

Secure E-Payment System using Visual Cryptography

^{#1}Kaustubh Gandhi, ^{#2}Sandip Bhasme, ^{#3}Arvind Abu, ^{#4}Prof.Ritu Phadnis

¹kaustubh2151@gmail.com

²bhasmesandy123@gmail.com

³kulkarniarvind78@gmail.com

^{#123}Department of Computer Engineering

^{#4}Prof. Department of Computer Engineering4



Anantrao Pawar College of Engineering and Research
Parvati,Pune

ABSTRACT

In recent time there is rapid growth in E-Commerce market. Major concerns for customers in online shopping are debit card or credit card fraud and personal information security. Identity theft and phishing are common threats of online shopping. Phishing is a method of stealing personal confidential information such as username, passwords, credit card details from victims. It is a social engineering technique used to deceive users. In this paper new method is proposed that uses text based steganography and visual cryptography. It represents new approach which will provide limited information for fund transfer. This method secures the customer's data and increases customer's confidence and prevents identity theft.

Keywords: E-Commerce, steganography, visual cryptography, Online Shopping.

ARTICLE INFO

Article History

Received: 3rd February 2016

Received in revised form : 4th February 2016

Accepted: 7th February 2016

Published online : 8th February 2016

I. INTRODUCTION

Online shopping also called as e-tail is a way of purchasing products over internet. It allows customers to buy goods or services using web browsers and by filling credit or debit card information. In online shopping the common threats are phishing and identity theft. Identity theft is a form of stealing someone's identity i.e. personal information in which someone pretends to be someone else. The person misuses personal information for purchasing or for opening bank accounts and arranging credit cards. As a result of identity theft, the customer's information was misused for an average of 48 days in 2012. Phishing is a method of stealing personal confidential information such as username, passwords, credit card details from victims. It is a criminal mechanism that uses social engineering. Phishing email directs the users to visit website where they take users personal information such as bank account number, password. It is email fraud conducted for identity theft. In 2013, Financial and Retail Service, Payment service are the targeted industrial sectors of phishing attacks. The method which is proposed in this paper uses both steganography and visual cryptography. It reduces information sharing between customer and merchant

server and safeguards customers information. It enables successful fund transfer to merchant's account from customer's account and prevents misuse of information at merchant side.

II. STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

Steganography is a technique or a method of hiding the information into the image. It is the practice of concealing a file, message or image into another file, message or image. Steganography combines the word steganos and graphein. The meaning of steganos is covered or protected, the meaning of graphein is writing. The term steganography was first used in 1499 by Johannes Trithemius. The message which is hidden may be in invisible link between the visible lines of personal letter. The advantage of this technique is that the hidden message does not pay attention to itself as an object scrutiny. It includes hiding of information within computer files. For the transmission purpose media files are considered as ideal because of their large size. Electronic communication involves steganography coding within transport layer. This term has been widely used including recent times even present day. In ancient

Greece people wrote text on wood and protect it with wax. In 1985 steganography entered into modern world with the advantage of personal computer being applied to traditional steganography problems. Hiding message within lowest bits of noisy images. Concealing information within encrypted data. The message which is to be hidden is encrypted then used to overwrite part of a much larger block of encrypted data. Cryptography is the practice and the study of techniques for secure communication in the presence of third parties. It is special encryption technique in which visual information is encrypted in such a way that decryption does not require a computer. This technique was developed by Moni Naor and Adi Shamir. Cryptography was developed in year 1994. Visual cryptography uses two transparent images. One image contains random pixels and other contains secret information. It is impossible to retrieve secret information from one of the images. But both transparent images are required to reveal the information. In this technique the image was broken into n number of parts so that someone can decrypt this image using these n numbers of parts.

III. LITERATURE SURVEY

Phishing:

a) Microsoft Phishing Filter uses a combination of Microsoft's URL Reputation Service (URS) and local heuristics built into the IE7 browser.

b) Netscape Browser 9.0 includes a built in phishing filter which relies solely on a blacklist, which is maintained by AOL and updated frequently.

