ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (88-92), Month: January-April 2016, Available at: www.noveltyjournals.com

Online Secure Payment System Using Visual Cryptography and Steganography

Bhoite Bhupali Vikas[1], Rathod Varsha Digambar[2], Shaikh Hina Lala[3],
Bhapkar Shivanjali Bhimrao[4], Mrs. Prof. R. P. Karande[5]

Department of Computer Engineering NBN Sinhgad School of Engineering, Pune-411041, India

Abstract: **There is a rapid growth in E-Commerce market in recent time throughout the world. Also with the ever increasing popularity 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 approach. Only limited information is provided which is necessary for fund transfer during online shopping thereby safeguarding customer data and increasing customer confidence and preventing identity theft. The method uses combined application of visual cryptography and steganography for this purpose.**

Keywords: **Information security; Steganography; Visual Cryptography; Online shopping.**

1. INTRODUCTION

Online shopping is the retrieval of product information through the Internet and issue of purchase order through electronic purchase request, filling of credit or debit card information and shipping of product by mail order or home delivery by courier.

[1]. Identity theft and phishing are the dangers of online shopping. Identity theft is the stealing of someone's identity in the form of personal information and misusing that information for making purchase and opening of bank accounts or arranging credit cards.

Phishing is a criminal mechanism that employs both social engineering and technical loop hole to steal consumers' personal identity data and financial account credentials. In 2013, Payment Service, Financial and Retail Service are the most targeted industrial sectors of phishing attacks [3]. Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the online merchant and consumer. However, one must trust merchant and its employees not to use consumer information for their own purpose of purchases and not to sell the information to others.

In this paper, a new method is proposed, that uses text based visual cryptography and steganography, which minimizes information sharing between consumer and online merchant but enable successful fund transfer from consumer's account to merchant's account but safeguarding consumer information and preventing misuse of information at the merchant side. The proposed method is specifically for E-Commerce but can also easily be extended for online as well as physical banking.

2. RELATED WORK

[1] The online shopping is increasingly being accepted Internet users, which reflects the online shopping convenient, fast, efficient and economically advantageous. Online shopping, personal information security is a major problem of the Internet. Summarizes the characteristics of online shopping and the current development of the main safety problems, and make online shopping related security measures and transactions.

[2] The APWG continues to refine its tracking and reporting methodology and to incorporate new data sources into our reports. APWG has re-instated the tracking and reporting of unique phishing reports (e-mail campaigns) in addition to unique phishing sites. An e-mail campaign is an unique e-mail sent out to multiple users, directing them to a specific phishing web site (multiple campaigns may point to the same web site). APWG counts unique phishing report e-mails as those in a given month with the same subject line in the e-mail.

[4] A new data hiding scheme for binary image authentication that has a small distortion of the cover image is proposed in this paper. Using the data-embedding algorithm that is based on Hamming codes, the proposed scheme embeds authentication information into the cover image with flipping only a small number of pixels. A special type of the pixels are selected and flipped by a new algorithm to minimize visual distortion. This new algorithm is based on ELSSM (Edge Line Segment Similarity Measure). Randomly shuffling the bit-order of the authentication information to be embedded, the information can only be extracted by the designated receiver who has the symmetric key. We employ two measurement metrics: miss detection rates for the degree of security and PSNR (Peak Signal-to-Noise Ratio) and ELSSM for the degree of the image distortion to demonstrate the feasibility of the proposed scheme. We analyze the proposed scheme and the previous schemes using these metrix. The analysis reveals that the proposed scheme requires less image distortion than the previous schemes whilst achieving the same level of the miss detection rate. Experimental results demonstrate that the proposed scheme is more resilient against recent steganalysis attacks than the previous schemes.

3. TRANSACTION IN ONLINE SHOPPING

Fig. 2 shows the traditional online shopping. In which consumer selects items from online shopping portal and then is directed to the payment page. Online merchant may have its own payment system or can take advantage of third party payment systems such as PayPal, payonline system, WebMoney and any others. In the payment portal, consumer submit his or her credit or debit card details such as credit or debit card number, name on the card, expiry date of the card.

