ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Prohibition of Phishing Attacks in Banking using Visual Cryptography and One-Time Password

Harshitha Prem[1], Shalini.J[2], Deepa.D[3], Kapila Vani.R.K[4],

Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India[1,2]

Assistant Professor, Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India[3]

Assistant Professor, Department of Computer Science and Engineering, Prince DR.K Vasudevan college of Engineering and Technology, Chennai, India. [4]

ABSTRACT: The Internet is playing vital role these days in purchasing, selling, learning and in banking. Online Banking is highly popular because of its ease of access. There are also various security threats associated with this and one such risk is phishing. Phishing is a security active attack that attempts to get sensitive information such as pin numbers, credit card details by masquerading as a legitimate entity. To protect the online users from phishing site, we propose a two level of authentication to authenticate a legitimate website. The first level of authentication is through a visual cryptography scheme using linear programming and the next level of authentication by one-time password. Thus, the user will be protected from falling prey to a phishing attack.

KEYWORDS: Image captcha, shares, phishing attack, visual cryptography scheme, linear programming, one-time password.

I. INTRODUCTION

The Internet has become indispensable part of our life. It has simplified our way of living. It made everything as easier and faster so that the world may not wait for anyone. Online transactions have become as trendy and as cashless payments are encouraged many of us are interested in moving towards the digital transaction. In spite of proving ease of payment, tracking of status it has also some pitfalls that are not visible through naked eyes. Phishing is an information breach attack that is usually used against normal people or some targeted ones in order to get their sensitive details that can be sold or can be used in their benefit [1]. The attacker usually masquerades as a legal entity and tries to send e-mails or phone calls for which people can fall as prey.

Now a day, the phishing attacks are increasing day by day and there is also warning from the US-based cyber security firm that there are many identified domains that tries to pass off as payment gateway but which is actually a phishing site[2]. Nearly, 85% and more organizations have suffered because of phishing threats during year 2015 and 2016[3]. According to the most recent Verizon Data Breach Investigations Report, two-thirds of all cyber-espionage-style incidents used phishing as vector [4].The Internet scammers will try to get the information from you by sending you an e-mail which has a URL that might lead to a phishing website. Usually the phishing emails can be identified by some indicators. The indicators [5] are some of them such as general greetings that is, it will not have a specific greeting for the victim, it has a forged link that might look similar to the legitimate URL but actually is not, further it has requested to update your personal details and most important indicator is the sense of urgency to click that link. Similarly the phishing site has become more sophisticated; even they try to place an image in place of secure connection in order to make the site to become similar to the secure website.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

The most common type of phishing is spear phishing. Spear phishing is used mainly in business e-mail compromise [6] (BEC) which is considered as the significant threat in the year 2015-2016. The scam's objective of spear phishing is direct target to acquire your bank details or the business important datasets.

In this paper, we are trying to authenticate the website in two levels using the concept of visual cryptography and one-time password which proves to protect the user against the phishing attack.
The remainder of this paper has the details as follows. We review the background and the related work in section 2. We describe the current methodology in section 3 and then we detail about the proposed methodology in section 4 along with the details of algorithm used, before we conclude in section 6, we describe about results and the discussions in section 5.

II. BACKGROUND AND RELATED WORK

The phishing attacks have interested many people, including the academicians and the researchers as it is a serious security and privacy risk.

A. *Brief History:* phishing attacks were originated around 1995[7] but only after ten years from that the common people came to know about phishing. According to the cyber records the foremost time the word phishing was used in the month of January 1996, this was mentioned in Usenet newsgroups. In 2001, the phishing attackers started to evolve and they reached their peak during 2004. But still the techniques for phishing are growing more and more such that the detection of phishing threat has become a complex task.

