A secure framework for online transaction involving cardholder and merchant

Santosh Kumbhar, Bharat Tidke

ME. Computer Network, Dept. of CSE., Savitribai Phule Pune University,Pune, Maharashtra, India
Assistant Professor, Dept. of CSE., Savitribai Phule Pune University, Pune, Maharashtra India

Abstract **A rapid growth in E-Commerce market is seen in recent time throughout the world. With 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 is a new approach for providing limited information only that is necessary for amount transfer during online shopping hereby safeguarding customer data and increasing customer confidence and preventing identity theft. The method uses combined application of steganography and visual cryptography for this purpose.**

IndexTerms **- Information security; Steganography; Visual Cryptography; online shopping**

I. INTRODUCTION

Online shopping is the recovery of product information via 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 common dangers of online shopping. Identity theft is the stealing of someone's identity in the form of personal information and misuse of 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 subterfuge to steal consumers' personal identity data and financial account credentials [2]. Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between the consumer and the online merchant. However, one must still trust merchant and its employees not to use consumer information for their own purchases and not to sell the information to others.

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

Steganography is the art of hiding of a message within another so that hidden message is indistinguishable. The key concept behind steganography is that message to be transmitted is not detectable to casual eye. Text [3], image [4], video [5], audio [6] are used as a cover media for hiding data in steganography. In text steganography, message can be hidden by shifting word and line [4], in open spaces [7], in word sequence [8]. Properties of a sentence such as number of words, number of characters, number of vowels, position of vowels in a word are also used to hide secret message. The advantage of preferring text steganography over other steganography techniques is its smaller memory requirement and simpler communication [9]. Visual Cryptography (VC), proposed by Naor et al. in [10], 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.

II. RELATED WORK

A brief survey of related work in the area of banking security based on steganography and visual cryptography is presented in this section. A customer authentication system using visual cryptography is presented in [11] but it is specifically designed for physical banking. A signature based authentication system for core banking is proposed in [2] but it also requires physical presence of the customer presenting the share. [13] Proposes a combined image based steganography and visual cryptography authentication system for customer authentication in core banking. A message authentication image algorithm is proposed in [14] to protect against e-banking fraud. A biometrics in conjunction with visual cryptography is used as authentication system [15].

III. PROPOSED METHODOLOGY AND DISCUSSION

A. *Proposed Text Based Steganography Method*

Proposed text based steganography uses characteristics of English language such as inflexion, fixed word order and use of periphrases for hiding data rather than using properties of a sentence. This gives flexibility and freedom from the point view of sentence construction but it increases computational complexity. The steganography technique is based on Vedic Numeric Code [16] in which coding is based on tongue position. For applying the Vedic code to English alphabet, frequency of letters in English vocabulary [17] is used as the basis for assigning numbers to the letters in English alphabet. Number assignments of letters are

shown in table 1. No separate importance is given for vowels and consonants as compared to [18]. Each letter is assigned a number in the range of 0 to 15. For different frequencies, different numbers are assigned to the letters. Number assigned in range (N+0.99) % to (N+0.3) % and (N+0.2) % to (N+0.01) % is same where N is any integer from 0 to 11. It basically represents frequency of letters in integer form. Above number assignment method is used to maximize no of letters in a particular assigned number group which in turn gives flexibility in word choosing and ultimately results in suitable sentence construction.

Table 1: Number Assignment

c	Number Assigned	Letter	Number Assigned
E	15	M	7
A	14	H	7
R	13	G	6
I	13	B	5
O	12	F	4
T	11	Y	4
N	11	W	3
S	10	K	3
L	10	V	3
C	9	X	2
U	8	Z	2
D	8	J	1
P	7	Q	0

B. *Encoding Steps*

- Representation of each letter in secret message by its equivalent ASCII code.
- Conversion of ASCII code to equivalent 8 bit binary number.
- Division of 8 bit binary number into two 4 bit parts.
- Choosing of suitable letters from table 1 corresponding to the 4 bit parts.
- Meaningful sentence construction by using letters obtained as the first letters of suitable words.
- Omission of articles, pronoun, preposition, adverb, was/were, is/am/are, has/have/had, will/shall, and would/should in coding process to give flexibility in sentence construction.
- Encoding is not case sensitive.

C. *Decoding Steps*

- First letter in each word of cover message is taken and represented by corresponding 4 bit number.
- 4 bit binary numbers of combined to obtain 8 bit number.
- ASCII codes are obtained from 8 bit numbers.
- Finally secret message is recovered from ASCII codes.

