An Anti Phishing Framework For Blocking Service Attacks Using Visual Cryptography

Mary Ruby Star .A.L. #1, T.Venu *2

Mary Ruby Star .A.L., pursuing M.Tech from Holy Mary Institute of Technology and Science, , Affiliated to JNTU Hyderabad, A.P., India

T. Venu, working as Assistant Professor, at Holy Mary Institute of Technology and Science, , Affiliated to JNTU Hyderabad, A.P., India

***Abstract:*-In today's environment internet communication become a massive in use. Peoples made communication with other people as well as with the business organization through internet. Most of the time they transfer their sensitive information through internet .Sensitive information such as userid, Password, account information, credit card information etc are important information of a person. For getting those sensitive information from internet Fishing become popular in recent time. Fishing is a technique by which an individual or a group of individual can thieve personal confidential information like password, account information etc from unidentified victims for identity information, financial information or for other fraudulent activities on internet. For securing our information from fishing attack we are proposing here a new technique or framework which is based on visual cryptography technique. Visual cryptography is a cryptographic technique which allow information like image, text etc to be made encrypted in such a form and break the image in number of part and each part having its own part of information .These breaked image can be distributed to n number of user and until unless all part of image will not summarized no one can get the information. By using this technique we can pass the sensitive information like password through visual cryptography. In our proposed framework the original image captcha will divided into two parts and each part is stored into different servers such that the original image captcha can be made only when both parts are available, the single part can not create the original image captcha. Once the original image captcha is there then user can use it as the key to his account.**

Keyword:-Thrawrting,Phishing, visual cryptography, image captcha.

I-INTRODUCTION

In current scenario internet become a huge medium for communication. Everyone doing communication through internet. People making personal communication through social websites, banking websites where they transferring their personal information to other side. These personal information contain sensitive data like as their userid,password,banking password, credit card information etc.If these information can theft by other party they can use these information for wrong purpose. it will affect person identity and also can harm their financial wealth.

Fishing becoming a popular technique for thefting that king of sensitive information over internet. Fishing technique will use by attacker to get the authenticate user information over internet and can use for wrong purpose. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. A phishing expedition, like the fishing expedition it's named for, is a speculative venture: the phished puts the lure hoping to fool at least a few of the prey that encounter the bait. Considering all the above threats to electronic users we propose a method that can be used as a secure way to online E-Transactions against phishing named as "A New Framework for Thwarting Phishing attacks based on Visual Cryptography".

Visual cryptography means applying cryptography concepts with images and is a branch of secret sharing key. Here in this VC scheme, a secret image is encoded into transparencies using algorithms, and then the content of each and every transparency is noise-like so that the secret information cannot be retrieved from any one transparency via human visual observation or signal analysis techniques. In general, a - threshold VC scheme has the following properties: The stacking of any out of those VC generated transparencies can reveal the secret by visual perceptions and any other technique, but the stacking this of any or fewer number of transparencies cannot retrieve any information other than thesize of the secret image. Naor and Shamir proposed a – threshold VC scheme based on basis matrices, and the model had been further studied and extended. The related works include the VC schemes based on probabilistic models, general access structures, VC over halftone images, VC for color images, cheating in VC, the general formula of VC schemes, and region incrementing VC. Contrast is one of the important performance metrics VC schemes. Generally, the stacking revelation of the secret with higher contrast represents the better visual qualities, and also therefore with this the stacking secret with high contrast is the goal of pursuit in VC designs. Naor and Shamir define a contrast formula which has been used widely in many more experiments. So by this based on this definition on contrast with, there are many studies we are attempting here to achieve the contrast bound of VC scheme. Moreover, there exist VC related researches using differential definitions of contrast. Another important metric is the pixel expansion denoting the number of sub pixels in transparency used to encode a secret pixel. The minimization of pixel expansions has been investigated in previous studies.