B. *Phishing mechanism:* In figure 1, the mechanism of the phishing attack has been explained. The steps of the phishing mechanism is as follows

Step1: The attacker creates a visually similar web page of the legitimate website.
Step 2: In this step he constructs the whole phishing site and host it into a web server.
Step 3: The attackers send an email by showing himself as a legitimate person and he shows the urge to update the details on the website.
Step 4: The victim opens the phishing website and fills all his details.
Step 5: The victim's information is obtain by the attacker from his own dark website.
Step 6: The attacker may use the information obtain to get the legitimate access to the victim's account or he may sell the information he gained.

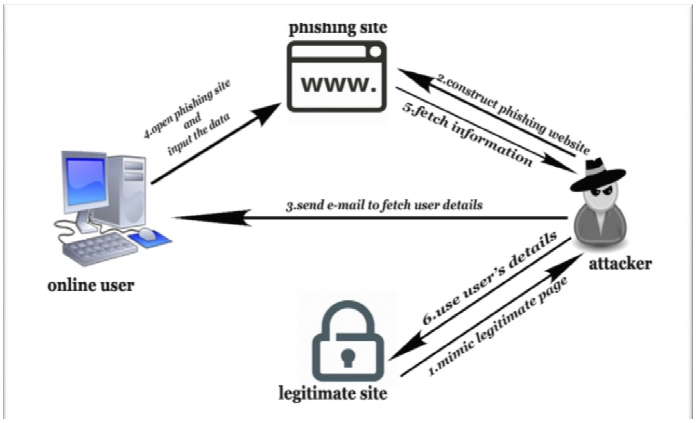

Figure 1.phishing attack mechanism

C. *Types of phishing [8]:* there are several types of phishing the most common six types of phishing are described below

a. *Deceptive Phishing*: in this attack, the attackers used to send an email claiming to come from a recognized source that might ask you to verify your details or re enter the information.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

b. *Spear Phishing*: in this attack, a more sophisticated technology is used so that the specific information of the user can be fetched conveniently.
c. *CEO Fraud*: In this phishing attacker uses an email address similar to that of a legitimate source to request payments, or data from others within the company.
d. *Pharming*: In this fraudsters hijack a website's domain name and use it to redirect visitor to a dark website.
e. *Dropbox Phishing*: a very real looking email that is said to come as a Dropbox request to secure their account is sent to the victim.
f. *Google Docs Phishing*: a message from the Google Docs asks the victim to view that, but the resultant page would be a fraudulent website.

D. *Anti phishing techniques implemented so far:* there are so many anti phishing techniques that are been implemented earlier and a brief about those techniques are described here.

a. *Blacklist based anti phishing* [9]: they contain a blacklist database that contains all the set of URLs that are identified as an illegitimate site. In this technique they cannot detect the websites that are not stored in the database and more over the lifecycle of the phishing website is too small because of which detecting that website and storing it the blacklist fails often.
b. *Heuristic based anti phishing* [10]: this technique tries to identify the fraudulent site by using the URL features and detecting based on the structure of the URL, but unfortunately this technique can be tackled by the attackers if they have good technical knowledge to construct the URL of the illegitimate site.
c. *Visual similarity based approach* [11]: It uses the features of web pages such as the CSS script, HTML tags, images and so forth to decide whether it is a legitimate website or not. This technique is time consuming and has high false rate.
d. *Finding the linchpins in dark web* [12]: it tries to provide security at host level. The objective is to detect the malicious hosts in the cyber space using page rank algorithm [13]. The major drawback is cannot capture the redirection when the attackers uses JavaScript.
e. *Automatically detecting vulnerable websites* [14]: It is used to secure the websites before it gets compromised by using the classifiers. There were many difficulties in building the classifiers and the classifiers also slow the performance of the system.
f. *Black box vulnerability scanner* [15]: It tries to secure the web application in the cyberspace using the scanners. These scanners use modified state change detection algorithm [16]. Unfortunately, it cannot be used in AJAX enabled applications and for public web applications (web application accessed by more than one user at a time).

