Modern Method for Detecting Web Phishing Using Visual Cryp- tography (VC) and Quick Response Code (QR code)

Sonali Kadam
Bharati Vidyapeeth College of Engineering for Women

RESEARCH ARTICLE OPEN ACCESS

Modern Method for Detecting Web Phishing Using Visual Cryptography (VC) and Quick Response Code (QR code)

Ms. Ashvini Kute[1], Ms. Damini Deokar[2], Ms. Dhanashree Moholkar[3], Ms. Namrata Kadam[4], Prof. Sonali Kadam[5]
Department of Computer Engineering Bharati Vidyapeeth College of Engineering for women, Pune 411043, India.

Abstract
Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information etc from unsuspecting victims for identity theft, financial gain and other fraudulent activities. Here an image based (QR codes) authentication using Visual Cryptography (VC) is used. The use of Visual cryptography is explored to convert the QR code into two shares and both these shares can then be transmitted separately. One Time Passwords (OTP) is passwords which are valid only for a session to validate the user within a specified amount of time. In this paper we are presenting a new authentication scheme for secure OTP distribution in phishing website detection through VC and QR codes.

Keywords- OTP, Phishing, QR code, Shares, Visual Cryptography.

I. INTRODUCTION

Online transactions are nowadays become very common and there are various attacks present behind this. In these types of various attacks, phishing is identified as a major security threat and new innovative ideas are arising with this in each second so preventive mechanism should also be so effective. Thus the security in these cases be very high and should not be easily tractable with implementation easiness.

Phishing is a major security threat to the online community. It is a kind of identity theft that makes use of social engineering skills and technical subterfuge to entice the unsuspecting online consumer to give away their personal information and financial credentials [1].Today, most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, their detection is a difficult problem. As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. Phishing scams are also becoming a problem for online banking and e-commerce users. The question is how to handle applications that require a high level of security. The damage caused by phishing ranges from loss of access to email to substantial financial loss. This style of identity theft is becoming more popular, because of the ease with which unsuspecting people often divulge personal information to phishers, including credit card numbers, social security numbers, and mothers' maiden names. There are also fears that identity thieves can add such information to the knowledge they gain simply by accessing public records. Once this information is acquired, the phishers may use a person's details to create fake accounts in a victim's name, ruin a victim's credit, or even prevent victims from accessing their own accounts. Phishers can deliver specially crafted emails to millions of legitimate email addresses very quickly and can fool the recipients utilising 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. There are DNS-based anti-phishing approach technique which mainly includes blacklists, heuristic detection, the page similarity assessment. But they do have some shortcomings. The life cycle of phishing websites is too short and the establishment of blacklist has a long lag time, the accuracy of blacklist is not too high. In Heuristic-based anti-phishing technique it is easy for the attacker to use technical means to avoid the heuristic characteristics detection. So here we introduce a new method which can be used as a safe way against phishing which is named as "Modern Method for Detecting Web Phishing Using Visual Cryptography (VC) and Quick Response Code (QR code)"As the name describes, in this approach the fake websites are detected using VC and QR codes which let the client differentiate between phishing and legitimate websites.

II. BACKGROUND

QR code (abbreviated from Quick Response Code) is the trademark for a type of matrix barcode (or two-dimensional barcode) first designed for the automotive industry in Japan. A barcode is a machine-readable optical label that contains information about the item to which it is attached. A QR code uses four standardized encoding modes (numeric, alphanumeric, byte / binary, and kanji) to efficiently store data; extensions may also be used.

Uses :- QR codes can be used to log in into websites: a QR Code is shown on the login page on a computer screen, and when a registered user scans it with a verified smart phone, they will automatically be logged in on the computer. Authentication is performed by the smart phone which contacts the server. Google tested such a login method in January 2012. Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. One of the best-known techniques has been credited to Moni Naor and Adi Shamir, who developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. Using a similar idea, transparencies can be used to implement a one-time pad encryption, where one transparency is a shared random pad, and another transparency acts as the cipher text.*Example:* In this 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. So, 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.

III. METHOD

3.1 PROPOSED SYSTEM

In Proposed System Visual Cryptography (VC) and Quick Response Code (QR) codes are merged together. Here anti phishing framework based on visual cryptography and QR code is used to solve the Image based authentication using Visual Cryptography (VC) is used. Visual Cryptography is used to decompose an image (QR) into shares. Original image (QR) is revealed by combining the appropriate image shares. Finally it helps in preventing the password and other confidential information from the phishing websites. The proposed approach can be divided into two phases:

A. Registration Phase B. Login Phase

A. Registration Phase- In this phase the bank contains a database of registered original websites. The users also have their accounts in the bank database.

