IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 5, May 2018

Securing Online Transaction using Visual Cryptography

P.Y.Pawar[1], Pooja Rajguru[2], Jaishree Dhomse[3]

Department of Information Technology, Sinhgad Academy Of Engineering, Pune, India[1,2,3]

Abstract: Nowadays many people are using online financial transactions. This transaction needs to be secure. A rapid growth in E-Commerce market is seen in recent time throughout the world. With the ever-increasing use of online shopping, Debit or Credit card fraud and personal information security are major concerns for customers, merchants and banks specifically in the case of CNP (Card Not Present). This paper presents a new technique for providing limited data only that is required for fund transfer during online shopping thereby safeguarding customer data. To overcome these problems using visual cryptography.

Visual Cryptography is a secret sharing scheme which owns the technique of sharing the visual information. The Captcha (image) is getting divided into two shares. The basic idea is that the secret captcha is divided into two irregular patterns of images called shares and they can be unravelled without any complicated cryptographic computation.

Keywords: Visual Cryptography, Share generation, Image (Captcha).

I. INTRODUCTION

Information security plays a very important role in the current era of technologies. Multimedia data like images, video etc are widely used and they are widely transmitted using the network. So security is an important aspect. Visual cryptography is a type of secret sharing for encrypting written material like text, images in a perfectly secure way [3]. This paper presents a new scheme for providing limited data only that is necessary for fund transfer during online shopping because it is safe customer data. In this paper, we are using steganography and visual cryptography in combine [3].

In this paper anti-phishing for detecting this attack, there many types of anti-phishing mechanisms are used. In phishing process, suppose attacker sends out thousands of phishing emails with a link to the fake website [4]. User clicks on links in email believing it is legitimate. They enter personal information on that fake website. Attacker collects the stolen information and login to correct website. This is an overall process of phishing. To overcome the phishing we use anti-phishing mechanism.

Hash-Based password schemes are easy and fast because those are based on text and famed cryptography. So, cyber-attacks getthe password by cracking tool or hash-cracking online sites. Attackers can get easily original password from the hash value when that is relatively simple and plain. As a result, many hacking accidents have been happened in systems adopting those hash-based schemes [2]. In this work, password processing scheme based on an image using visual cryptography (VC).Different from the traditional scheme based on hash and text, this scheme transforms a user ID of text type to two images encrypted by VC. The user should make two images consisted of subpixels by random function with SEED which includes personal information [2]. The server only has user's ID and one of the images instead of the password. When the user logsand sends another image, the server can extract ID by utilizing OCR (Optical Character Recognition). As a result, it can authenticate the user by comparing extracted ID with the saved one. Our proposal has lower computation, prevents cyber-attack aimed at hash cracking and supports authentication not to expose personal information such as ID to attackers [2].

II. LITERATURE REVIEW

A. Visual Cryptography using EVC and QR code:

In these paper new scheme for providing security during an online transaction for online frauds detection using Extended Visual Cryptography (EVC) and QR code. By using this technique, we provide better security to people. In proposed system user first registered on the website. The client sends ID and password to bank server for verification. If it is valid then generate One Time Password (OTP) and apply EVC for shares generation. Bank server sends one share to the client and one share to the server [1]. At the time of reconstruction, two shares are combined to reveal the original OTP. Then the client sendsthis OTP to bank server for verification.

DOI 10.17148/IJARCCE.2018.7517

B. Hash-Based Scheme:

For user authentication, we have to proceed through verification of the ID and password to the system verification of password system uses a hash-based password scheme that converts the original password into hash-value by famed function. [2]. The advantages this system without difficulty, and computational velocity of a process is fast because a type of hash-based scheme is fundamentally based on text utilizing popular hash function such as MD5, SHA256. Suppose that someone writes password “1qaz2wsx” in a system. If an attacker is aware of the hash value “1c63129ae9db9c60c3e8aa94d3e00495”, the value can be sufficiently cracked simply by thefree crack site. If the attacker doesn’t know any information about hash function, he or she can easily guess which kind of hash function is used in the system. As the result, the attacker can cause damage to the system. Participants have the responsibility for this kind of attacks [2].

