Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 3, March - 2018

Extended Visual Cryptography and QR code Techniques for Online Fraud Transaction prevention

Gulnaaz Rafiq Pathan[1], Amey Ravindra Godbole[2], Kajal Pramod Chaudhari[3], Priti Jagannath Pawara[4]

Guided by: Prof. B. R. Quazi[5]

[12345] Computer Department, *AISSMS COE Pune, Maharashtra, India.*

Abstract —***With the advent of internet, various on-line attacks have been increased and among them, the most well-liked attack is phishing. Phishing is a trial by an individual or a group to get personal confidential information like passwords, credit information from unsuspecting victims for identity theft, financial gain and different fraudulent activities, by simulation to be a trustworthy entity. Victims are tricked into providing such data by a combination of spoofing techniques and social engineering. Visual Cryptography (VC) is used. Visual cryptography is explored to convert the QR code into two shares and both these shares will then be transmitted separately. One time Passwords (OTP) is passwords that are valid just for a session to validate the user within a fixed amount of time. Here an image based mostly authentication using Visual Cryptography is implemented with the combination of OTP (One Time Password). The use of visual cryptography is explored to preserve the privacy of a picture captcha by moldering the original image captcha into two shares. the initial image is obtained at the user finish only once both the user and the server under test are registered with the trusted server.***

Keywords-component; Phishing, visual cryptography, shares, OTP.

I. INTRODUCTION

Phishing is analogous to fishing in a lake, however rather than attempting to capture fish; phishers plan to steal your personal data. It are often an act of sending email that falsely claims to be from a legitimate organization or websites like eBay, Flipkart, or alternative banking establishments. This can be sometimes combined with a threat or request for information: for example, that an account will close, a balance is due, or data is missing from an account. The e-mail can ask the recipient to provide guidance, like checking account details, PINs or passwords; the owners of the web site to conduct fraud then use these details. Some e-mails can ask that you simply enter even additional data, like your full name, address, phone number, Social Security number, and credit card number. However, although you visit the false web site and simply enter your username and password, the phisher is also ready to gain access to more information by simply logging in to your account.

Communications purporting to be from well-liked social internet sites, auction sites, banks, on-line payment processors or IT administrators are usually wont to lure unsuspecting public. Phishing emails might contain links to websites that infected with malware. Phishing is often meted out by email spoofing or instant messaging. Phishing (Ollmann G, 2004) may be a continual threat that keeps growing to the present day.

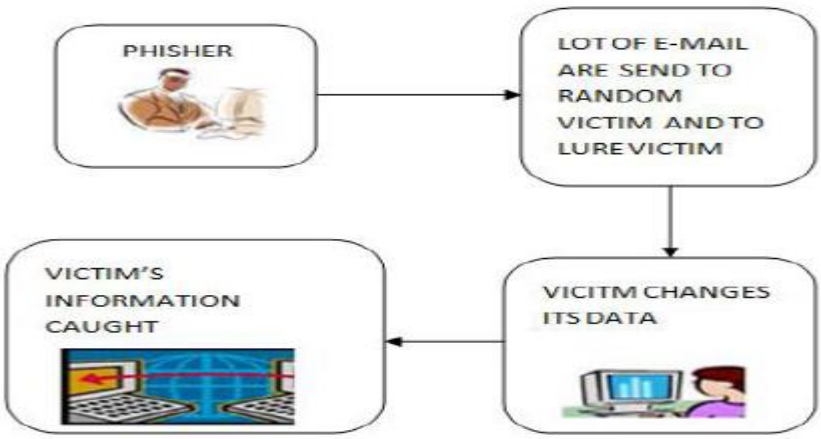

Figure 1 Phishing Process

The risk grows even larger in social media like Facebook, Twitter, and Myspace *Corresponding author: Manisha Bhat etc. Hackers usually use these sites to attack persons using these media sites in their workplace, homes, or public so as to require personal and security information that may have an effect on the user and also the company (if in a very

workplace environment). Phishing (Xiaoqing GU et al, 2013) is employed to portray trust within the user since you will sometimes not tell that the location or program being visited/ used is not real, and once this happens, is once the hacker has the prospect to access the non-public data like passwords, usernames, security codes, and MasterCard numbers among alternative things.
So here, we have a tendency to introduce a replacement methodology, which may be used as a secure approach against phishing. During this approach, web site cross verifies its own identity and proves that it is a real web site (to use bank transaction, E-commerce and on-line booking system etc.) before the top users and build the each sides of the system secure additionally as an authenticated one. The concept of OTP is used for the aim of randomness and time-out session that strengthens the security. This OTP is built into an image. Visual Cryptography (VC) is used here to divide the image into shares and to reveal the initial image, appropriate number of shares should be combined.