D. *Transaction in Online Shopping*

In traditional online shopping as shown in Fig. Online merchant may have its own payment system or can take advantage of third party payment systems such as PayPal, payonlinesystem, WebMoney and 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.

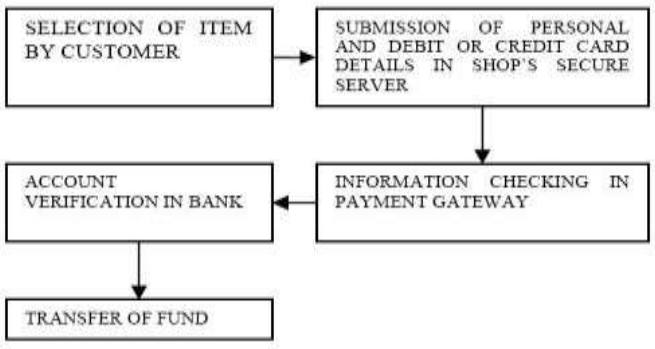

Fig.1. Block diagram of online transaction shopping

Details of information sought from shopper vary from one payment gateway to another. For example, payment in IRCTC website 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), which is basically an authorizing code in CNP transactions. According to the PCI Data Security Standard [19], merchants are prohibited 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. However 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 outside and inside. A solution can be forcing merchant to be a PCI complaint but cost to be a PCI complaint is huge and the process is complex and time consuming [20] and it will solve part of the problem. One still has to trust the merchant and its employees not to use card information for their own purposes.

IV. Proposed Payment Method

In the proposed solution, information submitted by the customer to the online merchant is minimized by providing only minimum information that will only verify the payment made by the said customer from its bank account. This is achieved by the introduction of a central Certified Authority (CA) and combined application of steganography and visual cryptography. The information received by the merchant can be in the form of account number related to the card used for shopping. The information will only validate receipt of payment from authentic customer. The process is shown in Fig.2. In the proposed method, customer unique authentication password in connection to the bank is hidden inside a cover text using the text based steganography method as mentioned in section IV. Customer authentication information (account no) in connection with merchant is placed above the cover text in its original form. Now a snapshot of two texts is taken. From the snapshot image, two shares are generated using visual cryptography.

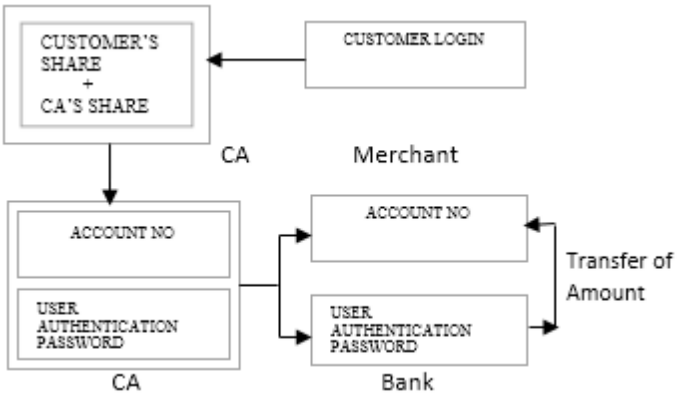

Fig. 2. Proposed payment method.

Now one share is kept by the customer and the other share is kept in the database of the certified authority. During shopping online, after selection of desired item and adding it to the cart, preferred payment system of the merchant directs the customer to the Certified Authority portal. In the portal, shopper submits its own share and merchant submits its own account details. Now the CA combines its own share with shopper's share and obtains the original image. From CA now, merchant account details, cover text are sent to the bank where customer authentication password is recovered from the cover text. Customer authentication information is sent to the merchant by CA. Upon receiving customer authentication password, bank matches it with its own database and after verifying legitimate customer, transfers amount from the customer account to the submitted merchant account. After receiving the amount, merchant's payment system validates receipt of payment using customer authentication information.

V. Experimental Study

To implement the text based steganography method, a secret message is considered. Suppose it is ―text.
text = 01110100011001010111100001110100. Result of encoding is shown in Fig. 3.

