

Secure Server Verification Using Visual Cryptography on Images

Prof.S.A.Hadke¹, Smita Solunke², Saili Pawar³, Ritika Thorat⁴, Neha Kamble⁵

Information Technology^{1, 2, 3, 4, 5},

Assistant Professor (Bharati Vidyapeeth's College of Engineering for Women, Pune-411043)¹, Student^{2, 3, 4, 5}

Email: hadkeseema@gmail.com¹, smitasolunke999@gmail.com², sailipawar1997@gmail.com³, 12ritikathorat@gmail.com⁴, nehaanant246@gmail.com⁵

Abstract- This paper gives a survey of several method used by the researcher to avoid phishing attacks which is one of the online attacks that have been increased due to an online transaction. Here we propose an abstract view of the system which we are developing named as "Secure Server Verification Using Visual Cryptography on Images" to solve the problem of phishing using Visual Cryptography. In this system, a random password is generated before initialization of a transaction in such a way that, image containing the password is taken as input and is divided into different number of shares depending upon the banks scheme. One share is preserved with the applicant initiating the transaction and all other shares are given to other members sharing the same account. The applicant need to provide his shares during every transaction and those shares are over lapped with the shares generated for the other owner members of the account to check for authentication and approval. The system will check for authentication and this will be done by using correlation technique. If a higher correlation coefficient is achieved, then the authentication is succeeded. Once the authentication is done, CAPTCHA is displayed to distinguish human from machine input. Once the password matches, transaction can be initiated.

Keywords- VC; OTP; URN; NTRU; Captcha.

1. INTRODUCTION

Phishing is [6][7] an online attack in which confidential and sensitive information can gain by the attacker. Phishing is an online identity theft whose aim is to steal secret information such as User ID, passwords, URN and OTP which are sending via e-mails [6][8] which come into view to from trusted source like Banks. Emails generated an emergency for updating bank account related data. Phishing attacks have been receiving unlimited press exposure because such attacks have been getting higher in number day by days. Phishers attempt to illusively acquire sensitive information, for instance, passwords and credit card details by masquerading attack where he behaves as a trustworthy person.

Nowadays online transaction [8] becomes very common and frequent which are prone to more number of online attacks. Phishing attacks are becoming an adversity for online transactions and e-commerce users. So we introduce a method which can be used as a secure way against phishing attack which is named as "Secure Server Verification using Visual Cryptography on Images". Here an image-based authentication using Visual Cryptography (VC) [1][2] [3][4][6][7][8] is used. Visual Cryptography is a confidential data sharing method which is the technique of sharing the visual information. The image is getting divided into two shares.

The basic idea is that the secret image is divided into two irregular patterns of images called shares and they can be unraveled without any complicated cryptographic computation.

2. LITERATURE SURVEY

Sozan Abdulla et al.[1] defines Visual Cryptography Algorithm i.e. the encryption technique for a color image to hide information in images which divide the secret image into multiple layers.

InKoo Kang et al.[2] generate high quality of meaningful color shares as well as the colorful decrypted share using VIP synchronization and error diffusion methods. The VIPs are pixels that take pixel values of original images to create significant shares. When these VIPs are not assigned throughout the halftone stage, the consequential shares are identical as that of standard VC schemes except the colorful decrypted messages. This method generates meaningful color shares with high visual quality.

Divya James et al.[3] gives a technique for avoiding phishing and detection of an image based on authentication using Visual Cryptography. To defend the privacy of an 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 exposed only when both are available at the same time; the original image captcha. Formerly the original image captcha is used as the password.

Roberto De Prisco et al.[5] shows two models of visual cryptography i.e. deterministic visual cryptography that deterministic and random grid visual cryptography are strictly related.

4. PROPOSED SYSTEM

Nowadays various online attacks have been rise. The most known attack is phishing which is done by hackers or any unauthentic users. In the proposed system there is by Visual Cryptography.

a new method for "Secure Server Verification Using Visual Cryptography on Images" to solve the problem of phishing where image-based authentication, visual cryptography is used. Secret sharing scheme is perform