Details of information sought from shopper vary from one payment gateway to the another. For example, payment in IRCTC requires Personal Identification Number (PIN) when paying using debit card whereas shopping in Flipkart or Snapdeal requires Visa or Master secure code. In addition to that merchant may require a Card Verification Value code, CVV (CVV2 for Visa, CVC2 for MasterCard). According to the PCI Data Security Standard [10], merchants are debar from storing CVV information or PIN data and if permitted card information such as name, card number and expiration date is stored, certain security standards are required. Recent high profile breaches such as in Epsilon, Sony’s PlayStation Network and Heartland Payment Systems show that card holders’ information is at risk both from inside and outside. A solution to this is, merchants can be forced to be a PCI complaint but cost to be a PCI complaint is large and the process is complex and time consuming [11] and it will solve part of the problem. One still has to trust the merchant and its employees not to use card information for there own purposes.

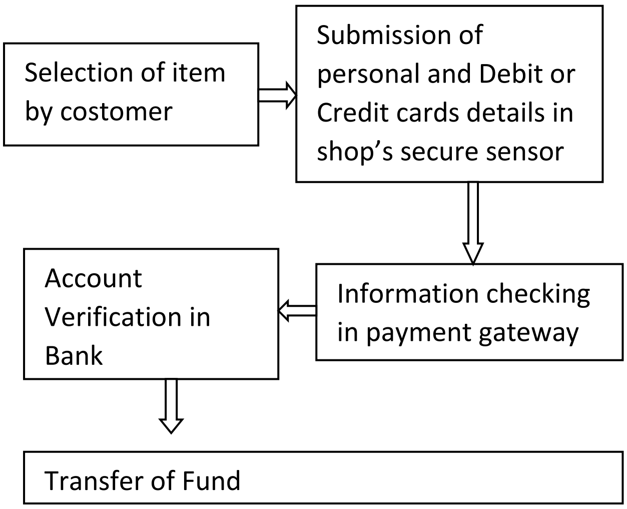
Selection of item by costomer
Submission of personal and Debit or Credit cards details in shop’s secure sensor
Information checking in payment gateway
Account Verification in Bank
Transfer of Fund

Fig 1: Transaction in Online Payment System

4. PROPOSED PAYMENT METHOD

In the proposed system, information which is submitted by the consumer to the online website at merchant's site is minimized by providing only minimum information. It will only verify the payment made by the consumer from its account. This is accomplished by the introduction of a central Certified Authority (CA) and combined application of visual cryptographic Steganography and technique. The information which is obtained by the merchant will only validate receipt of payment from authentic consumer. It can be in the form of account number related to the card used for shopping.

1. Sequence Of Proposed Payment System:

Step 1: Consumer registration process.

Step 2: Share 1 generated using Visual Cryptography and Steganography.

Step 3: Consumer choose for online shopping (Merchant Side).

Step 4: Consumer completes the shopping process and is directed to payment process.

Step 5: Consumer submits the share 1 provided to him while registration and Merchant provides its account details.

Step 6: CA verify the consumer share and bank share which is combined.

Step 7: If the share is valid then the transaction will be synchronized with the bank. If share is not valid then error message will be sent via mail.

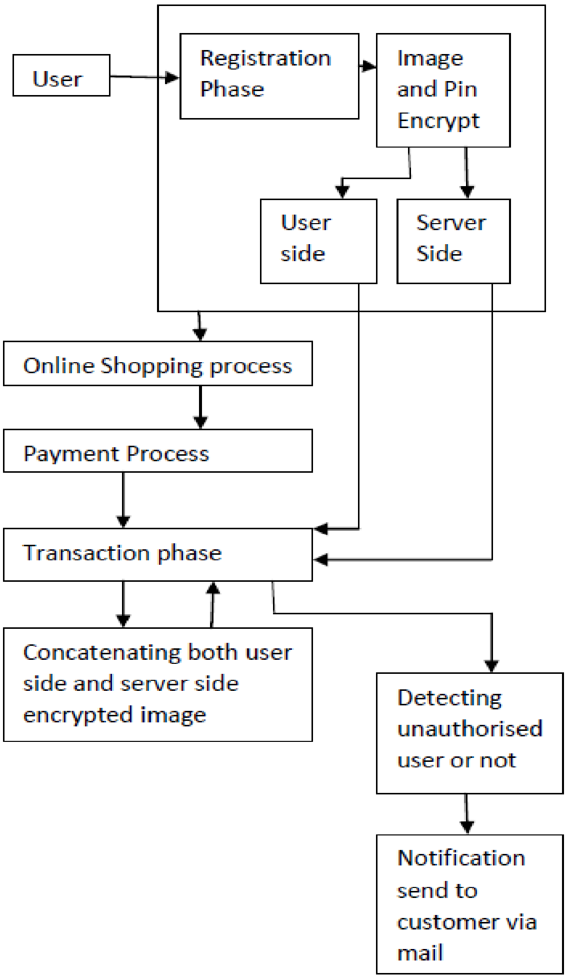
User
Registration Phase
Image and Pin Encrypt
User side
Server Side
Online Shopping process
Payment Process
Transaction phase
Concatenating both user side and server side encrypted image
Detecting unauthorised user or not
Notification send to customer via mail