Visual Cryptography:
Visual Cryptography is a special encryption technique to hide information in images in such some way that it may be decrypted by the human vision if the proper key image is employed. Naor and Shamir planned the technique in 1994. Visual Cryptography uses two transparent images. One image contains random pixels and the alternative image contains the key info. It is impossible to retrieve the secret info from one of the images. Each clear pictures or layers are needed to reveal the knowledge. The simplest thanks to implement Visual Cryptography is to print the two layers onto a transparent sheet.
When the random image contains truly random pixels it may be seen as a one-time pad system and can supply unbreakable encryption. in the overlay animation you'll observe the two layers sliding over each other until they're properly aligned and also the hidden information appears. To try this yourself, you will copy the instance layers one and a couple of, and print them onto a transparent sheet or thin paper. Always use a program that displays the black and white pixels properly and set the printer so all pixels are printed accurate (no diffusion or photo enhancing etc). you'll also copy and paste them on one another in a drawing program like paint and see the result right away, however make sure to select clear drawing and align both layers exactly over each other.

In example, the image has been split into two component images. Each component image has a pair of pixels for every pixel in the original image. These pixel pairs are shaded black or white according to the following rule: if the original image pixel was black, the pixel pairs in the component images must be complementary; randomly shade one ■□, and the other □■. When these complementary pairs are overlapped, they will appear dark gray. On the other hand, if the original image pixel was white, the pixel pairs in the component images must match both ■□ or both □■. When these matching pairs are overlapped, they will appear light gray.
Therefore, when the two component images are superimposed, the original image appears. However, considered by itself, a component image reveals no information about the original image; it is indistinguishable from a random pattern of ■□ / □■ pairs. Moreover, if you have one component image, you can use the shading rules above to produce a counterfeit component image that combines with it to produce any image at all.

Figure 2 Component Image

Figure 3 Result Image

One-time positive identification (OTP):
One-time positive identification (OTP) may be a positive identification that is valid for under one login session or group action. OTPs avoid variety of shortcomings that area unit related to ancient (static) passwords. The foremost necessary defect that's self-addressed by OTPs is that, in distinction to static passwords, they're not liable to replay attacks. This

implies that a possible entrant WHO manages to record associate degree OTP that was already wont to log into a service or to conduct a group action will not be able to abuse it, since it will be not valid. On the drawback, OTPs have to be compelled to be delivered to the user as and once generated.

OTP (Himika Parmar et al, 2012) generation algorithms usually create use of pseudo-randomness or randomness. This is often necessary as a result; of otherwise it would be straightforward to predict future OTPs by perceptive previous ones. Concrete OTP algorithms vary greatly in their details. Varied approaches for the generation of OTPs area unit listed below:

A. Supported time-synchronization between the authentication server and also the shopper providing the positive identification (OTPs area unit valid just for a brief amount of time).
B. Employing a mathematical algorithmic rule to come up with a replacement positive identification supported the previous positive identification (OTPs area unit effectively a sequence and should be employed in a predefined order)
C. Employing a mathematical algorithmic rule wherever the new positive identification is predicated on a challenge (e.g., a random variety chosen by the authentication server or group action details) and/or a counter.

II. LITERATURE SURVEY

1) An Efficient Approach for Phishing Website Detection using Visual Cryptography (VC) and Quick Response Code (QR Code):

The proposed system satisfies the high security requirements of the online users and protects them against various security attacks. In addition, the system does not require any technical pre-requisite and this makes it very user-friendly. Hence, QR code proves to be versatile at the same time beneficial for both the customers in terms of security and vendors in terms of increasing their efficiency. In the near future, this work may also be enhanced by taking action on the detected phishing websites.

