IWNEST PUBLISHER

Journal of Industrial Engineering Research

(ISSN: 2077-4559)

Journal home page: http://www.iwnest.com/AACE/

Losseless Tagged Visual Cryptography Scheme For Online Payment

S. Dhivya and Mrs.Alice M.E(Ph.D)

Department of Computer Science & Engineering GKM College of Engineering & Technology Tamilnadu, India

ARTICLE INFO

Article history:
Received 20 March 2015
Accepted 25 May 2015
Available online 5 June 2015

Keywords:

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). The presents a new approach for providing limited information only that 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 Steganography and visual cryptography for this purpose. The proposes a technique of processing the signature of a customer and then dividing it into shares. Total number of shares to be created is depending on the scheme chosen by the bank. When two shares are created, one is stored in the bank database and the other is kept by the customer. The customer has to present the share during all of his transactions. This share is stacked with the first share to get the original signature. The correlation method is used to take the decision on acceptance or rejection of the output and authenticate the customer.

To Cite This Article: S. Dhivya and Mrs.Alice M.E(Ph.D)., Losseless Tagged Visual Cryptography Scheme For Online Payment **J. Ind. Eng. Res.**, ***1(4),*** *109-112, 2015*

INTRODUCTION

OLTP system is a popular data processing system in today's enterprises. Some examples of OLTP systems include order entry, retail sales, and financial transaction systems. Online transaction processing system increasingly requires support for transactions that span a network and may include more than one company. For this reason, modern online transaction processing software use client or server processing and brokering software that allows transactions to run on different computer platforms in a network. In large applications, efficient OLTP may depend on sophisticated transaction management software (such as CICS) and/or database optimization tactics to facilitate the processing of large numbers of concurrent updates to an OLTP-oriented database. For even more demanding decentralized database systems,OLTP brokering programs can distribute transaction processing among multiple computers on a network. OLTP is often integrated into service-oriented architecture (SOA) and Web services.

Online Transaction Processing (OLTP) involves gathering input information, processing the information and updating existing information to reflect the gathered and processed information. As of today, most organizations use a database management system to support OLTP. OLTP is carried in a client server system.

OLTP system is a popular data processing system in today's enterprises. Some examples of OLTP systems include order entry, retail sales, and financial transaction systems. Online transaction processing system increasingly requires support for transactions that span a network and may include more than one company. For this reason, modern online transaction processing software use client or server processing and brokering software that allows transactions to run on different computer platforms in a network. In large applications, efficient OLTP may depend on sophisticated transaction management software (such as CICS) and/or database optimization tactics to facilitate the processing of large numbers of concurrent updates to an OLTP-oriented database. For even more demanding decentralized database systems,OLTP brokering programs can distribute transaction processing among multiple computers on a network. OLTP is often integrated into service-oriented architecture (SOA) and Web services.

Online Transaction Processing (OLTP) involves gathering input information, processing the information and updating existing information to reflect the gathered and processed information. As of today, most organizations use a database management system to support OLTP. OLTP is carried in a client server system.

Corresponding Author: S. Dhivya, Department of Computer Science & Engineering GKM College of Engineering & Technology Tamilnadu, India

Journal of Industrial Engineering Research, 1(4) July 2015, Pages: 109-112

II. Related Work:

An efficient national payment system reduces the cost of exchanging goods and services, and is indispensable to the functioning of the interbank, money, and capital markets. A weak payment system may severely drag on the stability and developmental capacity of a national economy; its failures can result in inefficient use of financial resources, inequitable risk-sharing among agents, actual losses for participants, and loss of confidence in the financial system and in the very use of money The technical efficiency of payment system is important for a development of economy. Real-time gross settlement systems (RTGS) are funds transfer systems where transfer of money or securities takes place from one bank to another on a "real-time" and on "gross" basis. Settlement in "real time" means that payment transaction does not require any waiting period. The transactions are settled as soon as they are processed. "Gross settlement" means the transaction is settled on one to one basis without bunching or netting with any other transaction. Once processed, payments are final and irrevocable.

III. *Proposed Payment Method:*

An e-commerce payment system facilitates the acceptance of electronic payment for online transactions. Also known as a sample of Electronic Data Interchange (EDI), e-commerce payment systems have become increasingly popular due to the widespread use of the internet-based shopping and banking. Over the years, credit cards have become one of the most common forms of payment for e-commerce transactions. In North America almost 90% of online B2C transactions were made with this payment type.[1] Turban et al. goes on to explain that it would be difficult for an online retailer to operate without supporting credit and debit cards due to their widespread use. Increased security measures include use of the card verification number (CVN) which detects fraud by comparing the verification number printed on the signature strip on the back of the card with the information on file with the cardholder's issuing bank. Also online merchants have to comply with stringent rules stipulated by the credit and debit card issuers (Visa and MasterCard) this means that merchants must have security protocol and procedures in place to ensure transactions are more secure. This can also include having a certificate from an authorized certification authority (CA) who provides PKI(Public-Key infrastructure)for securing credit and debit card transactions.

