International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 03 | Mar-2016 www.irjet.net p-ISSN: 2395-0072

Visual Cryptography and Steganography Techniques for Secure E-Payment System

Sandip Bhasme[1], Arvind Abu[2], Kaustubh Gandhi[3], Professor Ritu Phadnis[4]

[1]*Sandip Bhasme, Dept. Of Computer Engineering, APCOER, Maharashtra, India*
[2]*Arvind Abu, Dept. Of Computer Engineering, APCOER, Maharashtra, India*
[3] *Kaustubh Gandhi, Dept. Of Computer Engineering, APCOER, Maharashtra, India*
[4]*Professor Ritu Phadnis, Dept. Of Computer Engineering, APCOER, Maharashtra, India*

Abstract -

In recent days there is rapid growth in online payment and E-Commerce market . Major factors that affects to customers in online shopping and payment are fraud in debit card or credit card and personal information security. personal Identity theft and phishing attack are common issues of online shopping. Phishing is a method of stealing personal confidential information as like password, bank details, username, credit card detail information from victims. It is a social engineering technique used to deceive users. In this paper new method is proposed that steganography and visual cryptography. these methods represents new approach which will provide limited information for fund transfer. This method ensures the security to the customer's data and decreases customer's risk and prevents identity theft.

Key Words: Blowfish, steganography, visual cryptography, OTP(One time Password), Phishing.

1.INTRODUCTION

Online shopping is the process of retrieving the product information via the web and issue of purchase order/product through electronic purchase request, filling of bank's credit or debit card information and shipping of order/product by home delivery using courier service. Identity theft and phishing are the common dangers of online shopping. Using the another customers Identity is the stealing of that persons identity in the form of personal/private information and misusing that personal information for making purchase/buying and opening of fake bank accounts or arranging credit and debit cards. In 2012 consumer information was misused for an average of 48 days as a result of identity theft. Phishing is an illegal method which employs both social and technical subterfuge to steal or misusing customers personal identity data and financial and bank account credentials. Payment Service, Financial and Retail Service are the most focused industry sectors for attacks using phishing method. Secure Socket Layer (SSL) encryption inhibits the interference of customer personal data in transit between the customer and the online merchant. However, one must still trust merchant and its employees not to misuse customer data for their purchases and orders and not to sell the information to others attackers/intruders .

a new method is Discovered, that goes through both steganography and visual cryptography, which reduces detailed information sharing between customer and online merchant or owner and enable successful fund transaction from customer's account to merchant's account thereby safety to customer information and avoiding misuse of information at merchant's side. The method proposed is applied to E-Commerce and online shopping but can be easily extended for other applications like online banking..

2. BASICS OF STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

Steganography is the method for hiding of a message within another message so that hidden message is indistinguishable or unidentical. The key concept behind steganography is that message to be transmitted is not detectable to normall eye. Text , videos, image, audio,etc are used as a cover media message for hiding data in steganography. In text steganos, message can be hidden by shifting word and line, in open spaces, in word sequence. Properties of a sentence such as number of words, characters, vowels, and position of vowels in a word are also used to hide the message. The main advantage of preferring this text based steganography over other steganography techniques is its smaller memory requirement and simpler communication.

Visual cryptography: it is a cryptographic method that allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes using sight reading. it can be decrypt the job of person

This is the best visual cryptography methods has been credited to Moni Naur and Adi Shamir, who developed it in 1994. They Described visual secret Sharing method, where an image was broken up into no of shares so that only someone with all nth shares could decrypt the image, while

any n – 1 shares revealed no information about the original image. Each and every share was printed on a separate and different transparency, and decryption was performed by overlaying the no of shares. When all n shares were overlaid, the original image would appear /created. There are several generalizations of the basic scheme including k-out-of-n visual cryptography.

3. LITERATURE REVIEW

3.1 Phishing

What is Phishing? Phishing is a ambigious communication. It's Facilitates identity theft environment in website. thefts or attackers use fake email messages that appear to be originating from legitimate businesses.

Phishing attacker key point is

1. Attacker sends an e-mail.
2. Internet user is re-directed to a mimicking
3. website to key in their personal identification details.
4. The attacker will then use this information to commit identity fraud.

Effects of Phishing:

There are two main effect of phishing:

1. Inflicts financial losses
2. Corrodes consumer trust

There are so many phishing techniques such as

- Email / Spam
- Web Based Delivery
- Instant Messaging
- Trojan Hosts

Web Based Delivery:

Web based delivery method is one of the most sophisticated phishing techniques. Also known as "man-in-the-middle," the hacker or attacker is found in between the original website and the phishing systems. The phisher accesses well as traces details of the customers during a transaction between the legitimate website and the user. As the customer continues to send data, it is catched and store by the phishers/attacker.

Instant Messaging:

It is the method in which the user receives a message with a link directing them to a fake phishing website which has the same look and feel as the actual original website. If the user doesn't look at the URL, it may be hard to check the difference between the fraud and original websites. Then, the user is asked to provide personal sensitive data on the page. For phisher/attacker personal use they can use customers stolen data.

3.2 Steganography

a] Text-Based Steganography:

It uses the features of english Language like inflexion, fixed word order and use of periphrases for minimizing data rather than using properties of a statement .

B] BPCS Steganography:

The minimizing information capacity of a true color image is around mostly 50% . A sharpening operation on the duplicate image increases the embedding capacity quite a littel bit. Randomization of the secret data by a compression operation makes the enclosing data more unreal. The steganos program for each user is easy. It further protects against bug on the embedded information. BPCS steganography is most secured method and provides high security.