Visual cryptography is similar to image processing, in image processing image is coded or modified in a particular mechanism and send through network, on receiver side it should de-modified in same mechanism to get original image. In this proposed model we are using advanced visual cryptography. Here images are decomposed into two parts one store in network and other sent to user. When recompose the original image these two shares are must be combined together. Visual Cryptography is used for secure communications; the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

II-RELATED WORK

Phishing web sites are making duplicates of web sites that are created by hacking people to catch the content or sensitive information of Web pages of real web sites. Many of this type of web sites have maximum design similarities so that we cannot vitiate them from original sites. Some of the hackers make sites of web pages look exactly like the real ones. Phishes may target to users bank account, password, credit card number, or other important information. They try to trick customers with email and spam messages, man in the middle attacks, installation of key loggers and screen captures.

A. Phishing Technique

Phishing is defined as “The fraudulent practice of sending e-mails purporting to be from legitimate companies in order to induce individuals to reveal personal data”. Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, Emails are most common technique 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. Phishers are targeting the customers of banks and online payment services. Emails, supposedly from the Internal Revenue Service, have been used to glean sensitive data from U.S. taxpayers. While the first such examples were sent indiscriminately in the expectation that some would be received by customers of a given bank or service It will call the get response application which is deployed in the client side. Once the challenge response is validated user credentials and it is validated by server to proceed the transaction. 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 which is called by the browser and third man interruption is impossible.

B. Visual Crptography

Visual cryptography scheme for secretly sharing the data. The major contribution is that the proposed scheme accommodates dynamic changes of users in the group sharing a VC secret. The proposed scheme allows changes of users without regeneration and redistribution of VC transparencies, which reduce the computing and communication resources in accommodating user changes to the experiment. Here scheme is capable of generating all arbitrary number of transparencies and the explicit algorithms are proposed to generate the transparencies. For a group with initial users there , and the proposed Algorithm 1 was explicitly generates for the required transparencies. For newly joining participants, the new transparencies can be explicitly generated by using the Algorithm 2 in our project, and also the newly transparencies will be distributed to the new participants without the need to update the original transparencies that are to be distributed. Then the secondary contribution of experiments in paper is that this paper designs an implementation of VC based on the prospect mold, and the proposed scheme allows the unlimited number of users. For the conventional VC scheme to implement the case, the mathematical manipulations of infinite size of basis matrices and variables are often required, which is computationally prohibitive. Our approach designs an implementation scheme which is capable of producing a finite subset of the complete infinite transparencies through the proposed Algorithms 1 and 2, with computationally feasible operations. We also derive an optimization problem.

When the random image contains truely random pixels it can be seen as a one-time pad system and will offer unbreakable encryption

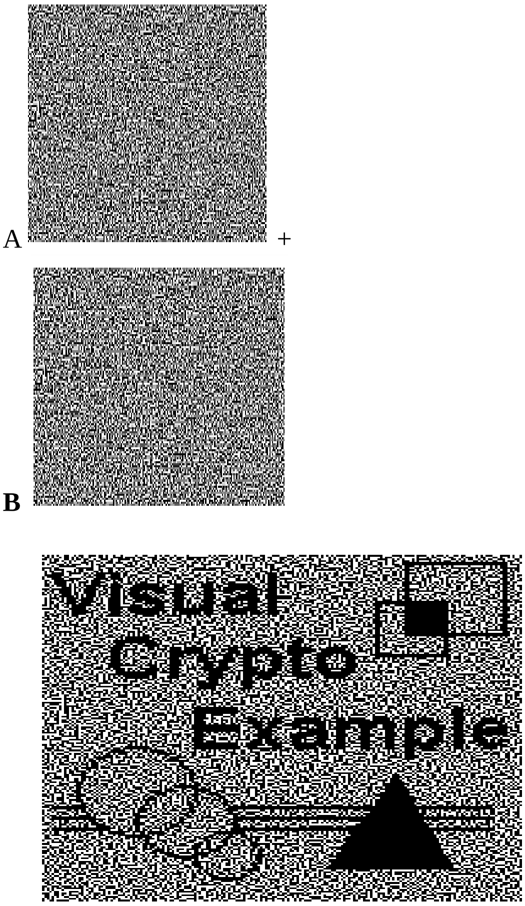

Fig 1-Visual cryptography .

