ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 3 March 2015, Page No. 11076-11080

A Phishing obligation analysis on web based secure authentication

M.Rajesh M.Tech.,[1] Mr.R.Hariharan M.Tech.,[2]
Student, Department Of
Information Technology, Veltech
Dr.RR& Dr.SR Technical University
Mail id:-rajeshwaran.cool16@gmail.com
Assistant Professor, Department Of
Information Technology, Veltech
.Dr.RR& Dr.SR Technical University.
Mail id:- hharanbtech@gmail.com

ABSTRACT:

Phishing websites is an attempt by an individual or a group to thieve personal confidential information such as the password,credit card information etc from unsuspecting victims for identify theft,the financial gain and other fraudulent activities.Visual cryptography is a special type of secret sharing .in this paper we have proposed a new approach for phishing websites classification to solve the problem of phishing website. Phishing websites comprises a variety of cues within it's the content-parts as well as the browser-based security indicators provided along with the website. The use of images is explored to preserve the privacy of image captcha by decomposing the original image captcha into two shares that are stored in separate database servers such that the original image captcha can be revealed only when both simultaneously available;the individual sheet images do not reveal the identity of the original image captcha. Once original image captcha is revealed to the used as password.Several solutions have proposed to tackle phishing websites.Nevertheless,there is no single magic bullet that can solve this threat radically.Since anti-phishing solutions aim to predict the website class accurately and that exactly matches the data mining classification.The important features that distinguish phishing websites from legitimate ones and assess how good rule-based data mining classification techniques are in predicting phishing websites and which classification technique is proven to be more reliable.

KEY WORDS:- Visual Cryptography, Visual Secret Sharing, Network Security, Error Diffusion, Detecting and Preventing of Attacks.

1.0 INTRODUCTION:

Phishing is a form of online identifies theft that aims to steal sensitive information such as online banking password and credit card information from users. Phishing scams have been receiving the extensive press coverage because such the attacks have been escalating in number and sophistication.

One definition of phishing is given as "it is a criminal activity using social engineering techniques.Phishers is attempt to fraudulently acquires sensitive information, such the passwords and credit card information details, by masquerading as a trustworthy person or business ".Phishing websites attacks rely upon a mix of technical deceit and social engineering practice. In the majority of cases the phisher must be persuade the victim to intentionally perform a series of actions that will provide access to confidential information.

Communication channels such as a email, webpage, IRC and instant messaging services are popular. To the most successful phishing attacks have been initiated by email – where the phisher impersonates the sending authority. In this introduce a new method which can be used as a safe way against phishing which is named as "as a novel approach against Anti-phishing websites using the visual cryptography (VC)". In this approach the website cross verities its own identity and proves that it is a genuine website (to use bank transaction details, E-commerce user and the online booking system etc). Before the end users and make the both sides of the system secure as well as authenticated one. The concept image processing and an improved the visual cryptography is used image processing is a technique of processing input image and to get the output as either improved form of the same image and/or characteristics of the input image. Visual cryptography (VC) is a method of encrypting a secret image to shares, such that stacking a sufficient number of shares reveals the secret image.

2.0 LITERATURE SURVEY:

[1]Gangling Huang, and Anthony Y.Fu deals with how to "**An Anti-phishing Strategy Based on Visual Similarity Assessment"**When the email monitor deployed on a mail server identified a message that contains a keyword requested by a customer,it sends the suspicious and true URLs to the visual similarity assessment module for further investigation. This module extracts the web pages' features and measures the similarity to the true pages according to three metrics:block level (details), layout (global),and style (overall). [2]Haijun Zhang describes"**Textual and Visual Content-Based Anti-phishing: A Bayesian Approach"** Automatically detecting phishing web pages has attracted researcher. It classified into the industrial tool bar based on Anti-phishing, user-interface-based the anti-phishing and web page content-based anti-phishing.[3]In this paper the author Mahmud Khonji, Youssef Iraqi how to **"Phishing Detection:"** A Literature Survey phishing is a social engineering attack that aims at exploiting the weakness found in system processes as caused by system users. A system can be technically secure enough asked password theft, however unaware end usersmay leaktheir passwords if an attacker asked them to update their passwords via a given Hypertext Transfer Protocol (HTTP) link, which ultimately threatens the overall security of the system.[4] Author Wei-Ho Chung **"A Probabilistic Model of (t,n) Visual Cryptography Scheme With Dynamic Group"** The Visual Cryptography (VC) is a secret sharing scheme where a secret image is encoded into n transparencies, and the stacking of any out of the transparencies reveals the secret image. This stacking of(t-1) or fewer transparencies is unable to extract any information about the secret. We discuss traditions and deletions of users in a dynamic user groups. To reduce the overhead of generating and distributing the transparencies in user changes, this paper proposes a (t,n) VC scheme with unlimited n based on the probabilistic model. The proposed scheme is allows n to change dynamically in order to include new the transparencies without regenerating and redistributing the original transparencies.