3.3 Visual Cryptography

A] Halftone visual cryptography:

Using half toning novel technique achieves visual cryptography. Based on the blue-noise dithering principles, this method promote the void and cluster algorithm to encode a secret binary image into halftone shares (images) carrying powerful visual information.

B] 2-0ut-2 Visual Cryptography:

In 2 out 2 visual cryptography Every secret pixel of the original binary image is converted into four sub pixel of two share images. It can be recovered by simple stacking process. This is dissimilar to using the logical OR operation between the shares

4. SYSTEM ARCHITECTURE

In this Architecture there are three main parts that are

1) Client,
2) Merchant server
3) Bank server.

• Client:

Client is a customers who wants to buy some product online on merchant site, but it is necessary that the customer knows about the merchant site is fraud or real. For that user first enter OTP which can generated by bank after that they verify the merchant site is phishing or not. After know that merchant site is real customer complete further proceed and select or buy product.

• Merchant Server:

Merchant server hosts the original website it created from all the database of products it is managed by DBA or it can be registered with bank server. Merchant verify if the user is authentic or not by using Login functionality. Merchant sends its Server ID and Unique Customer ID to bank server for verification purpose. Adding

removing products into cart and Managing database of products or Also checking transactions that has happened.

• Bank Server:

Using client UID or merchant id bank server verifies client and merchant server. For OTP Bank server creating Hash Function. It divide's OTP into two share's and this OTP shares sends to merchant and client. At last verify if OTP entered is correct or not.

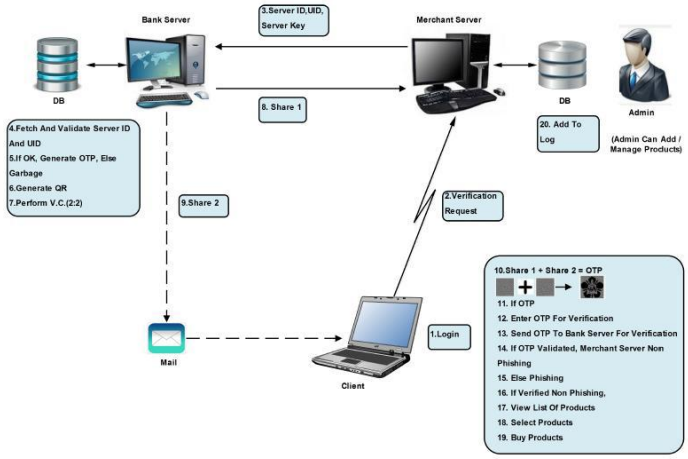

Fig 1: System Architecture.

ADVANTAGES

The proposed system minimize customer information sent to the online merchant it also provides two way authentication i.e. authenticating client and merchant server. It helps to prevent phishing and identity theft.The system provides security to users data. The using of steganography technique it ensures that the CA does not know customer aunthentication password thus maintaining customer privacy.

5. ALGORITHMS

5.1 Blowfish Algorithm

Blowfish is a method used for fast block cipher, except when changing keys. every new key needs pre-processing equivalent for encrypting near about 4 KB of text data , which is very slower as compared to other block ciphers techniques. This avoids its usage in perticular app, but it's not a problem in others applications.

Blowfish: it was one of the 1st safe and secure block ciphers not subject to any patents and therefore freely available for all users to use. This popularity benifit has contributed in cryptographic software.

1] Encryption algorithm has important role in securing the data in storing also in transferring it. The encryption algorithms are divided into two types as Symmetric (secret) key encryption and Asymmetric (public) key encryption.

2] In Symmetric key encryption the only one key is used for both encryption and decryption of secrete data.

3] In asymmetric key encryption uses two keys, one for encryption and other for decryption.

Steps of encryption and decryption:
Step 1: Get width and height of the image
Step 2: Horizontal block=image width/2
Step 3: Vertical block =image height/2
Step 4: Number of block = horizontal block * vertical block
Step 5: Encrypt all the pixels

6. CONCLUSION

A secure E-payment system for online shopping is proposed by combining steganography and visual cryptography that provides customer data minimizing and prevents misuse or fraud of data at merchant's side.customer data security or avoiding the identify theft this method is concerned. In comparison to other banking application which uses steganos and visual cryptography are basically applied for physical banking, the proposed method can be applied for E-Commerce with focus area on payment during online shopping as well as physical banking.

REFERENCES

[1] Souvik Roy, P.Venkateswaran, "Online Payment System using Steganography and Visual Cryptography," Proceedings of IEEE Students' Conference on Electrical, Electronics and Computer Science,2014.

[2] Pranita P. Khairnar, Prof. V. S. Ubale, " Steganography Using BPCS technology,"in Proc. International Journal Of Engineering And Science , May 2013. Vol.3(Issue 2),pp 08-16.

[3] Jihui Chen, Xiaoyao Xie, and Fengxuan Jing, "The security of shopping online," Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), vol. 9, pp. 4693-4696, 2011

[4] Anti-Phishing working group (APWG), "Phishing Activity Trends Reports,2013 " http://www.apwg.org/reports/apwg_trends_report_q2_2013.pdf

[5] Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, "Techniques for Data Hiding," IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 313-336, 1996.

[6] J.C. Judge, "Steganography: Past, Present, Future," SANS Institute, November 30, 2001.

[7] Hu ShengDun, U. KinTak, "A Novel Video Steganography Based on Non-uniform Rectangular Partition," Proceding of 14th International Conference on Computational Science and Engineering, pp. 57-61, Dalian, Liaoning, 2011