is also performed if it is necessary to protect information. Traditionally, an appropriate compression algorithm is applied to multimedia data and its output is encrypted by an independent encryption algorithm. This process must then be reversed by decoder. The processing time for encryption and decryption is a major bottleneck in real time image communication and processing. Along with that processing time required for compression and decompression is also important. The computational overhead incurred by encryption and decryption algorithms makes it impossible to handle tremendous amount of data processed [1], [2].

The above page looks like an original Gmail page. But it is a phishing page. Whenever this type of page appears before a user then the user enters the user name and password which gets stored in the attackers database. This type of attack will be a serious one if the attacker steals the user's bank user name and password and misuse it. The methodology and approaches of phishing attacks are discussed in section 3.

2. Related work

In a SOPHOS white paper-2005, Phish Guru is an embedded training system that teaches users to avoid falling for phishing attacks by sending them simulated phishing emails. People access these training emails in their inbox when they check their regular email.

The training emails look just like phishing emails, urging people to go to some website and login. If people fall for the training email that is, if they click on a link in that email. We provide an intervention message that explains that they are at risk for phishing attacks and offers tips they can follow to protect themselves. The training materials present the user with a comic strip that defines phishing, offers steps the user can follow to avoid falling for phishing attacks, and illustrates how easy it is for criminals to perpetrate such attacks [2].

Defending the weakest link, phishing websites detection by analyzing user behaviors, we have used a novel paradigm analysis of the users' behaviors to detect phishing websites. We have shown that it is an accurate method, discussed how it has been designed and implemented to be hard to circumvent, and have discussed its unique strength in protecting users from phishing threats. UBPD is not designed to replace existing techniques. We believe our approach fills a significant gap in current anti-phishing technology capability.

The image authentication a fundamental problem in computer vision. The existing prevention and detection schemes to combat Phishing in multiple ways. The endless competition between computer virus writers and antivirus software developers, phishers will certainly strive to develop countermeasures against antiphishing solutions. In the existing content-based approach, this analyzes the HTML code and text on a webpage, proved effective in detecting phishing pages. However, phishers responded by compiling phishing pages with non-HTML components, such as images, flash objects, and Java applets. The existing system phisher may design a fake page which is composed entirely of images, even if the original page only contains text information. In this case, the suspect page becomes unanalyzable by content based anti-phishing tools as its HTML code contains nothing but HTML elements [6]. The drawback of existing systems are ineffective to stop phishing attacks, low degree of accuracy, high error rates, not susceptible to changes in webpage aspect ratio and colors used.

In this paper we proposed detecting phishing pages based on the similarity between the phishing and authentic pages at the visual appearance level, instead of rather than using text-based analysis.

We proposed detecting phishing pages for Open System and Closed System. In Open System user has to register in that website and in closed system admin his going to register in that website, then user can login by using that password. Our scheme can detect phishing pages with a high degree of accuracy.

2.1 Proposed Solution

Phishing attack has become a serious threat to internet users. It results in stealing one's personal information like Gmail password, bank password, etc. It is an illegal way. To reduce phishing attacks there are many methods developed to avoid phishing attack. The method proposed here is very different. It's purely based on image comparison rather dealing with old text based analysis anti-phishing mechanism. The main objective of the project is to prevent phishing attacks. To make Online Banking and transaction of money more secured and to provide secure election voting system. To prevent the users of gmail, rapidshare, paypal, ebay, etc. getting hacked. To prevent the users loss of data in Internet.

2.2 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 [2] introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations. A brief survey of the related work in the area of visual cryptography is presented. Visual cryptography schemes were independently introduced by Shamir [3] and Blakley [4], their original motivation was to safeguard cryptographic keys from loss. These schemes also have been widely employed in the construction of several types of cryptographic protocols [5] and consequently, they have many applications in different areas such as access control, opening a bank vault, opening a safety deposit box, or even launching of missiles. A segment based visual cryptography suggested by Borchert [6] can be used only to encrypt the messages containing symbols, especially numbers like bank account number, amount etc. The VCS proposed by Wei-Qi Yan et al., [7] can be applied only for printed text or image.

A recursive VC method proposed by Monoth et al., [8] is computationally complex as the encoded shares are further encoded into number of sub-shares recursively.

Similarly a technique proposed by Kim et al., [9] also suffers from computational complexity, though it avoids dithering of the pixels.