[5] Author:- Xiaofei Wang, Wanhua Cao and YoupengHaung**"Visual Cryptography for General Access Structure Using Pixel-Block Aware Encoding"** Multi-pixel encoding is an emerging method in visual cryptography for that it can encode more than one pixel for each encoding run. Nevertheless, in fact its encoding efficiency is still low because of that the encoding length is invariable and very small for each run. This paper presents a novel multi-pixel encoding called pixel-block aware encoding to encode for each run. A pixel-block consists of consecutive pixels of same type during the scanning. The proposed scheme has advantage in encoding efficiency over single pixel encoding and other known multi-pixel encoding methods. Furthermore, this scheme can work well for both threshold access structure and general access structure and well for both gray-scale and chromatic images without pixel expansion. These experimental results also show it can achieve good quality foroverlapped images. It can work well for both threshold access structure. It also can achieve good quality for overlapped images and high efficiency for encoding. [6]R.Youmaran, A. Adler, A. Miri**"An Improved Visual Cryptography Scheme for Secret Hiding"**VCryptography is based on cryptography where n images are encoded ina way that only the human visual system can decrypt the hidden message without any cryptography computations when all shares are stacked togethers. This paper presents an improved algorithm based on Chang's and Yu visual cryptography scheme for hiding a colored image into multiple colored cover images. This scheme is achieves lossless recovery and reduces the noise in the cover images without adding any computational complexity.[7]Author:-Carlo Blundo,Stelvio Cimato and Alfredo De Santis1 **"Visual Cryptography Schemes with Optimal Pixel Expansion"** A visual cryptography scheme encodes a black & white secret image into n shadow images called shares which are distributed to the n participants. Such as shares are such that only qualified subsets of participants can "visually" recover the secret image. Usually, the reconstructed image will be darker than the background of the image itself. In such a model the recovered secret image can be darker or lighter than the background.We are prove a lower bound on the pixel expansion of the scheme and for (2,n)-threshold visual cryptography schemes. We provide schemes are achieving the bound. [8] Author:- Neha Gupta **" Journey of VCS from Black and White Images to Colored Images with their Performance Analysis"** Visual Cryptography(VC),emerging technology for secret sharing in which allows visual information (pictures,text,ets.) to be encrypted in such a way that the decryption can be performed by the human vision system(HVS). The originally it was proposed by Naor and Shamir in 1994 for black and white images. This paper is compares and analyzes the performance of various VCS on various parameters such as pixel expansion,contrast,shares generated etc. These compared algorithms came into aura by rectifying limitations of one another.[9] Hsien-Chu Wu, Rui-Wen Yu **"Color Visual Cryptography Scheme Using Meaningful Shares"** Visual cryptography(VC) schemes is hid the secret into two or more images which are called the shares. The secret image can be recovered simply by an stacking the shares together without any complex computation is involved. The shares are very safe because the separately they reveal nothing about the secret image. This paper, a color VC scheme is producing meaningful

shares proposed scheme is utilizes for the halftone technique,cover codingtables and secrets coding table to generate two meaningful shares. The secret image can be decrypted by the stacking two meaningful shares together. Experimental the results have demonstrated that he new scheme is perfectly applicable and achieves a high security level.

3.0 RELATED WORK:

Gangling Huang, and Anthony Y.Fu deals with how to An Anti-phishing Strategy Based on Visual Similarity Assessment When the email monitor deployed on a mail server identified a message that contains a keyword requested by a customer, it sends the suspicious and true URLs to the visual similarity assessment module for further investigation. This module extracts the web pages' features and measures the similarity to the true pages according to three metrics: block level (details), layout (global), and style (overall).

In this paper the author Mahmud Khonji, Youssef Iraqi how to Phishing Detection: A Literature Survey phishing is a social engineering attack that aims at exploiting the weakness found in system processes as caused by system users. A system can be technically secure enough asked password theft, however unaware end users may leak their passwords if an attacker asked them to update their passwords via a given Hypertext Transfer Protocol (HTTP) link, which ultimately threatens the overall security of the system.