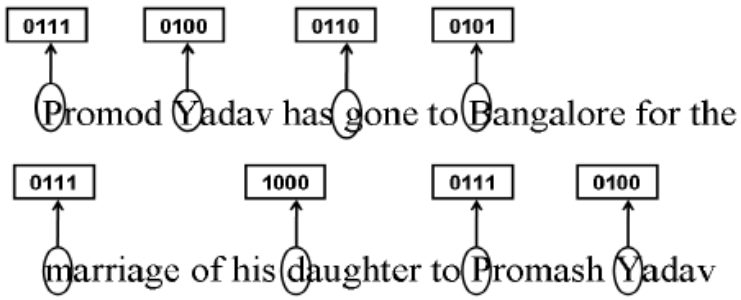

Fig. 3. Cover Image

The problem is that CA does not know to which bank to forward the cover text obtained from combining two shares. It can be solved by appending 9 digit routing or transit number of bank with customer authentication information. If ―text‖ is customer unique authentication password and account no of customer is 12345678910111, snapshot of cover text and account no is shown

in Fig. 4 and resultant shares by the application of visual cryptography on snapshot are Fig. 5 and Fig. 6. Fig. 5 shows share 1 kept by customer and Fig. 6 shows share 2 kept by CA. Fig. 7 shows the result of combing share 1 and share 2.

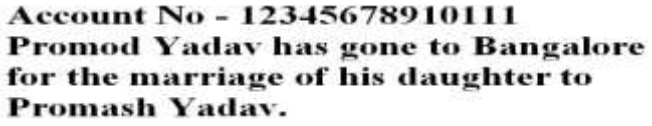

Fig. 4. Snapshot account no and cover text.

Fig. 5. Share 1 kept by customer.

Fig. 6. Share 2 kept by CA.

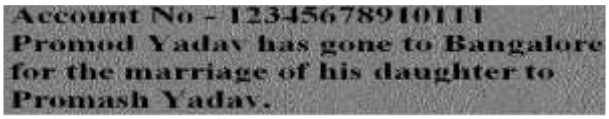

Fig. 7. Overlapping of share 1 and share 2.

