International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN No.:2349-9745, Date: 2-4 July, 2015

A Survey Paper on Online Payment System using Stegnography and Visual Cryptography with Hidden Markov Model

Mr.Amit R Bramhechar[1],Prof.Dinesh Patil[2]

[1]*ME CSE SSGBCOE&T,Bhusawal,bramhecha.amit@gmail.com*
[2] *HOD CSE, SSGBCOE&T, Bhusawal, dineshonly@gmail.com*

Abstract—A Rapid Growth in E-Commerce is seen in recent time throughout the world. The Increasing Growth of International interconnected computer networks and the pervasive trends of using these networks as a new field of conducting the business process in stimulating the demands for new payment methods. There are so many methods which are available for payment but it must attain high level of security, speed, privacy, decentralization and must work on international level for electronic commerce to be accepted by the Consumer and Business. With Increasing the Demand of Shopping Online Through Home, The Debit or credit card fraud and personal information security are major concern for the customers, merchants and banks specifically in the case of CNP. This paper surveys the state of the art in payment technologies and sketches emerging developments.

Keywords- CNP-Card Not Present.

I.INTRODUCTION

Commerce is the most major aspect of any civilization. Improving Commerce can bring prosperity into all segments of society. In today's world there have been major changes to the commerce industry. The most important of it is the introduction of computers into the commerce industry. Computerization of commerce has taken the world by a storm. There are significant improvements in the areas of initiating sale of products, placing orders, making payments, and transfer of funds. This has led to a much better global economy and better living standards for all**.**

The popularity of online shopping is growing day by day. According to an ACNielsen study conducted in 2005, one-tenth of the world's population is shopping online. Online shopping is the retrieval 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. In 2nd quarter of 2013, Payment Service, Financial and Retail Service are the most targeted industrial sectors of phishing attacks [2]. 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.

1.1 Motivation For Online Payment

Internet is growing at an extremely fast pace. It has been estimated that there is a new web page every minute. The ease of use, efficiency and quickness, search engines and international presence of Internet has been drawing millions of users towards it. The vast market opportunity on the Web means a challenging atmosphere to software engineers who work behind the screen to make things happen on the Web. With the exploding Online market, the E-Commerce software needs to process the transactions efficiently, more securely and with lesser communication delays. The payment information contains private financial data that should be transferred using the most secure methodologies. This paper discusses the various methods employed to incorporate security into electronic payment systems.

II . LITERATURE SURVEY

Jaya ,Sidhart Malik, AbhinavAggarwal, Anjali SardanaPraposed A customer authentication system using visual cryptography [3] but it is specifically designed for physical banking. ChetanaHegadem, S. Manu, P. DeepaShenoy, K.R.Venugopal,L.M.Patniak proposed A signature based authentication system for core banking [4] but it also requires physical presence of the customer presenting theshare. K. Thamizhchelvy, Q. GeethaPraposed A message authentication image algorithm is pin [5] to protect against e-banking fraud. S.Suryadevara,R. Naaz, Shweta, S kapoor proposed A biometrics in conjunction with visual cryptography is used as authentication system [6].Ghosh and Reilly [7] have proposed credit card fraud detection with neural network. They have built a detection system, which is trained on a large sample of labeled credit card account transactions. These transactions contain example fraud cases due to lost cards, stolen cards, application fraud, counterfeit fraud, mail-order fraud, and non received issues (NRI) frauds.Chiu and Tsai [8] have proposed Web services and data mining techniques to establish a collaborative scheme for fraud detection in the banking industry. With this scheme, participating banks share knowledge about the fraud patterns in a heterogeneous and distributed environment. To establish a smooth channel of data exchange, Web services techniques such as XML, SOAP, and WSDL are used.The problem with most of the abovementioned approaches is that they require labeled data for both genuine, as well as fraudulent transactions, to train the classifiers. Getting the real-world fraud data is one of the biggest problem associated with credit card fraud detections. Also these approaches cannot detect new kinds of fraud for which labeled data is not available.

III. PAYMENT SYSTEM USING STEGNOGRAPHY AND VISUAL CRYPTOGRAPHY

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 as in [9], [10], [11]. 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 [12] in which coding is based on tongue position. For applying the Vedic code to English alphabet, frequency of letters in English vocabulary [13] 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 [14].

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

Letter	*Numberassigned*	*Letter*	*Numberassigned*
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

3.1 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.

3.2 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.

3.3 Result

To implement the above text based steganography method, a secret message is considered. Suppose it is "text". text = 01110100011001010111100001110100
Result of encoding is shown in Fig. 1.

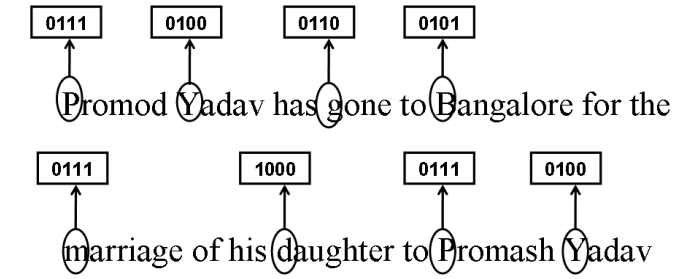

Fig 1. Result of Encoding

3.4 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 CertifiedAuthority (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.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 above. Customer authentication information (account no) in connection with merchant is placed above the cover text in its original form.