2) Malicious Website Detection using Visual Cryptography and OTP:

With our proposed methodology "Malicious Website Detection using Visual Cryptography and OTP", we can easily identify the phishing websites. Our proposed technique provides more security as a random OTP is chosen for a particular session and the visual cryptography is done on the authenticated server side. Since the generated shares are valid for a particular session and are not stored on either side i.e. server or user, there is no chance of the share being stolen by any other user. Hence, it provides much better security.

3) Anti-Phishing framework based on Extended Visual Cryptography and QR code:

In this paper, different Online Fraud Transaction prevention system is studied based visual cryptography. From study, we proposed a method for Online Fraud Transaction prevention using EVC and QR code techniques. In previous system cannot verify the shares are genuine or not but by using EVC we can verify the shares and provide better security than previous system. The system provides high security requirements of the online users and protects them against various security attacks. In addition, the system is very user-friendly. It is reliable method for detecting phishing websites.

4) Online Payment System using Steganography and Visual Cryptography:

In this paper, two methods are used such as Steganography and visual Cryptography to provide secure transaction during online shopping. It secure the customer confidential information as well as merchant credential and prevent misuse of data at bank side by Admin Application. . This method is mainly concerned With preventing identity theft and providing customer data security. It also prevents phishing. The system authenticates client as well as merchant server (i.e. two authentication).

III. PROPOSED SYSTEM

Now a day an onIine transaction has become very common. There are various attacks present during the online transaction. Phishing is a very common attack. We propose a new scheme for onIine frauds detection using EVC and QR code. Proposed system is shown in Fig.4. During this system the user registration is finished first. User sends request to merchant server and merchant server sends ID and password to bank server for verification. If it is valid, then generate OTP and apply EVC for shares generation. Bank server sends one share to the client and one share to the server. The merchant server sends this share to the client. At the time of reconstruction, two shares are combined to reveal the original OTP. Then, user sends this OTP to bank server for verification.

For the aim of detecting and preventing phishing, we are proposing new methodology to identify a phishing web site. As per our methodology, first, the user is registered with the trusted server (mostly, a bank server). The user gets his UID at the time of registration. Once the user is with success registered with the trusted server, he can login through the client application. For the verification, he sends his UID to the merchant server. The merchant server sends the server ID, server key and UID to the bank server. The bank server validates these things respectively. If the given data is registered

under the bank server i.e if the main points provided by the merchant server are valid, then the bank server generates associate OTP. This OTP is built into a picture.

Then (2,2) Threshold VCS theme is applied on the image. Share one is distributed to the merchant server and share two is distributed to the user via e-mail. Merchant server sends share one to the user for the verification method. At the user side, share one and share two are unified along to get the image. From this image, user will get the OTP. The user then enters this OTP and validates it with the bank server through the merchant server. If the OTP is valid, the merchant server is authenticated one. Otherwise, the merchant server could be a phishing.