Most of the previous research work on VC focused on improving two parameters: pixel expansion and contrast [10],[11],[12]. In these cases all participants who hold shares are assumed to be honest, that is, they will not present false or fake shares during the phase of recovering the secret image.

Thus, the image shown on the stacking of shares is considered as the real secret image. But, this may not be true always. So cheating prevention methodologies are introduced by Yan et al., [13], Horng et al., [14] and Hu et al., [15]. But, it is observed in all these methodologies, there is no facility of authentication testing. 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.

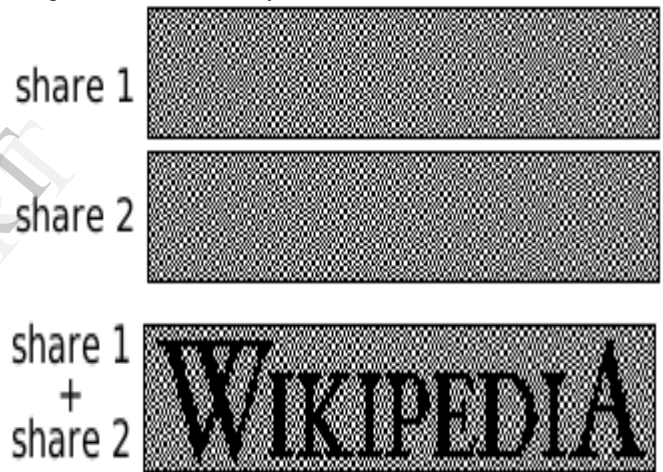


Fig 5: Visual cryptography example

We can achieve this by one of the following access structure schemes.

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 overlaid. No additional information is required to create this kind of access structure.

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

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

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

In the case of (2, 2) VCS, each pixel P in the original image is 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.

Pixel	Probability	Shares		Superposition of the two shares
		#1	#2	
White Pixel	$p = 0.5$	Black	White	White
	$p = 0.5$	White	Black	White
Black Pixel	$p = 0.5$	White	White	Black
	$p = 0.5$	Black	Black	Black

Fig 6: Illustration of a 2-out-of-2 VCS scheme.

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.

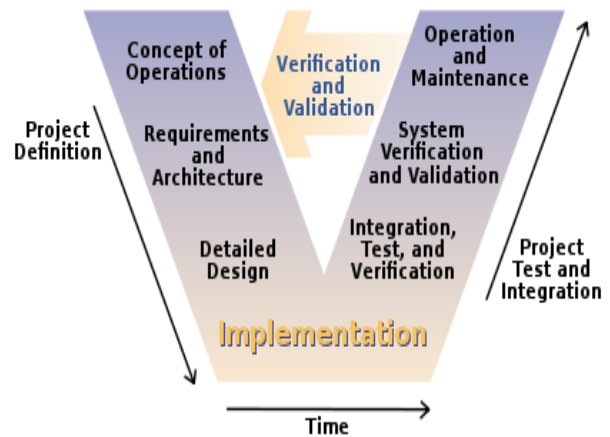
3. Current Methodology

This project is developed as web based application, The architecture used is MVC (Model-View-Controller) 3-Tier Architecture. Technology involved in development is J2EE with JDK 1.6. MyEclipse is IDE (Integrated Development Environment). The Web server is TomCat 6.0.Database used is MySQL 5.0. V-model represents a software development process (also applicable to hardware development) which may be considered an extension of the waterfall model. Instead of moving down in a linear way, the

process steps are bent upwards after the coding phase, to form the typical Vshape.

Trusting User Identity on the internet is quite difficult due to hacking of User identity on the internet. So it is nearly impossible to be sure whether a user connected to the internet is authenticated or not. In Online transaction there is a possibility of encountering forged Identity for transaction. In the Online transaction system, the password of the customer may be hacked and misused. This paper proposes a technique to improve security during transaction. An idea based on Steganography and Visual Cryptography is used. Visual Cryptography introduced by Naor and Shamir [1] is a method used for encrypting a secret image into shares, such that stacking the shares reveals the secret image. The main advantage of Visual Cryptography is the decryption of the message which does not involve more process. The decryption time is very less when Visual Cryptography technique is used. Visual Cryptography is used to check a person for his/her authentication.