VI. RESULT

Fig. 8. Encryption utility

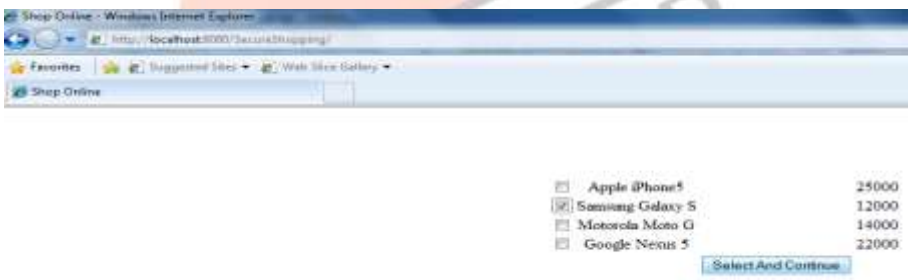

Fig. 9.Item Selection

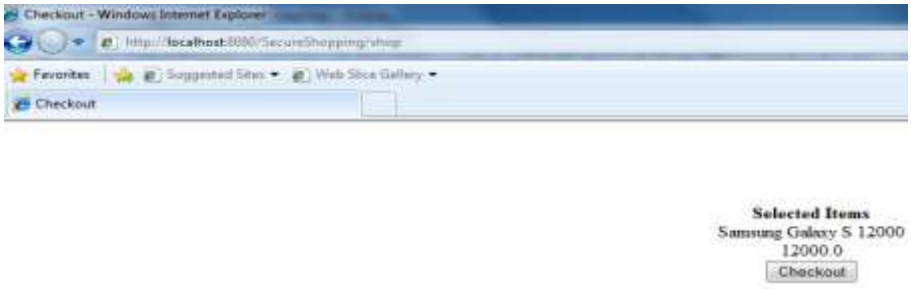

Fig. 10. Checkout

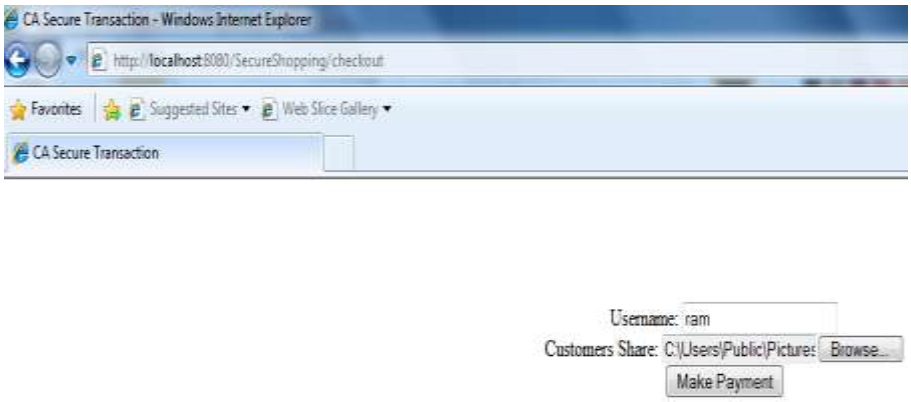

Fig. 11. CA Secure transaction

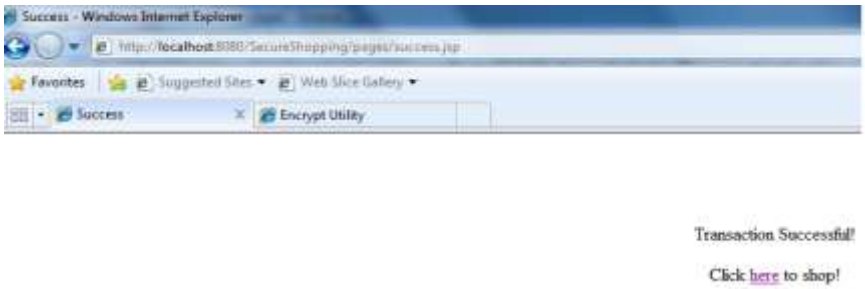

Fig. 12.Payment transfer from Customer account to Merchant account.

VII. Future Scope

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

VIII. Conclusion

A secure framework for online payment for online shopping is proposed by combining text based steganography and visual cryptography that provides customer data confidentiality and avoids misuse of data at merchant's side. The technique is concerned only with avoidance of identifying theft and customer data security. In comparison to other banking application which uses steganography and visual cryptography [12, 13, and 14], 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] Javelin Strategy & Research, "2013 Identify Fraud Report,"https://www.javelinstrategy.com/brochure/276.
[2] 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," Proceding 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.

[11] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptograhy: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.
[12] Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography," Proceedings of 2011World Congress on Information and Communication Technologies, pp. 1181-1186, Mumbai, India, 2011.
[13] Chetana Hegde, S. Manu, P. Deepa Shenoy, K. R. Venugopal, L M Patnaik, "Secure Authentication using Image Processing and Visual Cryptography for Banking Applications," Proceedings of 16th International Conference on Advanced Computing and Communications, pp. 65-72, Chennai, India, 2008.
[14] S.Premkumar, A.E.Narayanan, "New Visual Steganography Scheme for Secure Banking Application," Proceeding of 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 1013 – 1016, Kumaracoil, India, 2012.
[15] K. Thamizhchelvy, G. Geetha, "E-Banking Security: Mitigating Online Threats Using Message Authentication Image (MAI) Algorithm,"
Proceedings of 2012 International Conference on Computing Sciences (ICCS), pp. 276 – 280, 2012.
[16] S. Suryadevara, R. Naaz, Shweta, S. Kapoor, "Visual cryptography improvises the security of tongue as a biometric in banking system,"
Proceedings of 2011 2nd International Conference on Computer and Communication Technology (ICCCT), pp. 412 – 415, 2011.
[17] Bharati Krishna Tirthaji, "Vedic Mathematics and its Spiritual Dimension," Motilal Bansari Publishers, 1992.
[18] http://oxforddictionaries.com/words/what-is-the-frequency-of-theletters- of-the-alphabet-in-english.
[19] Kalavathi Alla, Dr. R. Siva Rama Prasad, "An Evolution of Hindi Text Steganography," Proceding of Sixth International Conference on Information Technology, pp. 1577-1578, Las Vegas, NV, 2009.
[20] PCI DSS Quick Reference Guide v2.0, pp 14-15.
[21] https://www.braintreepayments.com/blog/pci-compliance-and-the- cost of - a-credit-card-breach.
[22] Juan Chen, Chuanxiong Guo, "Online Detection and Prevention of Phishing Attacks," Proceedings of First International Conference on Communications and Networking in China (ChinaCom '06), pp. 1 - 7, Beijing, China, 2006.
[23] W. Stallings, Cryptography and network security: principles & practices, 3rd edition