B. Login Phase- When the user logins in any website he/she provides user id and password. The website i.e. the merchant server gives this id and his server key and password to the bank server. The bank server checks for his account in the database and if present bank checks for users account in database too. Then bank generates an OTP on the basis of User id, Password and the login time and date of user. And converts OTP into QR code and without storing this it divides it into two shares SH1 and SH2 using Visual Cryptography. Then one share SH1 is sent to the user through email and other share SH2 is sent to merchant server through network. The SH2 is then sent to the user by the merchant server through network. At user side now we have 2 shares which user combines by super-imposing and the user gets the QR code which he scans using any smart phone application. User gets an OTP which he mails to bank server and bank server then verifies it and mails user about the website whether it is phishing or not.

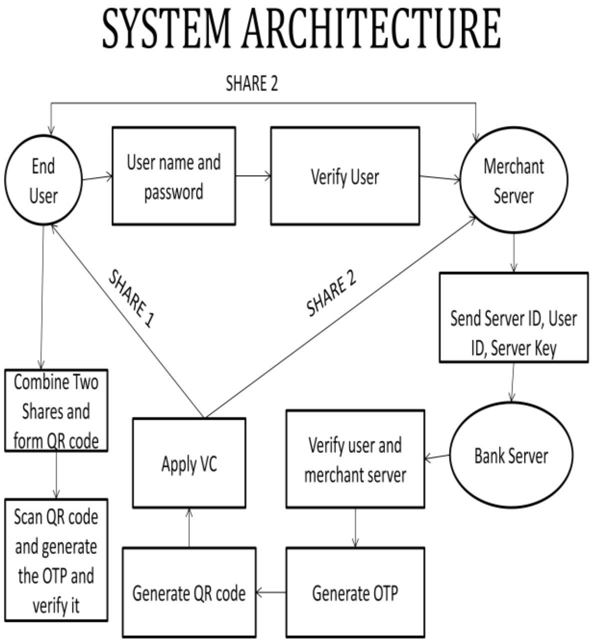
SYSTEM ARCHITECTURE
SHARE 2
End User
User name and password
Verify User
Merchant Server
SHARE 1
SHARE 2
Send Server ID, User ID, Server Key
Combine Two Shares and form QR code
Apply VC
Verify user and merchant server
Bank Server
Scan QR code and generate the OTP and verify it
Generate QR code
Generate OTP

Fig 1: System Architecture

A. Visual Cryptography Algorithm:

i) Encoding Phase: The input is the confidential data in the form of a black and white Secret image represented by matrix A of size mxn. The elements of A are 0’s and 1’s with 0 representing the black pixel and 1 the white pixel. Initial share sh1 is generated as a random image of 0’s and 1’s. The Second share, sh2 is generated by performing bitwise XOR operation of sh1 with the secret image A as follows.

sh1 = R1 ……..(1)

where, R1 is a random binary matrix of size mxn.

sh2 = sh1 XOR A ……(2)

The two shares generated are random looking shares and hence appear meaningless. Now from the property of XOR operation, it can be seen that,sh1 XOR sh2= sh1 XOR sh1 XOR A = A………(3). Thus, combining sh1 and sh2 through XOR reveals A.

Selection of Cover image:

Cover image is a grayscale image of the same size as that of the secret image. For some special cases the cover image can be the photograph of the owner of that confidential data.

Generation of Meaningful shares:

The cover image is customized by mixing a random noise to Cloud Security Using Visual Cryptography
it so that it is now different in its pixel values from the original cover image.

Let C be the cover image matrix of size mxn and let R2 be a random matrix of 0’s and 1’s of the same size as C. Then get the customized cover image D as,

D = C XOR R2 …….(4)

Since each pixel of the cover image is an 8 bit unsigned integer, (because the cover image is a grayscale image having pixel values ranging from 0 to 255) and since the random matrix R2 is made of only one bit number representing either black or white (0 or 1), only the LSB of the each byte in the cover image is affected. Therefore the customized cover image looks same as the original cover image. If the cover image is used directly, then there is a chance that a hacker, after somehow getting hold of the cover image, may pose a security threat.. So, this step is provides extra security. Meaningful shares designated as msh1 and msh2 are generated by XORing the random looking shares with the customized cover image as follows.

msh1 = sh1 XOR D ……(5)

msh2 = sh2 XOR D …….(6)

Here, sh1 and sh2 are binary images and the customized cover image D is a gray scale image. Hence only the LSB of each byte of D affected. Therefore, the meaningful shares look same as the customized cover image. For example, if a pixel value of the cover image is 255 and if a pixel value of the randomly looking share is 1, then XORing these two pixels results in a pixel value of 254 (11111111 XOR 00000001 is 11111110) which is only about 0.4 % change.

Algorithm 1: Share generation

Input: A 2-Dimensional black and white secret image A of size m x n and a grey scale cover image C of size m x n.