E. *Visual cryptography:* Cryptography is known as the study of secure communication techniques and also called as cryptology. The importance of cryptography has risen because of various activities carried out in cyberspace, which are virtual and vulnerable to many security attacks. In 1995, Naor and Shamir explored a new way of secret sharing called as Visual Cryptography. In the visual cryptography scheme, a secret image is encrypted as *n* transparencies (called as shares). The secret information cannot be recognized by any one of the single transparency through the human visual system or any signal analysis techniques. The significant characteristic of visual cryptography is that it uses human visual ability as the decoding scheme, instead of using any of the function or devices to decrypt the hidden secret image. There are various ways to construct the visual cryptographic schemes and some of them are listed below.

a. (2,N) Visual Cryptographic Scheme [17]: In this scheme a secret image is decomposed into 2 or more number of shares where each share is random and contains no decipherable data about the secret image. But the research paper entitled as cheating the (2, n) visual cryptographic scheme [18] took advantage of the underlying logic of pixel expansion in shares and proved that the illegitimate share would be created.
b. (R, N) Visual Cryptography Scheme[19]: in this scheme, the designed a r out of n threshold visual cryptographic scheme to encrypt a secret picture into n shares such that the picture can be recognized only when r or more shares are superimposed together, but it cannot be obtained by any group less than r shares in a theoretic senses.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

c. A Probabilistic Model of (R, N) Visual Cryptographic Scheme [20]: in this scheme, only one column of matrices is used to encode a binary secret pixel, instead of the traditional visual cryptographic scheme that utilizes whole basis matrix.

d. Region Incrementing Visual Cryptography [21]: A region incrementing visual cryptography deals with the sharing of images consisting of multiple regions with different secrecy levels, which can be incrementally reveal as the number of share increases. The variant of this scheme uses the integer linear programming algorithm to minimize the pixel expansion of shares. This algorithm is considered to be efficient and feasible; therefore this is used in our paper.

F. *One-time password [23]:* one-time password or abbreviated as OTP is an automatically generated numeric or it contains an alphanumeric string of characters that authenticates the user for a single session. OTP is a form of dynamic password. The reason why it is called as a dynamic password because they are generated on the go and it is valid only for a short period. The remarkable advantage of OTP is that it is not vulnerable to replay attacks because the OTP is valid only for a short duration. There are various ways in which the OTP are generated; the most distinct two approaches are namely time-synchronization between the server and the user's system and using a mathematical algorithm to generate a new secret key based on the previous password to preserve the uniqueness.

III. CURRENT METHODOLOGY

The figure 2 represents the current scenario of how the users may fall prey to a malicious website. In the current scenario the user searches for a website in search engine. Search engine lists a list of links and user enters into that website which may be a phishing site.

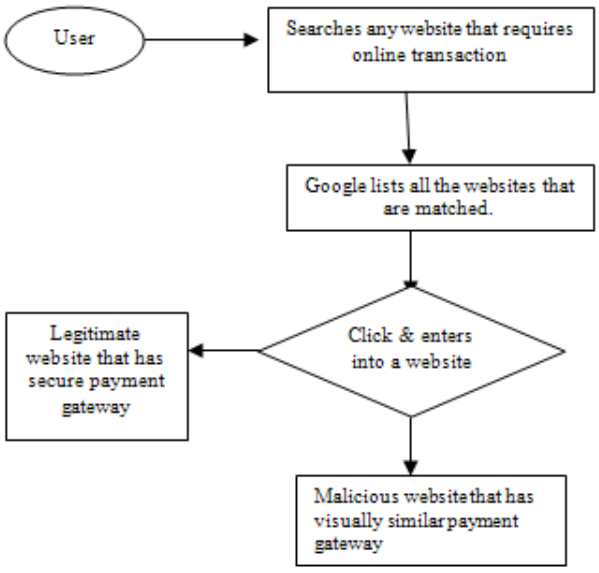

Figure 2: current methodology of accessing the websites.