C-Visual cryptography Sharing Scheme

In basis matrix approach the original image is devided into number of transparencies and those transparencies are distributed into user. The user belonging with the dynamic user group . In this group the adding or deletion of user will not make any effect on transparencies. The stacking of transparencies will give the original data . In our approach of basis matrix of(t,n) visual cryptography scheme a white and black secret image has been used which is also known as a binary image or pixel. In the basis matrix approach to make transparencies a binary secret image and each secret pixel will be converted into n blocks at the corresponding position of n transparencies .Each block contain of m sub pixel and each sub pixel is transparent. If any of two sub pixel are stacked with matching position, the representation of stacked pixel will be transparent.

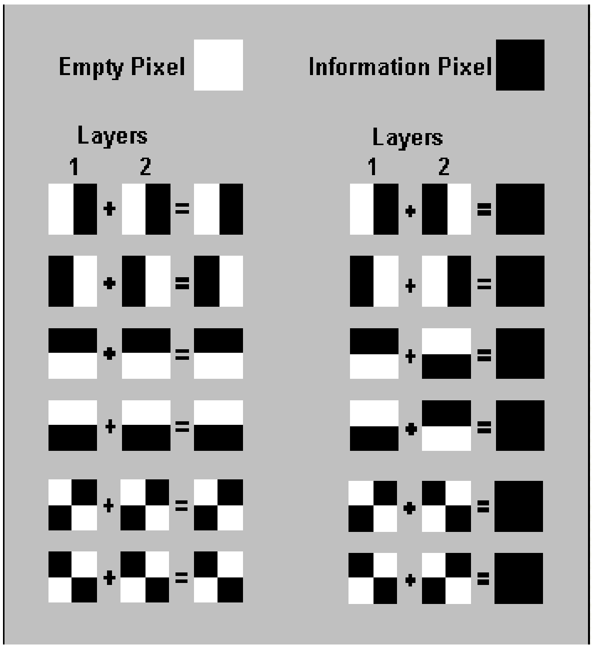

Fig2-Binary matrix image.

III- SYSTEM ARCHITECTURE

In this section we will discuss about the system architecture and implementation which will prevent user sensitive information from fishing attacking wesites.Our system architecture is based on the Anti- fishing Image Captcha validation scheme using visual cryptography. This technique will prevent our sensitive information from the fishing attack. We are dividing our system implementation into two parts-

A-*Image Demodulation:-*

This part is generally implemented at the time of registration or signup process of a site. Here a image which is chosen by a user is uploaded to our anti-phishing mechanism. This image is demodulated using (2,2) visual cryptography sharing scheme. Image is demodulated in such way that when these two demodulated shares are capable of re-construct the original image. In two demodulated shares one is stored at the server and one is sent to the user. The original image is also stored at the server side for further verification process.

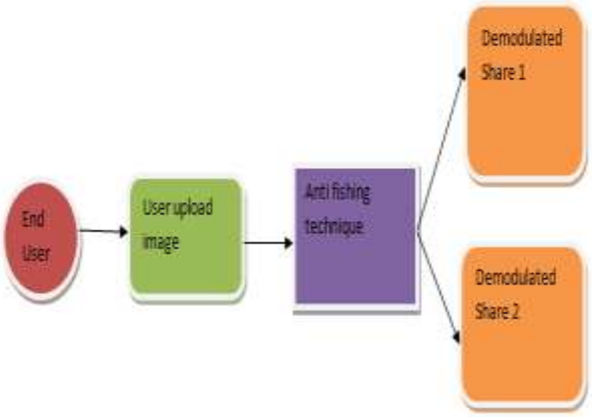

Fig3- Image demodulation using antifishing

B-Image re-Construction Phase

In this part we reconstruct the original image from demodulated shares which are stored at user and server. Based on the user credentials we get the server side stored demodulated image. After entering credentials user prompted for upload his image share which is sent him at the time of image demodulation process. By overlapping these user uploaded and server fetched shared images we construct the original image. If re-constructed image is genuine and matches with the user uploaded image at beginning then user is authenticated other wise he is not authenticated.