Despite widespread use in North America, there are still a large number of countries such as China, India and Pakistan that have some problems to overcome in regard to credit card security. In the meantime, the use of smartcards has become extremely popular. A Smartcard is similar to a credit card; however it contains an embedded 8-bit microprocessor and uses electronic cash which transfers from the consumers' card to the sellers' device. A popular smartcard initiative is the VISA Smartcard. Using the VISA Smartcard you can transfer electronic cash to your card from your bank account, and you can then use your card at various retailers and on the internet.

There are companies that enable financial transactions to transpire over the internet, such as PayPal. Many of the mediaries permit consumers to establish an account quickly, and to transfer funds into their on-line accounts from a traditional bank account (typically via ACH transactions), and *vice versa*, after verification of the consumer's identity and authority to access such bank accounts. Also, the larger mediaries further allow transactions to and from credit card accounts, although such credit card transactions are usually assessed a fee (either to the recipient or the sender) to recoup the transaction fees charged to the mediary.

The speed and simplicity with which cyber-mediary accounts can be established and used have contributed to their widespread use, although the risk of abuse, theft and other problems—with disgruntled users frequently accusing the mediaries themselves of wrongful behavior—is associated with them.

A. Advantage:

- Proposed method minimizes customer information sent to the online merchant. So in case of a breach in merchant's database, customer doesn't get affected. It also prevents unlawful use of customer information at merchant's side.
- Presence of a fourth party, CA, enhances customer's satisfaction and security further as more number of parties are involved in the process.
- Usage of steganography ensures that the CA does not know customer authentication password thus Maintaining customer privacy.
- Cover text can be sent in the form of email from CA to bank to avoid rising suspicion.
- Since customer data is distributed over 3 parties, a breach in single database can easily be contented.

B. Security Threat:

During payment, merchant's payment system requires to direct the shopper to CA's portal but fraudulent merchant may direct shopper to a portal similar to CA's portal but of its own making and get hold of customer own share. To prevent this type of phishing attack, an end-host based approach can be implemented for detection and prevention of phishing attack.

Journal of Industrial Engineering Research, 1(4) July 2015, Pages: 109-112

C. Method Extension:

The payment system can also be extended to 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.

IV. Proposed algorithm:

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 [4], [8], [9]. 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 in which coding is based on tongue position. For applying the Vedic code to English alphabet, frequency of letters in English vocabulary [18] 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 other. 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: Number Assignment.

Letter	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

A. 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.

B. 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.

C. 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 Cover message.

D. Drawback:

In result to hide 4 letter word, 8 words are required excluding the words that are added to provide flexibility in sentence construction. So to hide a large message, this technique requires large no of words and creates a

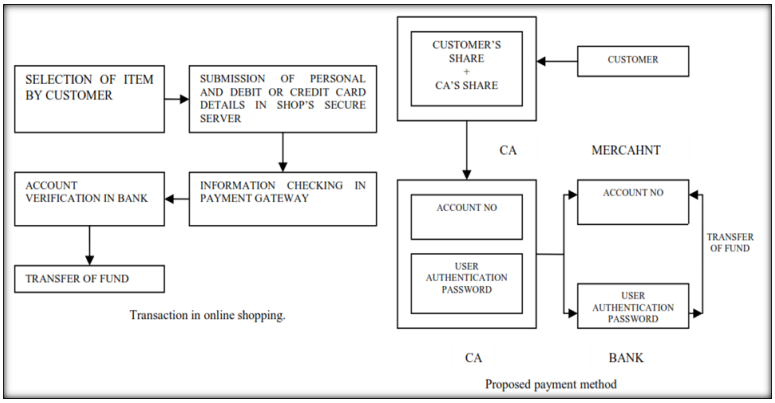
Journal of Industrial Engineering Research, 1(4) July 2015, Pages: 109-112

complexity in sentence construction. Disadvantage of this technique can be used in its advantage by applying it to online banking to create spam mail to hide one's banking information.

V. Transaction in online shopping:

In traditional online shopping as shown in Fig. 2 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, pay online system, Web Money and others. In the payment portal consumer submit his or her credit

VI. Architecture:



II. *Conclusion:*

A payment system for online shopping is proposed by combining text based steganography and visual cryptography that provides customer data privacy and prevents misuse of data at merchant's side. The method is concerned only with prevention of identify theft and customer data security. 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.

REFERENCES

[1] Thamizhchelvy, K., G. Geetha, 2012. ―E-Banking Security: Mitigating Online Threats Using Message Authentication Image (MAI) Algorithm,‖ Proceedings of International Conference on Computing Sciences (ICCS), 276 – 280.

[2] Suryadevara, S., R. Naaz, Shweta, S. Kapoor, 2011. Visual cryptography improvises the security of tongue as a biometric in banking system,‖ Proceedings of 2nd International Conference on Computer and Communication Technology (ICCCT), 412 – 415.

[3] Bharati Krishna Tirthaji, 1992. ―Vedic Mathematics and its Spiritual Dimension,‖ Motilal Bansari Publishers.

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

[5] Javelin Strategy & Research, 2013. Identify Fraud Report," https://www.javelinstrategy.com/brochure/276.

[6] Anti-Phishing Working Group (APWG), 2013. "Phishing Activity Trends Report," http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf .

[7] Jack Brassil, Steven Low, Nicholas Maxemchuk, Larry O'Gorman, 1995. "Hiding Information in Document Images," Proceedings of the Conference on Information Sciences and Systems, Johns Hopkins University, 482-489.

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