Output: Two meaningful shares msh1 and msh2.

```
Procedure SHARE GENERATION (A, C)
1. Get the first share sh1 as a binary random matrix as,   sh1 ← R1
2. Generate the second share sh2 by bitwise XORing the first share with the secret image as,
        sh2 ←sh1 XOR A.
```

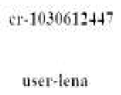

Fig.2a.Secret Image Fig.2b.Cover Image

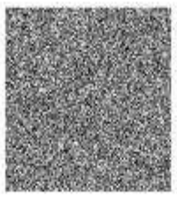

Fig.2c.Random looking Share 1 Fig.2d.Random looking Share 2

```
3. Mix a random noise matrix R2 to the cover image for extra security to get the customized cover
        image D as, D← C XOR R2
4. Generate meaningful shares msh1 and msh2 as,
        msh1← sh1 XOR D
        msh2← sh2XOR D
```

Once the two meaningful shares are ready, one share is stored in one server and the other share is stored. In another server, not easily accessible from the first server.

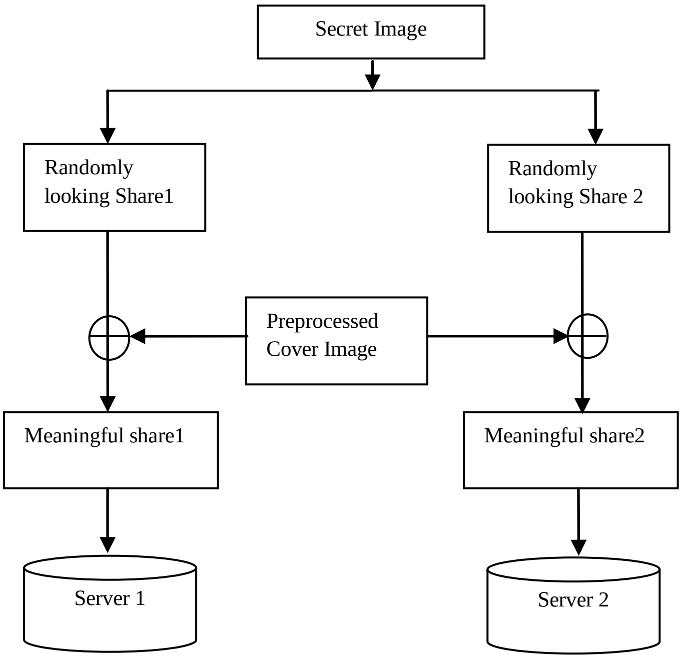

Fig 3: Encoding

ii) Decoding Phase: The decoding phase is performed by the legitimate user. He accesses the two meaningful shares from the two different servers and decodes the secret image by XORing the two meaningful shares.

From (5) and (6),

msh1 XOR msh2 = sh1 XOR D XOR sh2 XOR D = sh1 XOR sh2……(7)

From Eqs.(7) and(3)

msh1 XOR msh2 = sh1 XOR sh2 = A……(8)

The Decoding phase is given in Algorithm 2.

Algorithm 2: Decoding
Input: Two meaningful shares msh1 and msh2.
Output: Decoded Secret image I.
Procedure DECODE (msh1, msh2)
1. Decode the secret image A as,
A ← msh1 XOR msh2 The encoding and decoding phases are depicted in Fig.1.The proposed method provides data access security to the confidential data stored at the server site in cloud computing environment. Since the shares are meaningful, the inside malicious hackers do not pay any attention to it. Even if a hacker gets to know one share, the other share is inaccessible to him because it is located on another far away secured server. With only one share, the confidential data cannot be decoded. This scheme provides good security.

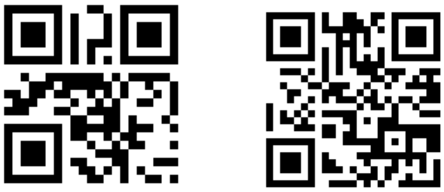

Fig 4: Sample QR codes

B. QR Code algorithm:

Ak = RkQk = Q∗kAk−1Qk, and hence Ak and Ak−1 are unitarily similar. The matrix sequence {Ak} converges (under certain assumptions) towards an upper triangular matrix [9]. Let us assume that the

Algorithm:

Let A ∈ Cn×n. This algorithm computes an upper triangular matrix T and a unitary matrix U such that A = UTU∗ is the Schur decomposition of A.

```
Set A0 := A and U0 = I.
for k = 1, 2, . . . do
Ak−1 =: QkRk; /* QR factorization */
Ak := RkQk;
Uk := Uk−1Qk; /* Update transformation matrix */
end for Set T := A∞ and U := U∞.
```

eigenvalues are mutually different in magnitude and we can therefore number the eigenvalues such that |λ1| > |λ2| > · · · > |λn|. Then – as we will show in Chapter 6 – the elements of Ak below the diagonal converge to zero like |a(k) ij | = O(|λi/λj |k), i > j.

