

# Secure Server Verification Using Visual Cryptography on Images

Prof. S. A. Hadke<sup>1</sup>, Smita Solunke<sup>2</sup>, Saili Pawar<sup>3</sup>, Ritika Thorat<sup>4</sup>, Neha Kamble<sup>5</sup>

Information Technology<sup>1,2,3,4,5</sup>, Assistant Professor(Bharati Vidyapeeth's College of Engineering for Women )<sup>1</sup>, Student<sup>2,3,4,5</sup>  
Email: hadkeseema@gmail.com<sup>1</sup>,smitasolunke999@gmail.com<sup>2</sup>, sailipawar1997@gmail.com<sup>3</sup>, 12ritikathorat@gmail.com<sup>4</sup>  
nehaanant246@gmail.com<sup>5</sup>

**Abstract-** This paper gives a survey of different 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. Phishing is an endeavor by an individual or a group to attain personal confidential information such as passwords, credit card information etc from unsuspecting victims for identity theft, financial gain and other fraudulent activities.

Here we propose an abstract view of the system which we are developing named as "Secure Server Verification by Using Visual Cryptography on Images" to solve the problem of phishing using Visual Cryptography.

**Index Terms-** VC; OTP; URN; NTRU; Captcha

## 1. INTRODUCTION

Phishing is one of the major attacks [6][7] among all online attacks in which confidential and sensitive information can gain by the attacker. Phishing is a form of online identity theft that aims to steal sensitive information such as User ID, passwords, URN and OTP by sending e-mails [6][8] which come into view to from trusted source like Banks, TAX authorities etc. These emails generate a sense of urgency for updating account related data. Phishing scams have been receiving widespread press exposure because such attacks have been getting higher in number and sophistication. Phishers attempt to deceptively acquire sensitive information, for instance, passwords and credit card details, by masquerading as a trustworthy person or business in electronic communication.

In recent days online transaction [8] becomes very common which gives rise to more number of online attacks. Phishing attacks are becoming a trouble for online transactions and e-commerce users. So here introduces a new method which can be used as a secure way against phishing which is named as " Secure Server Verification by Using Encryption Algorithm and Visual Cryptography by Using Normal Images" Here an image-based authentication using Visual Cryptography (VC) [1][2] [3][4][6][7][8] is used. Visual Cryptography is a top-secret sharing method which owns 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

This section consists of the work that has been already done on this system by various researchers using different methodologies and algorithms.

Sozan Abdulla et al.[1] define a New 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 can produce meaningful color shares with high visual quality.

Divya James et al.[3] gives a technique for phishing detection and prevention 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.

Tanashree Chavan et al.[ 6] provides an Anti-phishing structure based on visual cryptography and RSA algorithm. An image-based authentication using Visual Cryptography (VC) and the encryption algorithm (RSA) is used to avoid phishing.

This method of image authentication gives 100% result for image size less than 2.5MB. Consequently, security of image can be attained by visual cryptography and RSA algorithm.

Xingxing Jia et al.[7] designed A (k, n)-conventional visual cryptography (VC) method to share one secret and each participant takes one share. Collaborative visual cryptography (CVC) schemes into the multiple secrets VC scheme with a general access structure. The structure of the basis matrices in CVC method in between two VC schemes is formulated into an integer linear programming problem that minimizes the pixel expansion under the corresponding security and contrast constraints. In addition, the collaboration among more VC schemes is constructed.

Doshi Ruchali et al.[8] provides a system which will build a trust relationship between merchant and customer. For that, a cryptographic technique dependent on visual secret sharing is used for image encryption. In addition to this cryptographic technique, the advantages of steganography are combined to avoid cheating in visual cryptography.the individual sheet images do not reveal the identity of Using these techniques the proposed system will provide security to the customer's data using less information.

### **3. ALGORITHM USED**

#### **3.1 Visual cryptography**

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decrypted information appears as a visual image.