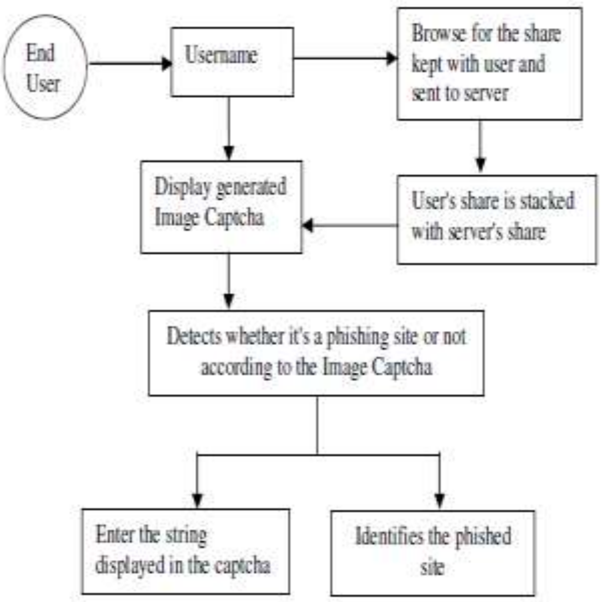
End User
Username
Browse for the share kept with user and sent to server
Display generated Image Captcha
User's share is stacked with server's share
Detects whether it's a phishing site or not according to the Image Captcha
Enter the string displayed in the captcha
Identifies the phished site

Fig 4-Image reconstruction

IV- EXPERIMENTAL EVALUATION

We have performed various test results on our proposed methodology. We sampled some of test results here. We evaluated test results with different types of images. They have shown good results on our methodology. We also performed test with different test cases like matching different image shares, with different image formats. 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. 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.

V-CONCLUSION

Nowadays phishing attacks are become common due to wide range of design and middle ware technologies. It is hard to detect the hackers who are targeted to user personal information like passwords and account information. In most hacking techniques, phishing is the common technique for crack the user passwords and sensitive information. It can attack globally and capture and store the users' confidential information. By using our proposed method Phishing websites as well as human users can be easily identified. The proposed methodology preserves confidential information of users using 2 layers of security. 1st we demodulate the image into two shares such that again these two shares are capable of regenerate the original image. One share send to user while other will store in the server and original image also stored in server side for further verification process. Second, image re construction. In this we will reconstruct the original image with user share and server share and we compare reconstructed image and original image for fishing detection. If in the case of original image and re constructed images are not matched then site is not authenticated. So, using our proposed method, no machine based user can crack the passwords or other confidential information of the users. 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.

REFFERENCE

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.

Nourian, A.; Ishtiaq, S.; Maheswaran, M.; "CASTLE: A social framework for collaborative antiphishing databases", in Proceedings of IEEE- 5th International Conference on CollaborativeComputing:Networking, Applications and Worksharing, 2009.

Sid Stamm, Zulfikar Ramzan, "Drive-By Pharming", v4861 LNCS,p495-506, 2007, Information and Communications Security - 9th International Conference, ICICS 2007, Proceedings.

Anthony Y. Fu, Liu Wenyin, "Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Mover's Distance (EMD)",IEEE Transactions on Dependable and Secure Computing, v 3, n 4, p301-311, October/December 2006.

M. Bose and R. Mukerjee, "Optimal visual cryptographic schemes for general ," *Designs, Codes, Cryptography*.

C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes,".

C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visualcryptography schemes," *J. Cryptology*.

AUTHORS PROFILE

Mary Ruby Star .A.L., pursuing M.Tech from Holy Mary Institute of Technology and Science, Hyderabad, Andhra Pradesh, India, Affiliated to JNTU Hyderabad.

T Venu, working as an Asst. Professor, at Holy Mary Institute of Technology and Science, Hyderabad, Andhra Pradesh, India, Affiliated to JNTU Hyderabad.