In the current world, there are n numbers of hidden dangers that are not aware to many of the ordinary users.
There are several hidden dangers such as shoulder surfing[24] attacks, quantum analysis used as cryptanalysis tool to decrypt the secret keys, search redirections, imitating the legitimate website or transaction portal which cannot be detect by the existing defences to malicious activities, virus to corrupt data, key loggers to snoop users password, Trojans etc.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

IV. PROPOSED METHODOLOGY

The objective of our system is to protect the online users from the suspicious and very difficult to detect the phishing attack using the visual cryptography scheme and the one-time password as an additional level authentication to websites.
In this section, we describe in detail about the phases of the system, algorithms used and the system architecture.

Phases of our proposed method:

The proposed system consists of two phases and they are as follows:

a. *Initial captcha generation phase:* The goal of this phase is to generate an image captcha which can be divided as shares and distributed between the user and the server.
b. *Authentication of website along with dynamic OTP*: The goal of this phase is to provide two-level authentication before entering into a legitimate website.

A. *Initial captcha generation:*
Figure 3 shows the sequences that are involved in the initial captcha generation phase.

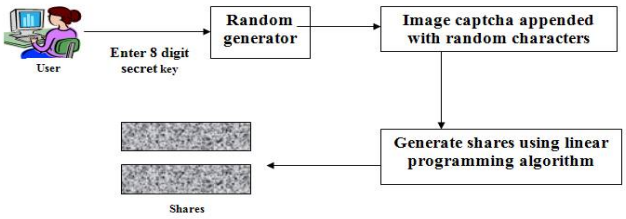

Figure 3: Initial captcha generation phase

The diagram is explained as follows:
In this phase, during registration the user enters the 8 digit secret code that acts as the seed for the random generator. Based on this seed the image captcha is generated. The generated image captcha has the user entered 8 digit code along with the randomly appended characters. This image captcha is then divided into two shares by Visual cryptographic scheme using a linear programming algorithm. The generated shares are randomly distributed between the user and the server. The user can download his share and save it in his system or drive. In order to save his file securely he can use the GNU privacy guard software so that the image file can be securely placed in his system.

B. *Authentication of website along with dynamic OTP:* Figure 4 explains how the authentication of website occurs when the user want to log in to the authenticated website when he wants to do some transactions.

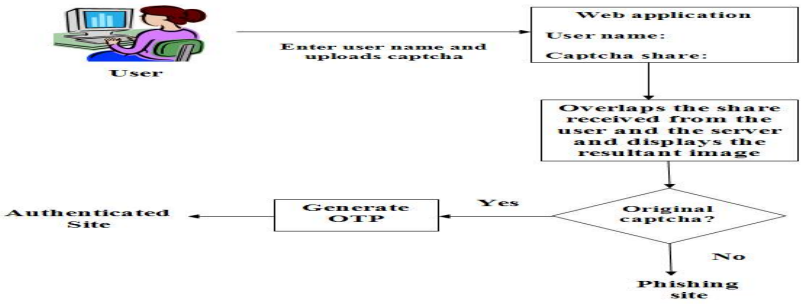

Figure 4: Authentication of website

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

The figure explains about this phase, while accessing any website for transaction the user has to follow the sequences described in the above figure. Initially the user has to enter his username and upload his share of image captcha, and then the server sends its own share of image to the application. By the linear programming algorithm that is through a visual cryptography scheme, both the shares are superimposed on one another to get back the original captcha. The user through his human visual system he decides whether it is original image or not. Once the original image captcha is revealed, a one-time password is sent to the users mobile for additional authentication. Once these authentications are over the user is directed to the legitimate or authenticated website to carry out his transaction.
If the original captcha is not displayed then the user can easily identify that only a malicious website tried to extract his information by masquerading itself as a legitimate source and hence avoid him falling as a prey to the attacker without causing any loss.

Algorithms used:

The algorithms that are mainly used in this paper are region incrementing visual cryptography scheme using linear programming for generating shares with minimized pixel expansion.