Visual Cryptography provides a very powerful technique by which one secret can be distributed in two or more shares. When the shares on transparencies are superimposed exactly together the original secret can be discovered without computer participation.



The V-Model demonstrates the relationships between each phase of the development life cycle and its associated phase of testing. The V represents the sequence of steps in a project life cycle development. It describes the activities to be performed and the results that have to be produced during product development. The left side of the "V" represents the decomposition of requirements, and creation of system specifications. The right side of the V represents integration of parts and their validation.

One Time Password uses information sent in an SMS to the user as part of the login process. One scenario is where a user either registers (or updates) their contact information on a website. During this time the user is also asked to enter his or her regularly used telephone numbers (home, mobile, work, etc). The next time the user logs in to the website, they must enter their username and password; if they enter the correct information, the user then chooses the phone number at which they can be contacted immediately from their previously registered phone numbers. The user will be instantly called or receive an SMS text message with a unique, temporary PIN code. The user then enters this code into the website to prove their identity, and if the PIN code entered is correct, the user will be granted access to their account

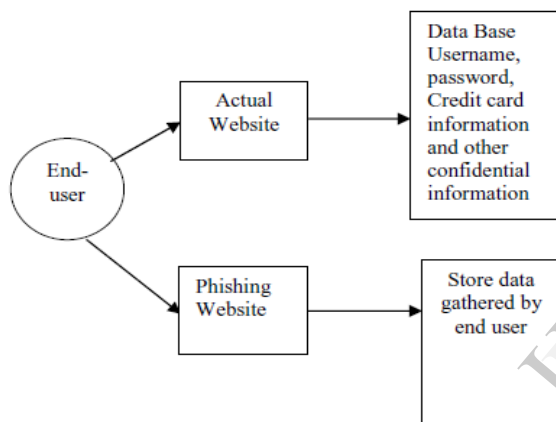


Fig 7: Current scenario

In the current scenario as shown in the Fig 7, 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, 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.

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. Here this methodology is used for both Open System and Closed System. In open System user

is going to register like giving name, password, etc. in the registration phase and then login in to the login phase. In Closed System there is no registration phase for user, admin is going to register like giving name, password, etc. in the admin phase. So in Closed System provides very good security and it prevents password and other confidential information from the phishing websites.

The Open System 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.

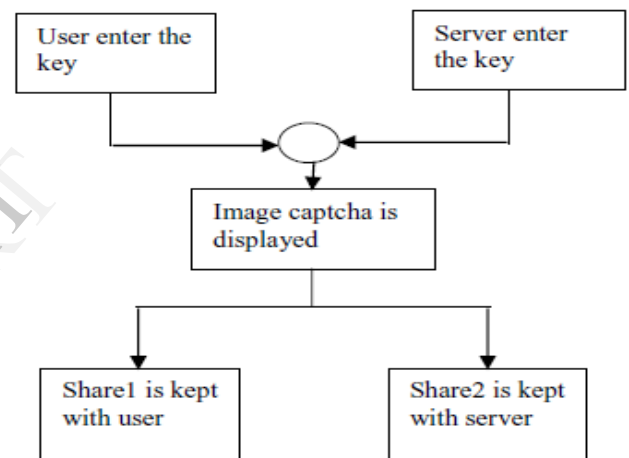


Fig 8: registration process for the website

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 [16][17] 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 the key string when it is needed. Registration process is depicted in Fig.8.

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.

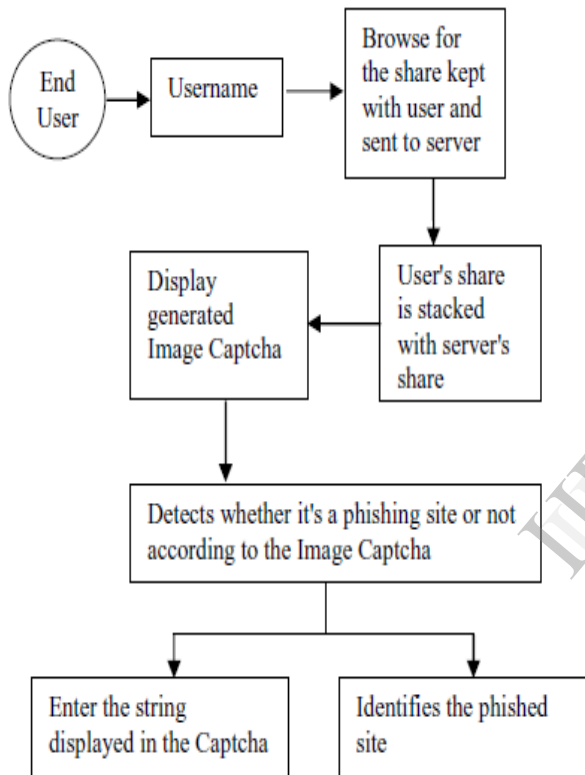


Fig 9: When user attempts to log in into site

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.9.