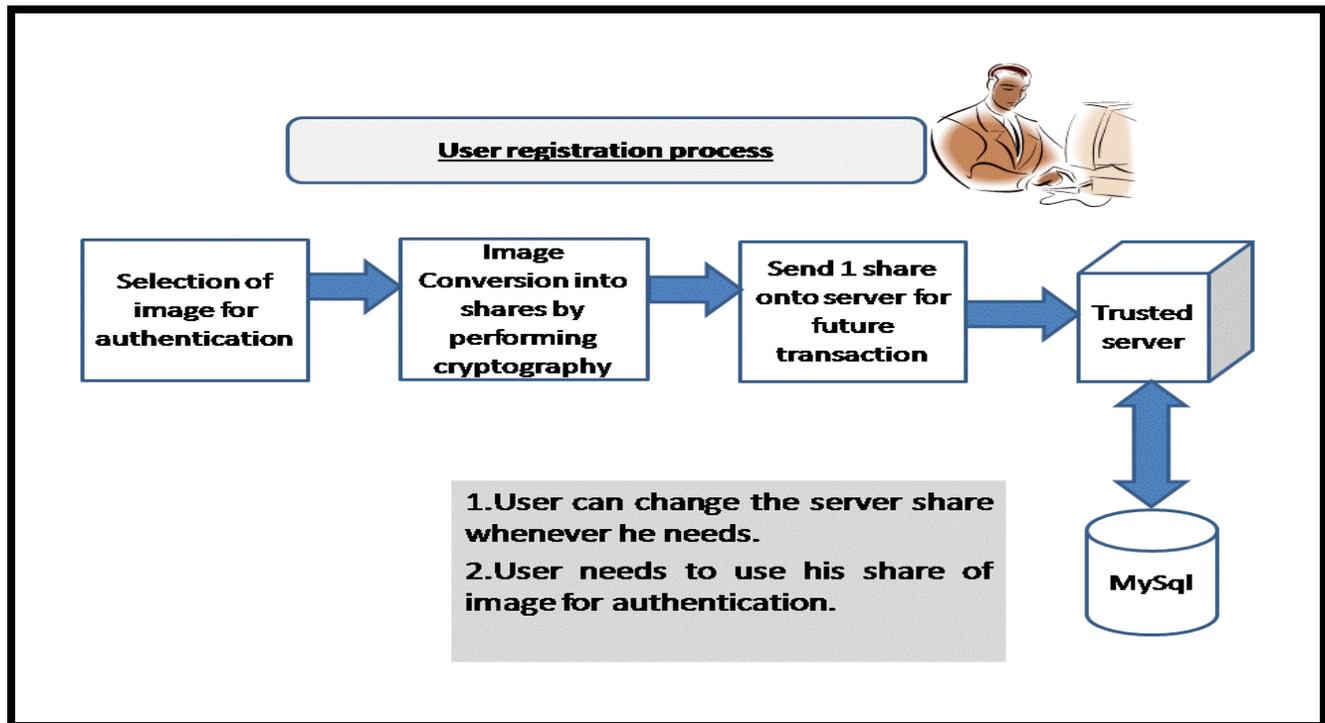


Fig.1. User Registration Process

(1) Registration Module for System

In this phase an essential part is the creation of shares from the image where one share is kept with the user and other share can be kept with the server.

(2) Verification of Shares or Login using Visual Cryptography

The user will upload his/her share and puts his user id and clicks on the login button. The share gets uploaded to the server and merged with share2 at the server using visual cryptography. If the server under test sends some unusual share then the loading of shares will create an unrecognizable form of an image.

- Visual Cryptography based phishing Website
- Creation of multiple image shares
- Forming Original Image on the client side

(3) Verification of Joint Accounts

User having joint accounts will upload their shares 1 by 1 and puts their user id and clicks on login button. These shares gets uploaded to server and merged with share3 at the server using visual cryptography. Merged shared are then compared with the original image to verify the joint account users for fund transfer.

(4) Encryption and Decryption

If images have to be transferred to each other, it will be transferred in encrypted way using NTRU Algorithm. Data will be encrypted using asymmetric key. Asymmetric key will be transferred after encrypting with public key of receiver along with the encrypted data.

(5) Avoiding Phishing in Banking

Avoid following attacks on the website
 In phishing attack the single person or group of people fake the URL, which appears in the user’s browser window. This redirects the user to a different web site with the intention of performing fraud and due to this user’s personal

information is leaked. Attackers send e-mails or SMS with a link which asks the user to update or confirm account related information as well as his confidential information. The intention behind performing these activities is to gain users sensitive data like user-id, password, credit or debit card details, bank details etc.