C.Steganography Scheme:

For hiding a message we are using steganography. The key concept behind steganography is that message to be transmittedis not detectable to casual eye[3]. For hiding data in steganography using text, video, and image cover the message. The text message can be hidden by shifting word and line, in open +spaces, in word sequence of a text steganography. Properties of a sentence such as a number of words, number of characters, the number of vowels, the position of vowels in a word are also used to hide a secret message. The advantage of text steganography over other steganography techniques is its smaller memory space requirement and simpler communication. Visual Cryptography (VC), proposed by Naor, is a cryptographic technique based on visual secret sharing used for image encryption. Using k out of n (k, n) visual secret sharing scheme a secret image is encrypted in shares which are meaningless images that can be transmitted or distributed over an untrusted communication channel [3]. Only combining the k shares or more give the original secret image.

III. PROPOSED SYSTEM

Visual Cryptography is a secret sharing scheme which owns the technique of sharing the visual information. The Captcha (image) is getting divided into two shares. It encrypts a secret message into two shares printed in transparencies and shared participant.The basic idea is that the secret captcha is divided into two irregular patterns of images called shares and they can be unraveled without any complicated cryptographic computation.

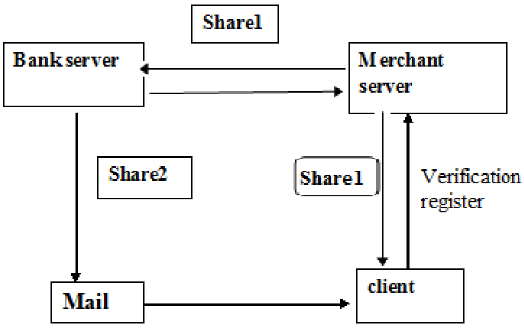

Figure 1.System Architecture.

The proposed System has the following Architecture.

The System is divided into following parts:
a) **User Login:**User Login is the act or process of entering user accounts for the reason to do online transaction.

b) Verification by Merchant Server: As the user authentication in general system has proceeded basically through verification of ID and Password. This verification is get done by this Merchant Server by sending a verification request to the Merchant server. The Merchant Server then sends Server ID and User ID to Bank Server to Validate with server key.

c) Verification by Bank Server:
As the merchant server sends server ID and User ID for validating the Bank is then responsible to fetch and validate server ID and User ID.

DOI 10.17148/IJARCCE.2018.7517

If the credentials are OK then Bank Server will generate One Time Password (OTP) otherwise transaction error will generate an Invalid Credentials!.

D) Share Generation:

Once the OTP is get generated the captcha image is formed automatically. Captcha is get generated by using the encryption algorithm. Once the captcha image is retrieved the shares will get generated by using share generation algorithm. The shares are generated at Bank Server side only. The share1 is getting transferred through a network on user interface and another share share2 is getting transferred through an E-mail to the user account.

E) **Combining shares and Verification:**

After two shares have downloaded both shares are combined together and we get an original password (OTP) by using decryption algorithm to complete the transaction process. That password (OTP) is get verified by bank server if that OTP is valid transaction is getting completed. If the OTP is not valid the session will get expired. So the user has to do again transaction.

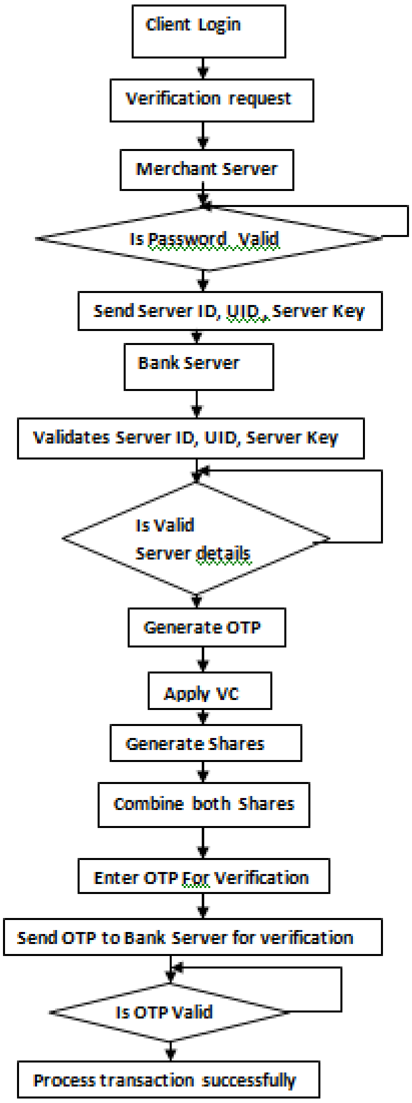
Client Login
Verification request
Merchant Server
Is Password Valid
Send Server ID, UID, Server Key
Bank Server
Validates Server ID, UID, Server Key
Is Valid
Server details
Generate OTP
Apply VC
Generate Shares
Combine both Shares
Enter OTP For Verification
Send OTP to Bank Server for verification
Is OTP Valid
Process transaction successfully