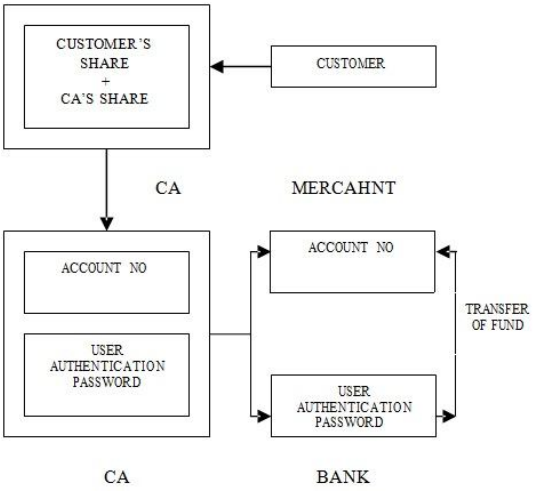

Fig 2. Proposed payment method

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 fund from the customer account to the

submitted merchant account. After receiving the fund, merchant's payment system validates receipt of payment using customer authentication information.

Account No - 12345678910111
Promod Yadav has gone to Bangalore
for the marriage of his daughter to
Promash Yadav.

Fig 3. Snapshot account no and cover text.

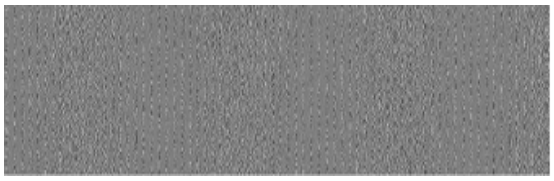

Fig. 4: Share 1 kept by customer

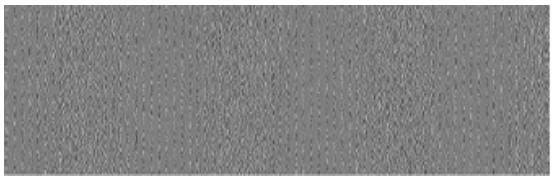

Fig. 5: Share 2 kept by CA

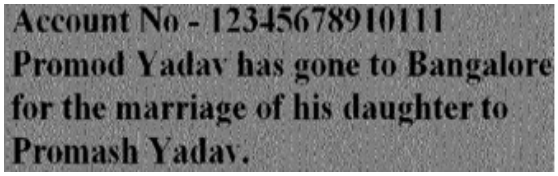

Fig 6 :Overlapping Share 1 and Share 2

3.5 Hidden Markov Model

We can Add Additional Level of Security through Hidden Markov Model. HMM model is going to be used to find out fraudulent access of Credit card. The Average Transaction of Card Holder is going to be recorded which is always going to checked at the time of transaction. If the Transaction is crossing the threshold limit of average transaction the Transaction will be treated as fraudulent transaction and the Security Questions will be asked before committing transactions.

REFERENCES

[1]Jihui Chen, XiaoyaoXie, 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]Anti-Phishing Working Group (APWG), "Phishing Activity Trends Reprt,2013,"http://docs.apwg.org/reports/apwg_trends_reports_q2_2013.pdf

[3]Jaya,SiddhartMalik,AbhinavAagrawal, Anjali Sardana, "Novel Authentication system using visual cryptography. " Proceedings of 2011 world congress on information and communication Technologies, p.p. 1181-1186, Mumbai, India, 2011

[4]ChetanaHegde, S. Manu, P. DeepaShenoy, K.R.Venugopal, L.M.Patnaik, "Secure Authentication using Image Processing And Visual Cryptography for Banking Applications." Proceedings of 16thInernational Conference on Advanced Computing and Communications,p.p. 65-72, Cheenai,India 2008.
[5]K.Thamizhchelvy, G. Geetha, "E-Banking Security: Mitigating Online threats Using Message Authentication Image (MAI) Algorithm", Proceeding of 2011 2nd International Conference on Computer And Computing Sciences (ICCS), p.p. 276-280,2012
[6]S.Suryadevara, R. Naaz, Shweta, S. Kapoor, "Visual Cryptography improvise the security of tounge as a biometric in banking system."Proceedings of 2011 2nd International Conference on Computer and Communication Technology (ICCCT), pp,412-415,2011
[7]S.Ghosh and D.L. Reilly, "Credit Card Fraud Detection with neural network"Proc.27th Hawaii Int'l Conf. System Sciences; Information Systems; Decision Support and Knowledge-based system,
Vol. 3,pp. 621-630, 1994
[8]C Chiu and C.Tsai, "A web service based collaborative scheme for credit card fraud detection" Proc. IEEE Int'Iconf, e-technology,e-commerece and e-service, pp 177-187,2004
[9] Jack Bassil, Steven low, NIchlosMaxemchuk, Larry O'Gorman,"Hidding Information in Document Images" Proceedings of 1995 Conference On Information Sciences and Systems, Jhons Hopkins University, p.p. 482-489, 1995
[10]Walter Bender, DanialGruhl,Norishige Morimoto, A. Lu, "Techniques for data Hiding," IBM system Journal Vol.35, Nos. 3 & 4, pp.33-336, 1996
[11] K. Bennet "Linguistic Steganography: Survey, Analysis And Robustness concern for hiding information in Text." Purdue University.Cerias Tech Report 2004-2013.
[12]Bharati Krishna Tirthaji, "Vedic Mathematics and its spiritual Dimension", MotilalBansari Publishers, 1992
[13] http://oxfordictonaries.com/words/what-is-the-frequency-of-the-letters-of-the-alphabet-in-english.
[14]Kalavathi Alia, Dr.D.R.Siva Rama Prasad, "An Evolution of Hindi Text Steganography," Proceeding of sixth International Conference on Information Technology, pp 1577-1578, Las Vegas, NV,2009