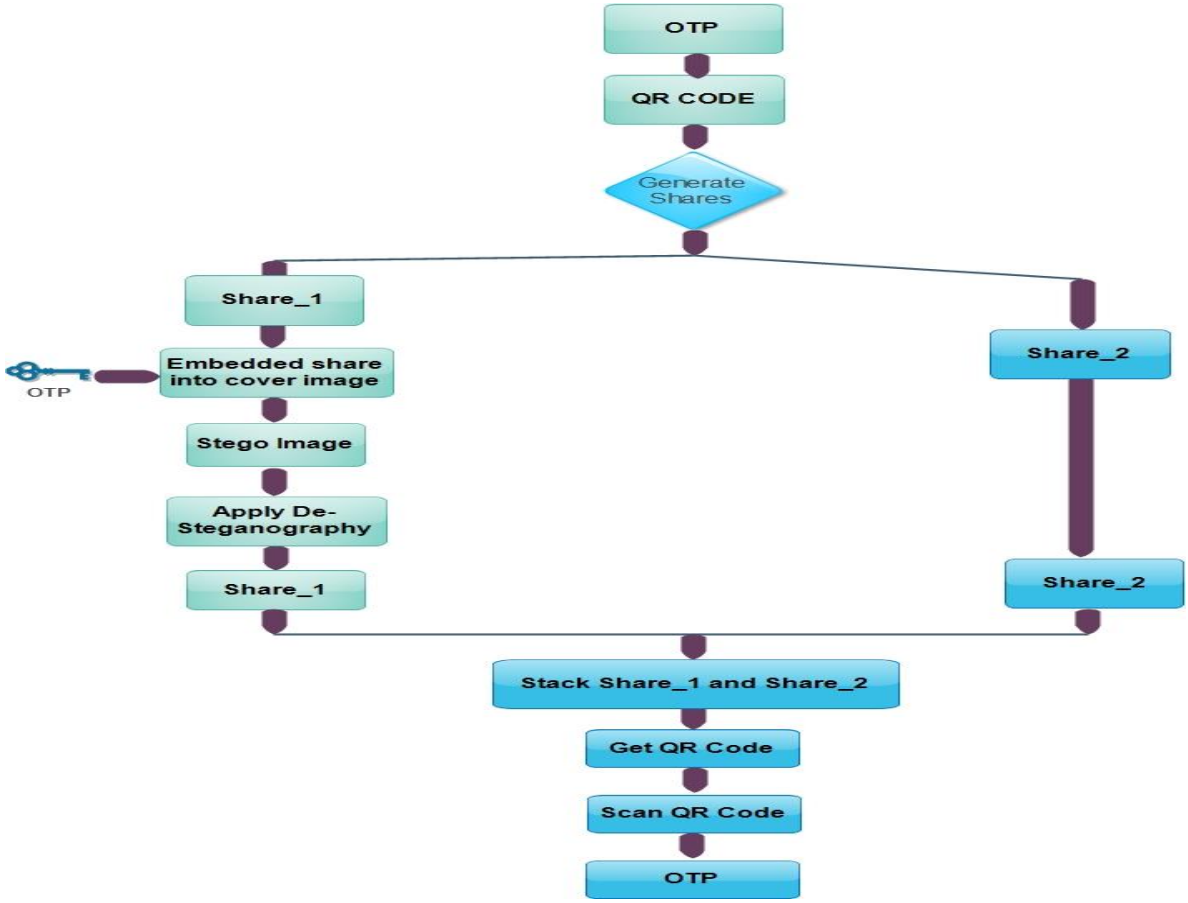

Figure 4 Proposed System

IV. CONCLUSION

Nowadays, due to increase in range of on-line transactions, phishing attacks are getting common to acquire the user's confidential information. The attackers use this data within the phishing attacks. We planned a way for on-line Fraud transaction prevention using EVC and QR code techniques. In previous system cannot verify the shares area unit genuine or not but by using EVC we can verify the shares and supply higher security than previous system. The system provides high security requirements of the web users and protects them against various security attacks. Additionally the system is incredibly easy. It is reliable technique for detecting phishing websites.

REFERENCES

A. Alnajim and M. Munro, "An anti-phishing approach that uses training intervention for Phishing websites detection," in Proceedings of the 2009 Sixth International Conference on Information Technology: New Generations. Washington, DC, USA: IEEE Computer Society, 2009, pp. 405-41 0.

Dhanashree Moholkar ,"An Efficient Approach for Phishing Website Detection using Visual Cryptography (VC) and Quick Response Code (QR Code)", International Journal of Computer Applications (0975 - 8887) Volume 1 15 - No. 12, April 2015.

Divya James, Mintu Philip, "A Novel Anti-Phishing framework based on Visual Cryptography' 978- 1 -4673-0449-8/ 12/$3 1 .00 m0 12 IEEE.

D. R. Anekar, Binay Rana, Vishal Jhangiani," Online Banking Security System Using OTP Encoded in QR-Code ", 2015, IJARCSSE

Gaurav Palande, Shekhar Jadhav," An Enhanced Anti-Phishing Framework Based on Visual Cryptography", International Joumal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3,Issue-3)

Kajal NanawareA, Kirti KanadeA, "Malicious Website Detection using Visual Cryptography and OIP", International Journal of Current Engineering and Technology, Vo1.4, NO.5 (Oct 20 14)

M. Noar, A. Shamir, "Visual cryptography," in: A. De Santis (Ed.),Advance in Cryptography: Eurpocrypt'94, Lecture Notes in Computer Science, Volume. 950, pp. 1 - 12, 1 955.

Souvik Roy and P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography," 20 1 4 IEEE Students' Conference on Electrical, Electronics and Computer Science.