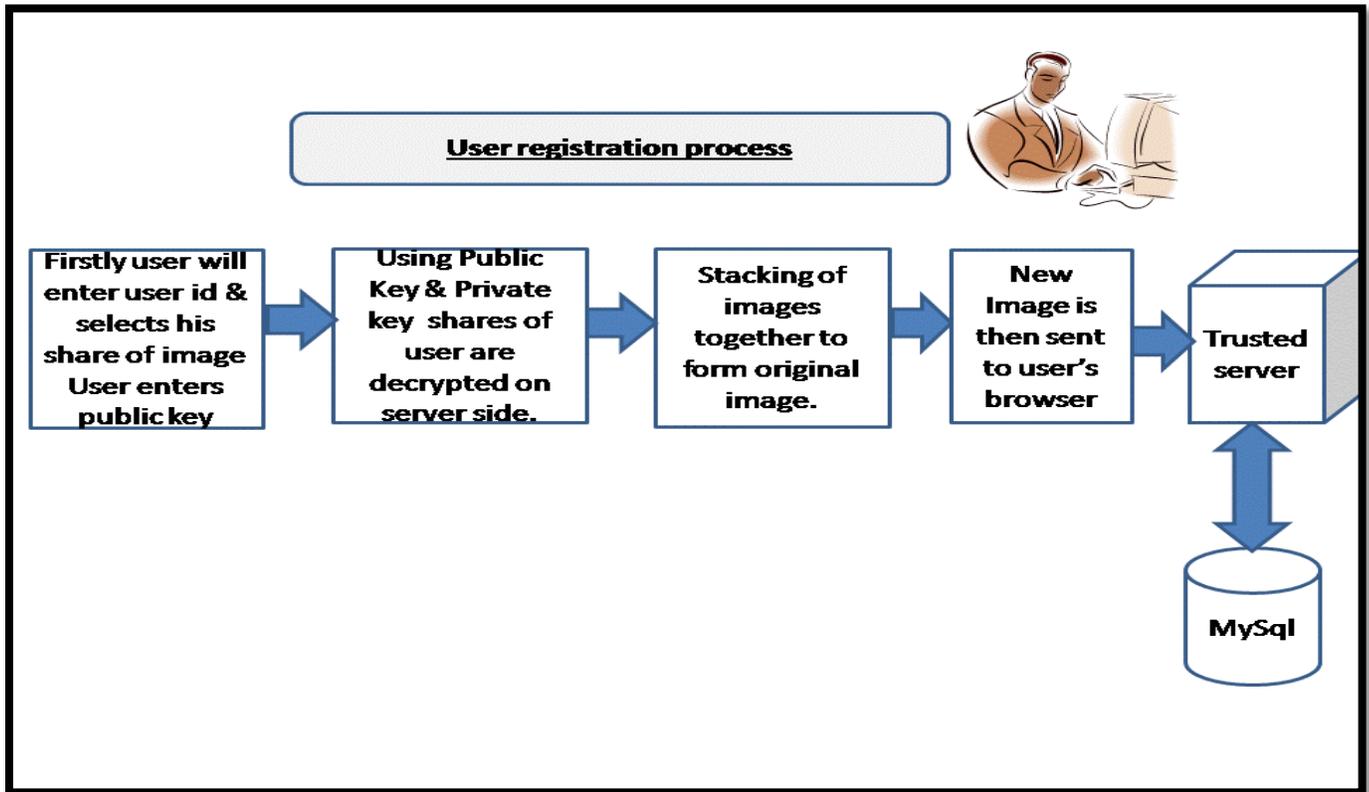


Fig.2. User Login Process

4.1. Advantages of Proposed System

- To prevent user account details from phishing attack.
- To perform authentication of both users of joint account to avoid anonymous use of account by single user

5. CONCLUSION

Based on the literature survey and papers studies, visual cryptography provides security against anti-phishing websites. It can also be used as an authorization method for the banking sector. Visual Cryptography use in banking increases usability and security as compared other methods available in the market.

As a future perspective we can use blockchain technology with this system for better transaction and we can use it for business accounts.

ACKNOWLEDGEMENT

We take this opportunity to thank our project guide Prof. S. A. Hadke and HOD Prof. Dr. D. A. Godse for their guidance and helping us in the completion of this project report. We are also thankful to all the staff members of the Department of Information Technology of Bharati Vidyapeeth’s College of Engineering for Women, Katraj for their valuable time and support. We would also like to thank the institute for providing the required facilities, Internet access and important books.

REFERENCES

- [1] Sozan Abdulla New Visual Cryptography Algorithm For Colored Image"JOURNAL OF COMPUTING VOLUME 2,ISSUE 4,APRIL 2010,ISSN2151-9617.
- [2] InKoo Kang, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Heung-Kyu Lee, Member, IEEE"Color Extended Visual Cryptography Using Error Diffusion",VOLUME 20 ,NO.1,JAN 2011.
- [3] Divya James,Mintu Philip,"A Novel Anti Phishing framework based on Visual Cryptography",2012 IEEE.
- [4] Mrs. A. Angel Freeda,M.Sindhuja , K.Sujitha"Image Captcha Based Authentication Using Visual Cryptography", International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 2 , April - May , 2013.
- [5] Roberto De Prisco and Alfredo De Santis,"On the Relation of Random Grid and Deterministic Visual Cryptography",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2014.
- [6] Shreya Zarkar, Sayali vaidya, Arifa Tadvi, Tanashree Chavan, Prof. Achal Bharambe "Image Based Authentication Using Visual Cryptography and Encryption Algorithm ", International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1692-1696.
- [7] Xingxing Jia, Daoshun Wang, Member, IEEE, Daxin Nie, Chaoyang Zhang, Member,IEEE,"Collaborative Visual Cryptography Schemes",Transactions on Circuits and Systems for Video Technology, 2016.
- [8] Doshi Ruchali 1 , Kale Prajakta 2 , Pasalkar Pranoti "Secured Transaction System Using Steganography and Visual Cryptography",2016, IJESC.