#### **3.2 NTRU Algorithm**

NTRU is an open source public-key cryptosystem that uses lattice-based cryptography to encrypt and decrypt data. It consists of two algorithms: NTRUEncrypt, which is used for encryption, and NTRU Sign, which is used for digital signatures.

### **4. PROPOSED SYSTEM**

In the area of the internet, different online attacks have been increased gradually and among them, the most popular attack is phishing Which is done by hackers or unauthorized users.

In the proposed system there is a new method for "Secure Server Verification by Using Visual Cryptography Using Normal Image" to solve the problem of phishing where image-based authentication using visual cryptography. Secret sharing scheme is done by visual cryptography as it is a technique for sharing the visual information. The image is divided into two shares. The secret image is divided into two irregular patterns of images called shares and they can be done without any complicated cryptographic computation.

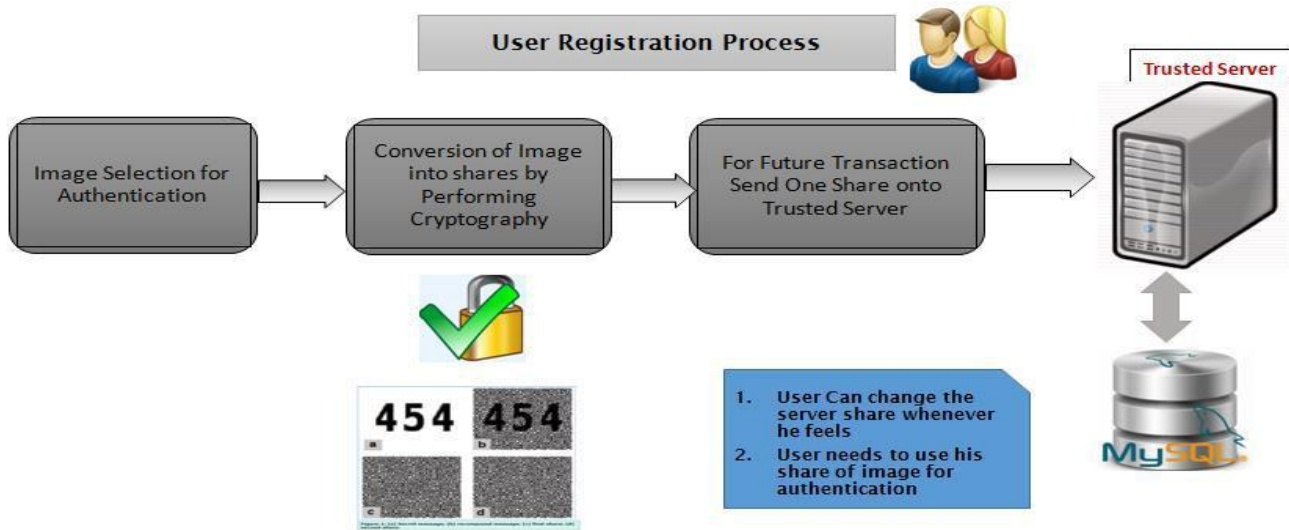


Fig.1. User Registration Process

**(1) Registration Module for Banking**

In the registration phase the most important 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.

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

**(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 this activities is to gain users sensitive data like user-id, password, credit or debit card details, bank details etc.

**Fig.2. User Login Process**

1

#### **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.

#### **4. 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.

#### **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, support, comments, suggestions and persuasion. 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  
<https://sites.google.com/site/journalofcomputing/>.
- [2] Inkoo kang, member, ieee, gonzalo r. Arce, fellow, ieee, and heung-kyu lee, member, ieee"color extended visual cryptography using error diffusion",iee transactions on image processing, vol. 20, no. 1, january 2011
- [3] Divya james,mintu philip,"a novel anti Phishing framework based on visual cryptography", 2012 ieee.
- [4] Mrs. A.angel freedda , 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",iee 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