From (3.1) we see that

Ak = Q∗kAk−1Qk = Q∗kQ∗k−1Ak−2Qk−1Qk = · · · = Q∗k · · ·Q∗1A0 Q1 · · ·Qk | {z } Uk.

With the same assumption on the eigenvalues, Ak tends to an upper triangular matrix and Uk converges to the matrix of Schur vectors.

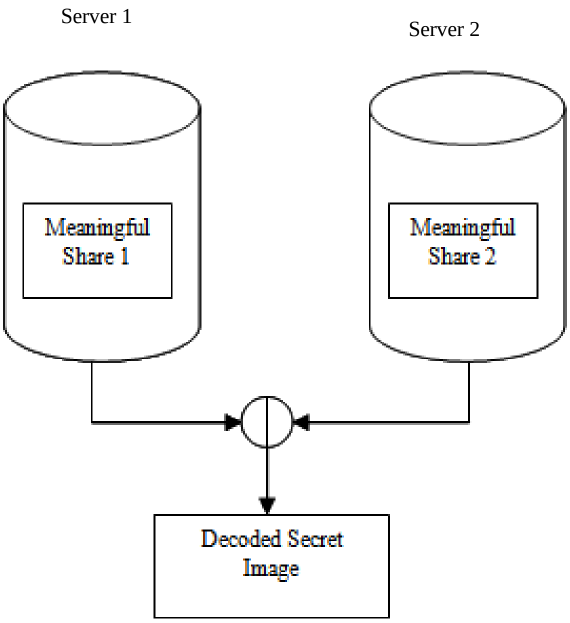

Fig 5: Decoding

IV. CONCLUSION AND FUTURE WORK

In this paper we have proposed a more secured mechanism through VC and QR code based on OTPs. In recent years there has been a steep increase in the number of online users. Hence the proposed system satisfies the high security requirements of the online users and protects them against various security attacks. Also 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.

REFERENCES

[1] J. S. Downs, M. B. Holbrook, Decision strategies and susceptibility to phishing, in: Proc. the second symposium on usable privacy and security(SOUPS 2006), pp. 79-90.

[2] Clarke, Dwaine; Gassend, Blaise; Kotwal, Thomas; Burnside, Matt; van Dijk, Marten: "*The Untrusted Computer Problem and Camera-Based Authentication*". Lecture Notes in Computer Science, 2002, Volume 2414, Pervasive Computing, Pages 114-124, Jan.2002.

[3] Denso-wave:http://www.denso-wave.com/ qrcode/index-e.html

[4] Lee, Jaesik; Cho, Chang-Hyun; Jun, Moon-Seog: "*Secure quick response-payment(QR-Pay) system using mobile device*". Advanced Communication Technology (ICACT), 2011 13th International Conference, Feb. 2011.

[5] I. Bose, A.C.M. Leung, *Unveiling the mask of phishing: threats*, preventive measures and responsibilities Communications of the Association for Information Systems 19 (24) (2007) 544-566.

[6] Google Inc, Google safe browsing for Firefox, http://www.google.com/tools/firefox/ safe browsing/

[7] Saurab K Prashar. "*Security issues in cloud computing*", serl .iit.ac.in/cs6600/saurabh. ppt

[8] M. Naor and A. Shamir, "Visual cryptography," Proceedings of Advances in Cryptology: Eurocrypt94, Lecture Notes in Computer Science, Vol. 950, pp. 1 - 12, 1995. H. Erdogmus, "*Cloud Computing: Does Nirvana Hide behind the Nebula?* " IEEE Software, vol. 26, no.2, pp. 4-6 ,2009.

[9] Y. S. Dai, Y. P. Xiang, G. W. Zhang., "*Self-Healing and Hybrid Diagnosis in Cloud Computing,* " Lecture Notes of Computer Science(LNCS), vol. 5931, pp. 45-56,2009.

[10] Amazon Elastic Compute Cloud [URL].http://aws.amazon.com/ec2, acess on Oct. 2009.

[11] Felt, Adrienne Porter; Wagner, David: "*Phishing on Mobile Devices*". Workshop on Web 2.0 Security and Privacy (W2SP), 2011.

[12] DeFigueiredo, Dimitri: "*The Case for Mobile Two-Factor Authentication*". Security &Privacy, IEEE, Sept.-Oct. 2011.

[13] Kuan-Chieh Liao;Wei-Hsun Lee:"*A Novel User Authentication Scheme Based on QR-Code"*. Journal of Networks, Vol 5, No Aug 2010.