Neha Gupta " Journey of VCS from Black and White Images to Colored Images with their Performance Analysis" Visual Cryptography(VC),emerging technology for secret sharing in which allows visual information (pictures,text,ets.) to be encrypted in such a way that the decryption can be performed by the human vision system(HVS). The originally it was proposed by Naor and Shamir in 1994 for black and white images. This paper is compares and analyzes the performance of various VCS on various parameters such as pixel expansion, contrast, shares generated etc. These compared algorithms came into aura by rectifying limitations of one another.

4.0 SOLUTION IMPLEMENTATION:

Detecting an phishing web pages is similar to the problem of detecting duplicate documents and plagiarisms, except that these focus on text-based features in similarity measurements, whereas phishing-page detection should focus more on visual similarities. We've demonstrated experimentally that pure text features are insufficient for detecting phishing pages.

End-users can be educated to better understand the nature of phishing attacks, which ultimately leads them into correctly identifying phishing and non-phishing messages. This is contrary to the categorization in where user training was considered a preventative approach. However, user training approaches aim at enhancing the ability of end-users to detect phishing attacks, and thus we categorize them under "detection".

VC schemes proposed for binary and grayscale images are not suitable for color images due to its various color levels. Some Color VC schemes produces meaningless shares which are vulnerable to suspicion of shares and the pixel value of one share can be determined by scanning the pixel values of another share. Some color VC schemes use complementary meaningful images for share generation which leads to suspicion of secret image and contrast loss in shares as well as decrypted secret image.

This method is use the density of the net dots to simulate the gray level is called "Halftone" and transforms an image with gray level into a binary image before processing. This method re expand every pixel of a color secret image into a 2x2 block in the sharing images and keep two colored and two transparent pixels in the block. Pixel expansion m refers to the number of sub pixels in the generated shares that represents a pixel of the original input image. Smaller pixel expansion results in smaller size of the share. Its represents the loss in resolution from the original picture to the shared one.

In This concept of image processing an improved the visual cryptography is used and the image processing form of the same image and/or characteristics of the input image. In Visual Cryptography (VC) an image is decomposed into shares and in order to reveal the original image appropriate number of shares should be combined. We can achieves this by one of following the access structure schemes.

(2,2) – The 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.

(n.n) – The 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.

(k,n) – The threshold HVCS scheme – This scheme encrypts the secret image to n shares such that when any groups of atleast 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.Denotes the shares of a white pixel and a black pixel. Note that choice of shares for a white and black pixel is randomly determined (there are two choices are available for each pixel).Neither share that provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent the random choices. When the two shares super imposed, then the value of the original pixel P can be determined. If P is black pixel, we have get two black pixels; if it is a white pixel we get one black sub pixel and one white sub pixel.

4.1 ADVANTAGES:

Phishing websites Methodology is based on the Anti-Phishing websites and image validation scheme using visual cryptography.

It is prevents an password and other confidential information from the phishing websites.

URL address is on the address bar of your internet browser begins with “https”; the letter ‘s’ at the end of “https” means ‘secured’.

Look for the padlock symbol is either in the address bar or the status bar (mostly in the address bar) but not within the web page display area. Its verify the security certificate by clicking on the padlock.

Most current anti-phishing strategies focus on the emails that are sent as phishing bait.

Email authentication and spam filtration can help reduce phishing attacks by filtering out messages, but the risk of losing important emails is also high.

Web browsers can use blacklisting to filter against known sites, but there is always latency between site reporting and blacklist updating.

It is possible to construct effective classification models when large data set samples are available.

Without the need of manually analyzing data to discover complex relationships.

ML classifiers can automatically evolve via reinforcement learning.

It is also possible to periodically construct never classification models by simply retraining the learner with updated sample data sets.

Visual information is a original images throughout the color channels and error diffusion generates shares pleasant to human eyes.

Binary and grayscale images are not suitable for color images due to its various color levels.

To construct the color EVC scheme with VIP synchronization and modified threshold error diffusion for visual quality improvement.

Solution of the (2,2) black-and-white VCS scheme by either dividing one pixel into two sub pixels or four sub pixels in the two shares.

Secret sharing improves the reliability and robustness of secure key management.

5.0 PHISHING ARCHITECTURE

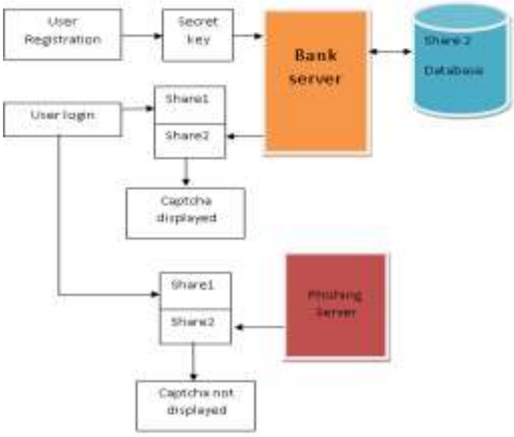

Fig 5.0 Phishing Diagram.