Figure 2. System Flowchart

ALGORITHM:

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;

DOI 10.17148/IJARCCE.2018.7517

sh2 sh1 A Symbol represents bitwise XOR operation.
3. Mix a random noise matrix R2 to the cover image for extra security to get the customized cover imageD as, D C R2
4. Generate meaningful shares msh1 and msh2 as, msh1 sh1 D msh2 sh2 D

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 msh2. The encoding and decoding phases are depicted in.

Algorithm 2: Encoding:
(1) Where, R1 is a random binary matrix of size mxn. sh2 sh1 A
(2) Where, Symbol represents bitwise XOR operation. 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 sh2 sh1 sh1 A A .
(3) Thus, combining sh1 and sh2 through XOR reveals A. Selection of Cover image: Cover image is a gray scale image of the same size as that of the secret image. For some special casesthe 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 store in one server and the other share is stored in another server, not easily accessible from the first server.

TEST RESULTS

The experimental results demonstrate an example of applying this scheme to online transaction. Fig. shows the OTP. This is the confidential data that has to be encrypted. Fig.shows the cover image. Fig.share1 and Fig.share2 are the inputs to encoding phase. One meaningful share is stored at one server and the other meaningful share is send at the a client. In the decoding phase, the share1 and share2 are inputs which are XORed to obtain the secret image given in OTP. From the experimental results it can be seen that there is no quality loss in the decoded image. Also the proposed scheme provides non expanded meaningful shares. These are the advantages of the proposed scheme. Another advantage is that this scheme is simple to implement (using XOR) and also robust when compared to other encryption schemes like AES, RSA etc.

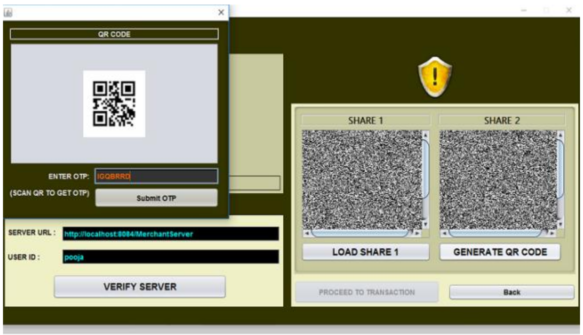
ENTER OTP: IGQBRRD
SERVER URL : http://localhost:8084/MerchantServer
USER ID : pooja

Figure3. Generating shares and OTP

CONCLUSION AND FUTURE SCOPE

The future scope can be as we are generating two shares and that is to be combined then only we can get the original message, in next step for an organisational purpose where the big transaction will be placed at that moment we can generate share like wise and we can also restrict the no of shares combined when we want to extract the original message. So,we are developing Visual cryptography scheme in which we are generating shares for general access structure. As this method does not have pixel expansion it does not requires code to design. Share generation technique gives more security to the OTP then gets converted into image captcha and this will provide more security. So this project provides the user more security to do online transaction securely.

REFERENCES

[1] "Online Fraud Transaction Prevention System Using Extended Visual Cryptography And QR Code" By Shubhangi Khaimar1 and Reena Kharta, Department of Computer Engineering, Pimpri Chinchwad College of Engineering,Pune-44,India.2017 IEEE.

[2] "Enhanced password Processing Scheme Based On Visual Cryptography and OCR" By Dana Yang, Inshil Doh and Kijoon Chae, Dept. Computer Science and Engineering Ewha Womans University Seoul, Korea. 2017 IEEE.

[3] Online Payment System Using Visual Cryptography and Steganography "By Souvik Roy1 and P.Venkateshwaran2, Department of Electronics & Telecommunication Engineering, Jadaypur University, Kolkata-700032, India. 2016 Online International Conference on Green Engineering And Technologies (IC-GET). 55500

[4] "A Navel Antiphishing Framework Based On Visual Cryptography "By Divya James and MintuPjilip.MtechIn Information Security, India Gandhi National Open University, India.

DOI 10.17148/IJARCCE.2018.7517