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

Dhanashree Moholkar
Department of Computer Engineering
Bharati Vidyapeeth College of Engineering for Women,
Pune 411043, India

Namrata Kadam
Department of Computer Engineering
Bharati Vidyapeeth College of Engineering for Women,
Pune 411043, India

Damini Deokar
Department of Computer Engineering
Bharati Vidyapeeth College of Engineering for Women,
Pune 411043, India

Ashwini Kute
Department of Computer Engineering
Bharati Vidyapeeth College of Engineering for Women,
Pune 411043, India

Sonali Kadam
Department of Computer Engineering
Bharati Vidyapeeth College of Engineering for Women,
Pune 411043, India

ABSTRACT
Phishing is an attack by a group or an individual to misuse personal information such as passwords, credit card information etc. for identity theft, financial gain and other fraudulent activities. In this paper image based (QR codes) authentication using Visual Cryptography (VC) is used. 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 doing comparison of our paper with the existing system and show how our method is more efficient and also show our results.

General Terms
Visual cryptography, Grayscale, Threshold algorithm.

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

1. INTRODUCTION
As mentioned in our previous paper named ‘An Modern approach for detecting web phishing using VC and QR code’ the concept of VC, it mentions its algorithm too. Another paper ‘An improved secure banking using QR codes’ presents the design and implementation of QRP, an open source, proof-of-concept authentication system that uses a two-factor authentication by combining a password and a camera-equipped mobile phone, acting as an authentication token.

Registration: This part is not implemented as the paper is only intended to present an authentication method. The following steps are a suggestion on how to complete the registration process:

1. The user would go into the registration section in the QRP web application and would submit her username, password and IMEI number1 of the phone she intends to use to authenticate.

2. After validating the data entered (correct IMEI, password complex enough,etc.), the server would store this information on the database.

3. Next, the server would generate a private and public pair of keys unique to the user, that would be stored on the server.

4. After this, the user would proceed to download and install the application on her phone.

through a https request to the application server.

5. The first time the mobile application is run, the user will need to enter her username and password (the IMEI can be verified by the mobile application) and the credentials (user/password) would be validated against the database through a https request to the application server.

6. If successful, three files would be imported and stored in the user's phone internal storage: the server's public key, the user's private key and a user data file, containing the user's encrypted credentials.

The server's public key will be used to decrypt the credentials file. The user's private key will be used to authenticate in the server.

Authentication: When the user opens the mobile application, she will need to input the password first. It will be verified against the user's encrypted file containing the credentials and if successful, the scanning application will run. The user can now proceed to scan the code from the web application screen. The contents of the QR code will be captured and sent back to our mobile application. Our mobile application will then generate a string containing the captured random number and the IMEI of the phone, that will be encrypted using our private key. Next, the mobile application will check the state of the phone and decide whether we are going to authenticate in online or offline mode.

2. PROPOSED SYSTEM
In Proposed System Quick Response Code (QR) codes and Visual Cryptography (VC) are merged together. Here anti phishing framework based on QR code and visual cryptography is used to solve the Image based authentication is used. Visual Cryptography is used to decompose an image (QR) into shares. Original QR image is revealed by combining the appropriate image shares. It helps in preventing the password and other confidential information

from phishing websites. The proposed approach is as follows:

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

In the Login Phase when the user logins in any website he/she provides user id and password. The merchant server (website) gives this id and his server key and password to the bank server. The bank server checks for his account in the database and checks for users account in database too. Then bank generates an OTP on the basis of User id, date of user, Password and the login time and converts OTP into QR code and without storing this it divides it into two shares SH1 and SH2 using VC. 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 which verifies it and mails user about the website whether it is phishing or not.

