Journal of Telecommunications System & Management

Rajguru et al., J Telecommun Syst Manage 2018, 7:1
DOI: 10.4172/2167-0919.1000158

Short Communication Open Access

Securing Online Transaction Using Visual Cryptography

Pooja Rajguru[1]*, Jaishree Dhomse[1] and Pawar PY[2]

[1]Department of Information Technology, Sinhgad Academy of Engineering, Kodhwa, Pune, Maharashtra 411048, India
[2]Faculty of Information Technology, Sinhgad Academy of Engineering, Kondhwa, Pune, Maharashtra 411048, India

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 and 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 unraveled without any complicated cryptographic computation.

Keywords: Visual cryptography; Share generation; Image (Captcha)

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 [1]. Its 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.

For this project we are using anti-phishing for detecting the 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 [2]. 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 get the 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 [3]. 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 sub pixels by random function with SEED which includes personal information. The server only has user's ID and one of the images instead of the password. When the user logs and 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 [4].

Literature Review

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. At the time of reconstruction, two shares are combined to reveal the original OTP. Then the client sends this OTP to bank server for verification.

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. 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 the free 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.

***Corresponding author:** Pooja Rajguru, Department of Information Technology, Sinhgad Academy of Engineering, Kodhwa, Pune, Maharashtra 411048, India, India, E-mail: elavarasi222@gmail.com

Received April 03, 2018; **Accepted** April 11, 2018; **Published** April 19, 2018

Citation: Rajguru P, Dhomse J, Pawar PY (2018) Securing Online Transaction Using Visual Cryptography. J Telecommun Syst Manage 7: 158. doi: 10.4172/2167-0919.1000158

Steganography scheme

For hiding a message we are using steganography. The key concept behind steganography is that message to be transmitted is not detectable to casual eye. 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. Only combining the k shares or more give the original secret image.

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.

The proposed System has the following Architecture in Figure 1. The System is divided into following parts:

User login

User Login is the act or process of entering user accounts for the reason to do online transaction.

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 in Figure 2.

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.

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

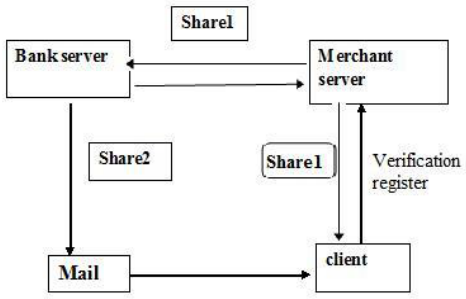

Figure 1: System architecture.

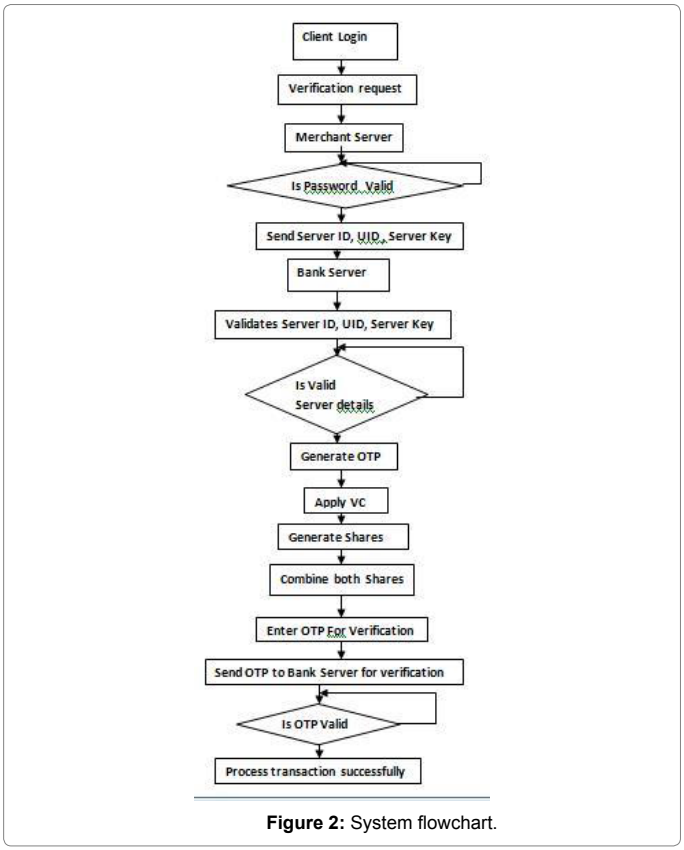

Figure 2: System flowchart.

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.

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.

Conclusion

In this paper, we are developing Visual cryptography scheme in which we are generating shares for general access structure. 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. Roy S, Venkateshwaran P (2016) Online Payment System Using Visual

Cryptography and Steganography 2016 Online International Conference on Green Engineering And Technologies.

2. James D, Pjilip M (2012) A Navel Antiphishing Framework Based On Visual Cryptography.
3. Yang D, Doh I, Chae K (2017) Enhanced password Processing Scheme Based On Visual Cryptography and OCR.
4. Khaimar S, Kharta R (2017) Online Fraud Transaction Prevention System Using Extended Visual Cryptography And QR Code.