5. Implementation

The proposed methodology is implemented using Matlab or Java Fig 9, Shows the result of creation and stacking of shares.

The Proposed approach is used for both Open System and Closed system. In Open System user can go and register in the registration phase, then login in to the login phase by using user name and password.

In closed System, admin is going to register in the admin page and that password is divided into two shares. One share i.e share1 is sent to user mail id and another share i.e share2 is kept with server. While user is going to login in login page then merging of shares takeplace.if both matches original captcha is generated other wise user will come to know that this is phishing website.

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.

Case.1

Original Captcha	Share 1	Share 2	Reconstructed Captcha

Case.2

Original Captcha	Share 1	Share 2	Reconstructed Captcha

Case.3











Share 1 of Case1	Share 2 of Case2	Reconstructed Captcha

Fig 10: Creation and stacking of shares

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

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 I. 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.

TABLE I

Original Captcha	Reconstructed Captcha	Correlation Coefficient
		0.9679
		0.9598
		0.9627
		0.9578
		0.9657

Each pixel of the original image will be encoded into n pixels, each of which consists of m subpixels. To share a white (black, resp.) pixel, we randomly choose one of the matrices and distribute row to participant. The chosen matrix defines the subpixels in each of the transparencies. If two captcha same then correlation coefficient is almost 1 is shown in above table.

6. Conclusions

Nowadays, all activities like banking, voting, shopping, etc. are carried out only using internet. There are more chances for the phishers to steal the information from the user. So security plays a major role. This project is developed to prevent attacks like phishing attack. By this attack the attackers steal the

personal information of a user and misuse it. To avoid phishing attack, here we proposed a image based comparison method is developed. To prevent phishing attacks there are methods which are inefficient. All methods uses only text based comparison which is not error free because the attackers has started to insert images which looks similar to that of the original image. So, by text based comparison the difference between the real and the fake page cannot be found.

So, in this project we have developed an image based authentication method.

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. In Future work, can develop a fully automated crawling framework by using attribute-based phishing attacks that developed for testing, along with main experimental results.

7. Acknowledgment

The authors gratefully acknowledge the contributions of M.Naor and A.Shamir for their work in

the field of visual cryptography and also Sincere thank and recognition goes to my advisor, Dr. Suresh M.B,HOD and Rajashree M Byala, Associate Professor,East west Institute of technology, who guided me through this research, inspired and motivated me.

REFERENCES

- [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. Kananahalli, .*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] P. A. Eisen and D. R. Stinson, .*Threshold Visual Cryptography with speci_ed Whiteness Levels of Reconstructed Pixels*., Designs, Codes, Cryptography, vol. 25, no. 1, 2002, pp. 15-61.
- [12] E. R. Verheul and H. C. A. Van Tilborg, .*Constructions and Properties of k out of n Visual Secret Sharing Schemes*., Designs, Codes, Cryptography, vol. 11, no. 2, 1997, pp. 179-196.
- [13] H. Yan, Z. Gan and K. Chen, .*A Cheater Detectable Visual Cryptography Scheme*., *Journal of Shanghai Jiaotong University*, vol. 38, no. 1,2004.
- [14] G. B. Horng, T. G. Chen and D. S. Tsai, .*Cheating in Visual Cryptography*., *Designs, Codes, Cryptography*, vol. 38, no. 2, 2006, pp. 219-236.
- [15] C. M. Hu and W. G. Tzeng, .*Cheating Prevention in Visual Cryptography*., *IEEE Transaction on Image Processing*, vol. 16, no. 1, Jan- 2007,pp. 36-45.
- [16] CAPTCHA:Using Hard AI Problems For Security Luis von Ahn¹, Manuel Blum¹, Nicholas J. Hopper¹, and John Langford.