A. *Efficient Region incrementing visual cryptography* [26] was first explored by Wang in early 2009. In this scheme for a secret image that has multiple levels of secrecy produces *n* shares such that more shares reveals more regions to eyes.
The encoding ability of visual cryptographic scheme with respect to a secret image *K* could be specified by a set of r x s binary basis matrices B^0 and B^1 for white and black pixel respectively, in K. The basis matrices must meet two requirements: 1) *condition for contrast:* the number of black sub pixels in the result of any *h* rows of B^1 is more than that of the same rows in B^0; and 2) *condition for security:* that of any group less than *h* rows in B^1 is equal to that of the same rows in B^0. To encrypt every pixel in *b* belongs to {0,1} in K, we set C^b=permuted_column(B^b), which permutes columns in B^b randomly, and assign $C^b[a,1]$, $C^b[a,2]$,…, $C^b[a,s]$ as the *s* sub pixels of share a for $1 \le a \le r$ where $C^b[a,b]$ denotes the value of row a and column b in C^b for $1 \le b \le s$.
There are two algorithms used in this scheme, algorithm 1 is used to create the basis matrix depending on the constraints and algorithm 2 is used to create the shares successively.

Algorithm 1

Input: integer t, $r \ge 2$.
Output: t r x s matrices $B^1, B^2, \dots, B^r$ which constitute the basis matrix with minimum pixel expansion s.
Step 1: prepare unit matrices $M_0, M_1, \dots, M_s$.
Step 2: compute A_s, where $A_s[a,b]$=the hamming weight of OR results of any a rows in the b^{th} unit matrix.
Step 3: FOR (each secrecy level i , $1 \le i \le s$) DO
{
Initialize variable vector $Y_i = [y_0, y_1, \dots, y_s]^T$;
Compute $H_i = M_s Y_i$;
}
Step 4: using integer linear program to minimize the pixel expansion using the encoding ability VCS constraints.
Step 5: for each secrecy level i, concatenate the values to the respective basis matrix.
Step 6: output ($B^1, B^2, \dots, B^r$).

Then, we can encode these t regions of the secret image K using the basis matrices that is generated by above algorithm. Note the unit matrices are introduced as the building blocks and the number of the unit matrices is selected from the basis matrices.

Algorithm 2

Input: secret image K containing *r* regions, number of participants *n* and basis matrices ($B^1, B^2, \dots, B^r$).
Output: *n* shares $S_1, S_2, \dots, S_n$ such that each share is a seemingly random picture and any group of *g* shares reveals $K_1, K_2, \dots, K_g$ but conceals $K_{g+1}, K_{g+2}, \dots, K_{g+r}$.
Step 1: FOR every pixel p in K DO

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

{

i = the secrecy level to which p belongs

C^i=permuted_column(B^i);

FOR each share a, $1 \leq a \leq r$ DO

Assign $C^i[a,1]$, $C^i[a,2]$,…, $C^i[a,s]$ as the *s* sub pixels of p corresponding block in share S_a

}

Step 2: output ($S_1, S_2, \ldots, S_n$).

By this we can create shares of the image captcha being generated and here the number of participants n =2 because one of the participants is the user and the other is the server. And this algorithm proves to be efficient than the other visual cryptographic scheme algorithm.

Advantages of this algorithm:

a. It minimizes the pixel expansion with feasible set of basis matrices.
b. The contrasts that are derived are better than the previous approaches.
c. The linear programming formulation makes the implementation easier and feasible.

B.Random generator methods [27]: The secure random class of java is used in the implementation to randomly generate the characters that are to be appended with the secret key given by the user. Secure random algorithms such as Pseudorandom Number Generators (PRNG) are used to generate the One-Time Password. This PRNG along with SHA1 specification indicates that there is no known (or) suspected weakness in the hash based approach for strong cryptographic hash algorithm such as SHA1. SHA1PRNG output is not related with the internal state of the cryptographic hash function. In current world this is known as the most secure random number generator combination that can be used to generate the One-Time Password.