Steganography:

a) Text-Based Steganography: It makes use of features of English Language like inflexion, fixed word order and use of periphrases for hiding data rather than using properties of a statement.

b) BPCS Steganography: The information hiding capacity of a true color image is around 50%. A sharpening operation on the dummy image increases the embedding capacity quite a bit. Randomization of the secret data by a compression operation makes the embedded data more intangible. The steganography program for each user is easy. It further protects against eavesdropping on the embedded information. It is most secured technique and provides high security.

Visual Cryptography:

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

b) 2-Out-2 Visual Cryptography: Every secret pixel of the original binary image is converted into four sub pixel of two share images and recovered by simple stacking process. This is equivalent to using the logical OR operation between the shares.

IV. ADVANTAGES

1. The proposed system provides two way authentication i.e. authenticating client and merchant server.
2. It helps to prevent phishing.
3. It prevents identity theft.
4. The system provides security to users data.

V. PROPOSED SYSTEM

An online payment system permits a consumer to make a payment to an online merchant or a supplier. Payment portal, a channel between consumers and payment processors, use numerous security tools to secure a consumer's payment information, ordinarily card data, during an online transaction. However, the security provided by a payment portal cannot completely protect a consumer's payment information when a merchant is also allowed to obtain the payment information in specific form. Moreover, not all merchants provide a secure payment environment to their consumers and, in spite of having a standard payment plan, adhere to it. Consequently, this exposes a consumer's payment information to risks of being compromised or misused by merchants or stolen by hackers and spammers. In this paper we propose a new approach for online transaction in which a consumer's payment information is minimized to that is only needed for transfer of funds. A consumer sends his payment information directly to a payment portal and a payment portal, upon verifying the consumer, allows the transaction and sends a payment receipt to the appropriate merchant. We use the text steganography and visual cryptography to securely transfer funds to a merchant and protect a consumer's payment data from any Internet susceptibilities.

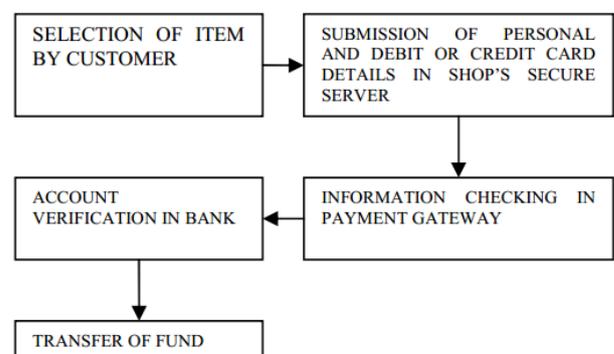


Fig 1. Transaction in online shopping

Modules:

Customer:

Customer can shopping any product and paid through online using card payment. But he has not any security policy our project give the advance security using cryptography technique.

Bank:

Bank check the valid customer for authentication that person is valid user or not.

REFERENCES

- [1] 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.
- [2] Javelin Strategy & Research, "2013 Identify Fraud Report," <https://www.javelinstrategy.com/brochure/276>.
- [3] Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report,2013,"http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf.
- [4] Jack Brassil, Steven Low, Nicholas Maxemchuk, Larry O’Gorman, "Hiding Information in Document Images," Proceedings of the 1995 Conference on Information Sciences and Systems, Johns Hopkins University, pp. 482-489, 1995.
- [5] J. Chen, T. S. Chen, M. W. Cheng, "A New Data Hiding Scheme in Binary Image," Proceeding of Fifth International Symposium on Multimedia Software Engineering, pp. 88-93, 2003.
- [6] Hu ShengDun, U. KinTak, "A Novel Video Steganography Based on Non-uniform Rectangular Partition," Proceeding of 14th International Conference on Computational Science and Engineering, pp. 57-61, Dalian, Liaoning, 2011.
- [7] Daniel Gruhl, Anthony Lu, Walter Bender, "Echo Hiding," Proceedings of the First International Workshop on Information Hidding, pp. 293-315, Cambridge, UK, 1996.
- [8] Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, "Techniques for Data Hiding," IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 313-336, 1996.
- [9] K. Bennet, "Linguistic Steganography: Surevey, Analysis, and Robustness Concerns for Hiding information in Text," Purdue University, Cerias Tech Report 2004—2013.
- [10] J.C. Judge, "Steganography: Past, Present, Future," SANS Institute, November 30, 2001.