3. EXPERIMENTAL RESULTS/OUTPUT

1. Conversion of color image into gray-scale

Fig. 1.a. Load Image

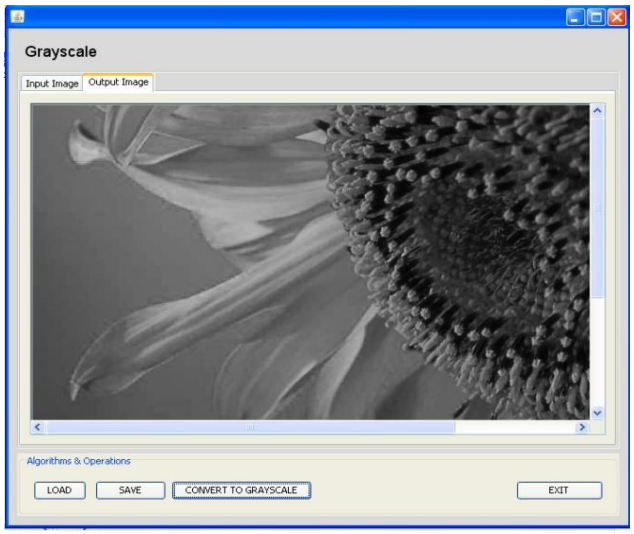

Fig. 1.b. Applying gray-scale

2. Threshold

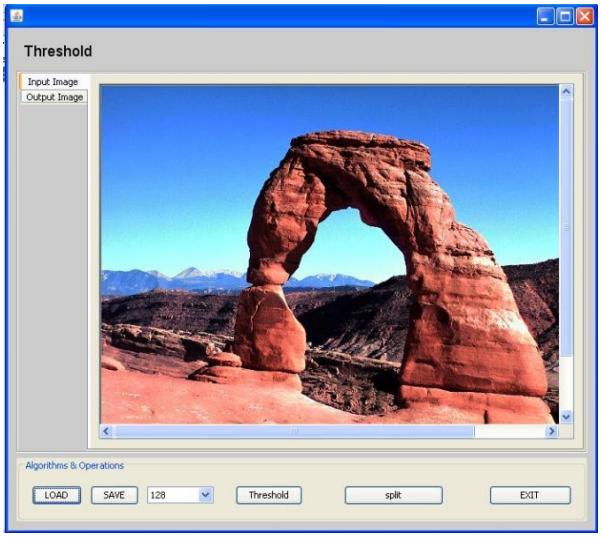

Fig.2.a. Load image

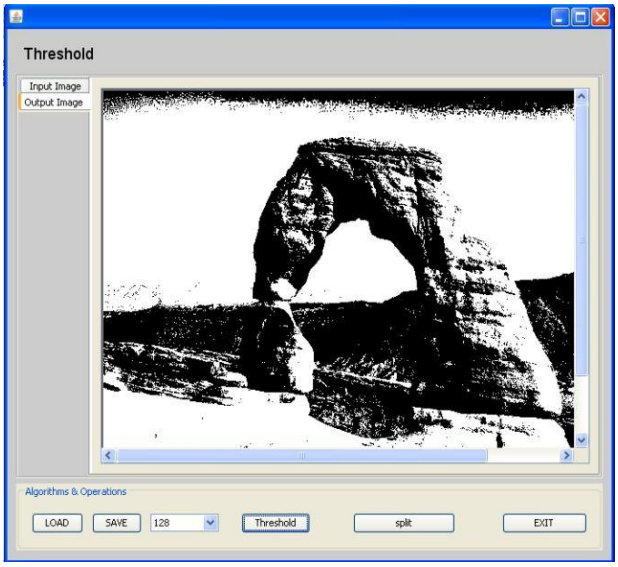

Fig.2.b. Output of threshold

3. QR code generation

3. Visual cryptography

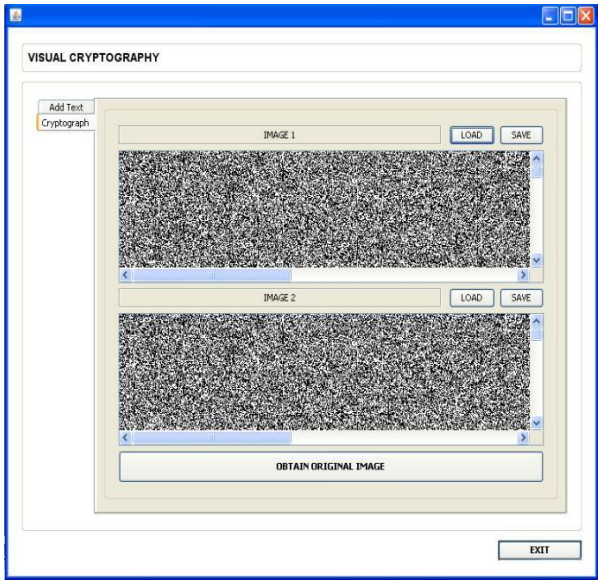

Fig.3.a. Loading Shares

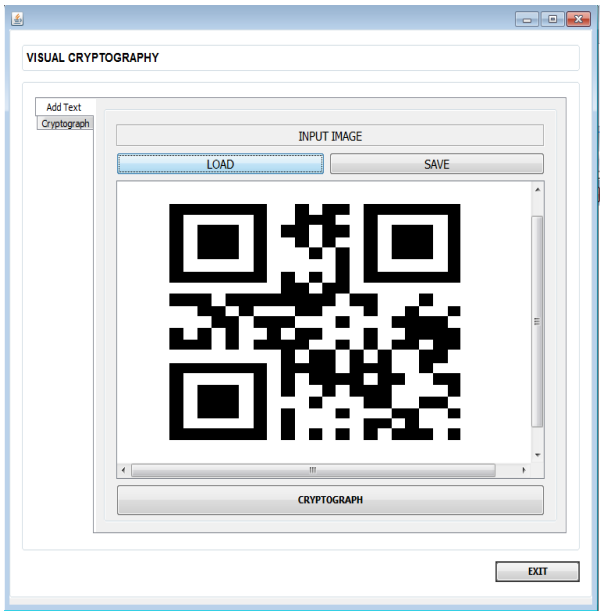

Fig.3.b. Applying VC and getting original image

4. COMPARISON BETWEEN EXISTING AND PROPOSED SYSTEM

1. In Existing system the method is used only to encrypt the credential information while in proposed system we are detecting the phishing websites.
2. In Existing system Visual Cryptography (VC) and QR code is used separately while in proposed system we are making use of both VC and QR code which enhances the method.
3. In Existing system encryption and decryption of shares is done on client side only but in proposed system it is done on server side.
4. Also, the time required for computation of encryption and decryption is more in existing system.
5. The Existing system always requires authentication.

5. OVERCOME DISADVANTAGES OF EXISTING SYSTEM

1. In Visual Cryptography we divide image into two shares and send this shares to two different Server. One single share can not reveal the whole image. So hacker cannot hack credential information with a single image.
2. QR code is versatile.
3. We can send any short text messages through QR code.
4. It is secure method of encryption.
5. It is reliable method for detecting phishing websites

6. CONCLUSION AND FUTURE WORK

Hence by comparison between existing and proposed system we prove that our method is more efficient and secured. In the near future this work may also be enhanced by taking action on the detected phishing websites. 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.

7. ACKNOWLEDGEMENT

We also thank the Head of Department Prof.D.D.Pukale and all the faculty members who have made the journey of our under-graduation and technical learning such an enjoyable experience.

Last but not the least we thank all the member of various research papers and articles who have provided us directions in this domain.

This report an1d Project would not have been possible without the essential and gracious support of many individuals. The personal support and interest of our guide Prof S.P.Kadam made it all happen. Hence we would like to take this opportunity to thank all the teachers and the staff of our Computer department for their support and cooperation. We would also like to thank our family and friends for their unconditional belief and faith in us.

8. 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