V. RESULTS AND DISCUSSIONS

We have compared our approach with various other visual cryptographic schemes in order to show the worthiness of the considered scheme in table 1.

s. no	Technique	No. of secret shares	Share type	Pixel expansion	Result
1	Visual cryptography scheme(1995)	2	meaningless	4	average
2	3,3 visual secret sharing(2003)	3	meaningless	2	poor
3	2,n region incremental technique	2 or more	meaningless	7	Very poor
4	Our approach using efficient region incremental technique	2 or more	meaningful	1	good

Table 1: comparison of various VCS techniques or schemes

In the proposed cryptographic scheme the pixel expansion is less as well as the contrast of the image is also preserved perfectly therefore this proves to be a efficient scheme than all others scheme considered.

Our technique to prohibit the phishing attack secures users because of the following advantages:

1. Client side prohibition: It saves the user from a compromised server [28] where as the black list approach or the automatic vulnerability detectors cannot find.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

2. Overcomes the drawback/disadvantage of heuristic based techniques that is, even if the phishing URL cannot be detected by heuristic technique, our approach secures user by showing that proper shares are not available.
3. Our approach is faster than the visual similarity based technique because of the visual cryptographic scheme used.
4. Simple and easier to implement where as classifiers in the automatic vulnerability scanners were complex to implement, visual similarity based approach was also complex as it had to consider many features.
5. Prevents user from the available phishing website because it does not consider the scripting language used where as the black box vulnerability scanner cannot support Ajax.
6. It also prevents from redirection attacks because of the concept of shares.
7. It also prevents shoulder surfing attacks, social engineering attacks.

VI. CONCLUSION AND FUTURE WORK

We establish an efficient way of prohibiting the user from getting into a phishing website by making use of concepts of visual cryptographic schemes and the one-time passwords. Since our approach uses a secure random generator it gives a initial level of security to the secret key given by the user and then we are using the novel and innovative way of visual cryptographic scheme using integer linear programming that minimizes the pixel expansion as well as it preserves the contrast of the image captcha and it is easy to be implemented practically. We give the second level authentication through one-time password that would be acting as a shield from replay attacks and as an authenticator. Our paper has some potential future studies. The way to secure the image captcha saved by the user in the system can be improvised as in our proposed system we are using and open source GNU privacy guard software. Also, the improvised version of saving large number images in the sever side can be implemented in the near future using the Big Data concepts in order to remove the scalability problem in the server side.