6.0 MODULE S CODES:

6.1 Registration with Secret Code:

In the registration phase, the user details user name, password, email-id, address, and a key string (password) is asked from the user at the time of registration for the secure website. The key string is concatenated with randomly generated string in the server.

6.2 Image Captcha Generation:

A key string is converted into image using java classes Buffered image and Graphics2D. The image dimension is 260*60. Text color is red and the background color is white. Text font is set by Font class in java. After image generation it will be write into the userkey folder in the server using imageIO class.

6.3 Shares Creation (VCS):

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 original image Captcha is sent to the user for later verification during login phase. This image Captcha is also stored in the original database of any confidential website as confidential data.

6.4 Login Phase:

When the user login by entering his information for using his account, the first the user is asked to enter his username (user id). This share is sent to the server, which is stored in the database of the website and it to produce the image captcha.

Here the end user is can check whether the displayed captcha image matches with the captcha created at the time of registration. When the end user is to enter the text displayed in the image captcha and this can serve the purpose of password and usin this, the user can log in into the website. Using the username and image captcha is generated by the two shares key one can verify whether the website is genuine/secure website or a phishing website.

7.0 CONCLUSION:

Online transactions are nowadays become very common. Anti-phishing is online identify theft that aims to steal sensitive information such as online banking password and credit card information from users. Phishing scams have been receiving the extensive press coverage because such the attacks have been escalating in number and sophistication. Phishing "it is a criminal activity using social engineering techniques. Phishers is attempt to fraudulently acquires sensitive information, such the passwords and credit card information details, by masquerading as a trustworthy person or business ".Phishing websites attacks rely upon a mix of technical deceit and social engineering practice. In the majority of cases the phisher must be persuade the victim to intentionally perform a series of actions that will provide access to confidential information.

REFERENCE:-

[1].Wenyin Liu, Xiaotie Deng, Guanglin Huang, and Anthony Y. Fu "An Anti-phishing Strategy Based on Visual Similarity Assessment" IEEE 2006.

[2]. Haijun Zhang, Gang Liu, Tommy W. S. Chow " Textual and Visual Content Based Anti-Phishing: A Bayesian Approach" IEEE 2011.

[3]. Mahmoud Khonji, Youssef Iraqi" Phishing Detection: A Literature Survey" IEEE 2013.

[4]. Sian-Jheng Lin and Wei-Ho Chung" A Probabilistic Model of (t, n) Visual Cryptography Scheme With Dynamic Group" IEEE 2012.

[5]. Haibo Zhang, Xiaofei Wang, Wanhua Cao and Youpeng Huang "Visual Cryptography for General Access Structure Using Pixel-block Aware Encoding" IEEE 2008.

[6]. R.Youmaran, A. Adler, A. Miri "An Improved Visual Cryptography Scheme for Secret Hiding" IEEE 2005.

[7]. Carlo Blundo, Stelvio Cimato and Alfredo De Santis1"Visual Cryptography Schemes with Optimal Pixel Expansion"IEEE 2006.

[8]. Neha Gupta, Manish Gupta, And Abhishek Mishra" Journey of VCS from Black and White Images to Colored Images with their Performance Analysis" IEEE 2013.

[9]. Hsien-Chu Wu, Hao-Cheng Wang, Rui-Wen Yu " Color Visual Cryptography Scheme Using Meaningful Shares" IEEE 2008.

[10]. Siward, "A new (2,n)-visual threshold scheme for color images," in Prof. 4th Int. Con f. Crystal., Dec. 2005, pp. 148–161.

[11]. De Santos, and D. R. Stimson, "Visual cryptography for general access structures," Inf. Com put., vol. 129, no. 2, pp. 86–106, Sept. 1996.

[12]. De Bones, a "Improved schemes for visual cryptography ", Des., Codes Cryptogram., vol. 24, no. 3, pp. 255–278, Dec. 2001.

[13]. C. Bl undo and A. De Santi's, "Visual cryptography schemes with perfect reconstruction of black pixels," J. Compute. Graph. vol. 22, pp. 449–455, Jan. 1998.

[14]. Wagner, "Validating microscopic traffic flow models", in Prof. IEEE TICS, 2006, pp. 1604–1608.