Fig2 :Proposed payment system

2. Steganograhy algorithm using ASCII Code   Encoding Steps:

- Take input in the form of text.
- ASCII code is used to represent each letter.
- Obtained ASCII code is represent in 8 bit binary number.
- The 8 bit binary number is then divided into two 4 bits parts.
- Each four bit part representing a number in the range 0 to F hex representations is then used to choose corresponding suitable words from the table below:

Number	Words	Number	Words
0	Am	8	I
1	Be	9	Jai
2	Come	A	Key
3	Dave	B	Lime
4	Elegant	C	Me
5	Fine	D	No
6	Go	E	Oh
7	Hi	F	Plan

Decoding Steps:

- Word of cover message is taken and represented by corresponding number from the table.
- Each number is represented by its four bit binary.
- 4 bit binary numbers are combined to obtain 8 bit number.
- ASCII codes are obtained from 8 bit numbers.
- Finally secret message is recovered from ASCII codes.

5. ALGORITHM

1. BPCS (Bit-Plane Complexity Segmentation) Steganography algorithm:

The algorithm can be described in concise steps as follows [12].

a) Convert the carrier image (of any file-format) from PBC (Pure Binary Code) to CGC (Canonical Grey Code) system and in png format.

b) Perform the histogram analysis.

c) After that the bit-plane analysis is performed.

d) Perform size-estimation i.e. calculate the places where we can store the secrete image.

e) Perform bit plane complexity segmentation on image i.e. embed secrete blocks into carrier image.

f) After embedding mail that image to another user.

g) For extracting the embedded image performs de- steganography which is exactly opposite to steganography.

2. Visual cryptography Algorithm:

Visual cryptography allows the visual information to be encrypted in such a way that their decryption can be performed by human visual system. 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 the logical OR operation between the shares [13].

6. CONCLUSION

A payment system for online shopping is proposed by combining text based steganography and visual cryptography that provides customer data privacy and also prevents misuse of data at merchant's side. The method is concerned only with prevention of identity theft and customer data security also. In comparison to other banking application which uses steganography 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.

7. FUTURE SCOPE

The payment system can also be extended to internet or physical banking. Shares may contain signature or consumer image in addition to consumer authentication password. In the bank, consumer submits its own share and consumer physical signature is validated against the signature obtained by combining consumer's share and CA's share along with validation of consumer authentication password. It prevents misuse of stolen card and stops illegitimate consumer. This can be also applied for standardizing a particular product or an organization by having their personal identification secured.

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] 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] K. Bennet, "Linguistic Steganography: Surevey, Analysis, and Robustness Concerns for Hiding information in Text," Purdue University, Cerias Tech Report 2004—2013.

[7] Bharati Krishna Tirthaji, "Vedic Mathematics and its Spiritual Dimension," Motilal Bansari Publishers,1992.

[8] http://oxforddictionaries.com/words/what-is-the-frequency-of-the-letters-of-the-alphabet-in-english.

[9] Kalavathi Alla, Dr. R. Siva Rama Prasad, "An Evolution of Hindi Text Steganography," Proceding of Sixth International Conference on Information Technology, pp. 1sssss577-1578, Las Vegas, NV, 2009.

[10] PCI DSS Quick Reference Guide v2.0, pp 14-15.

[11] https://www.braintreepayments.com/blog/pci-compliance-and-the-cost-of-a-credit-card-breach.

[12] 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.

[13] Chetana Hegde, Manu S, P Deepa Shenoy, Venugopal K R, L M Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications,",in Proc. 16th IEEE International Conference on Advanced Computing and Communications,2008.