REFERENCES

1. Rachna Dahamija ,J. D. Tygar and Marti hearst, ”why phishing works” in experimental social science laboratory, 2006
2. “phishing records”,http://timesofindia.indiatimes.com/topic/Phishing
3. “phishing targeted”//www.csoonline.com/article/3048263/security.
4. “spear phishing”, http://resources.infosecinstitute.com/spear-phishing-real-life-examples/#gref
5. ”phishing”, www.phishtank.com/what_is_phishing.php?view=website
6. APWG Q1-Q3 Report, 2015, http://docs.apwg.org/reports/
7. apwg trends report q1-q3 2015.pdf.
8. ”phishing”, http://www.phishing.org/history-of-phishing.
9. ”six common phishing attacks and how to protect against them”, https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/
10. Ma, Justin, et al. "Beyond Blacklists: Learning To Detect Malicious WebSites From Suspicious Urls." 15th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2009
11. Jin-Lee Lee,Dong-Hyun Kim and Chang-Hoon, “Heuristic-Based Approach For Phishing Site Detection Using URL Feautres”, proc. Of the third Intl. conf. on advancein computing,Electronics and electrical technology, CEET-2015.
12. Ankit kumar jain and B. B. Gupta, “Phishing Detection: Analysis Of Visual Similarity Based Approaches”, Hindawi Publishing Corporation Security and Communication Networks,Volume 2017, Article ID 5421046, 20 pages
13. Z. Li, S. Alrwais, Y. Xie, F. Yu, and X. Wang, “Finding The Linchpins Of The Dark Web: A Study On Topologically Dedicated Hosts On Malicious Web Infrastructures,” in 34th IEEE Symposium on Security and Privacy,2013.
14. Z. Gy¨ongyi, H. Garcia-Molina, and J. Pedersen.” COMBATING WEBSPAM WITH TRUSTRANK”. In Proceedings of the Thirtieth internationalconference on Very large data bases - Volume 30,VLDB ’04, pages576–587. VLDB Endowment, 2004.
15. K. Soska and N. Christin, “Automatically Detecting Vulnerable Websites Before They Turn Malicious,” in Proceedings of the 23rd USENIX Security Symposium (USENIX Security’14), San Diego, CA, Aug. 2014, pp. 625–640.
16. L. Invernizzi, P. Comparetti, S. Benvenuti,C. Kruegel, M. Cova, and G. Vigna. “Evilseed: A Guided Approach To Finding Malicious Web Pages”. In Proc. 2012 IEEE Symp. Sec. & Privacy, pages 428–442, San Francisco, CA, May 2012
17. State Change Detection Algorithm ,https://www.arduino.cc/en/Tutorial/StateChangeDetection.
18. M. Naor and A. Shamir, “Visual Cryptography”, Proc. of Advances in Cryptology-EUROCRYPT’94, Springer Berlin Heidelberg, pp.1–12, 1995
19. C. Blundo, A. De Santis and D.R. Stinson, “On The Contrast In Visual Cryptography Schemes”, Journal of Cryptology, Vol.12, No.4, pp.261–289, 1999.
20. H. Koga, “A General Formula Of The -Threshold Visual Secret Sharing Scheme,” in Proc. 8th Int. Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, Dec. 2002, pp. 328–345.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

21. S. Cimato, R. De Prisco, and A. De Santis, "Probabilistic Visual Cryptography Schemes," Computer J., vol. 49, no. 1, pp. 97–107, Jan. 2006.
22. R. Z. Wang, "Region Incrementing Visual Cryptography," IEEE Signal Process. Lett., vol. 16, no. 8, pp. 659–662, Aug. 2009.
23. S.J. Shyu and H.W. Jiang, "Efficient Construction For Contrast Visual Cryptography", IEEE Transactions on Circuits and Systems for Video Technology, Vol.22, No.5, pp.769–777, 2012.
24. "one-time password", https://en.wikipedia.org/wiki/One-time_password.
25. "what is shoulder surfing", http://searchsecurity.techtarget.com/definition/shoulder-surfing.
26. "PayPal phishing scam", http://www.phishing.org/scams/paypal-phishing/
27. LI Shundong, LI Jiliang and WANG Daoshum, "Region Incrementing Visual Cryptography Scheme With Same Contrast", Chinese journal of Electronics,volume 25,No. 4,july 2016.
28. Marie Vasek, John Wadleigh and Tyler Moore,"Hacking is not random:a case control study of webserver-compromise risk", IEEE Transactions on Dependable and Secure Computing, 2016

BIOGRAPHY

Harshitha Prem is a student doing B.E degree in computer science and engineering in Prince shri venkateshwara padmavathy Engineering college, Chennai. Her research interest includes Cryptography, network security, cyber security.

Shalini.J is a student doing B.E degree in computer science and engineering in Prince shri venkateshwara padmavathy Engineering college, Chennai. Her research interest includes visual cryptography, information security.

Deepa. D is an assistant professor in computer science department at Prince Shri Venkateshwara padmavathy Engineering college, Chennai. She is a M.E graduate. Her research interest includes computer graphics, internet programming, mobile computing.

Kapila Vani. R. K. as Assistant Professor in computer science department at Prince Dr.K vasudevan College of Engineering and Technology,Chennai. She is a M.E graduate. Her research interest includes compiler design, Theory of computation and Software project management.