IJRRECS/September 2016/Volume-4/Issue-9/6948-6952 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN INFORMATION SECURITY MODULE TO PREVENT IDENTITY THEFT AND IMPROVE THE CUSTOMER CONFIDENCE

Amrutha Vangari[1], Ranjith Kanna K[2]

[1]M.Tech Student, Dept of CSE, Ganapathi Engineering College, Warangal, T.S, India

[2]Assistant Professor, Dept of CSE, Ganapathi Engineering College, Warangal, T.S, India

ABSTRACT:

Suggested text based steganography uses characteristics of British language for example inflexion, fixed word order and employ of periphrases for hiding data instead of using qualities of the sentence. This provides versatility and freedom in the point look at sentence construction however it increases computational complexity. An immediate development in E-Commerce marketplace is observed in recent time around the world. With ever growing recognition of internet shopping, Debit or Charge card fraud and private information security are major concerns for purchasers, retailers and banks particularly within the situation of CNP. The technique uses combined use of steganography and visual cryptography for this function. This paper presents a brand new method for supplying limited information that is essential for fund transfer during shopping online therefore safeguarding customer data and growing customer confidence and stopping id theft.

Keywords: Information security; Steganography; Visual Cryptography; online shopping

1. INTRODUCTION:

Within this paper, a brand new technique is suggested, that utilizes text based steganography and visual cryptography, which minimizes information discussing between consumer an internet-based merchant but enable effective fund transfer from consumer's account to merchant's account therefore safeguarding consumer information and stopping misuse of knowledge at merchant side. The technique

suggested is particularly for E-Commerce but may be easily extended for online in addition to physical banking. Steganography is the skill of hiding of the message within another to ensure that hidden message is indistinguishable. The important thing concept behind steganography is the fact that message to become transmitted isn't detectable to casual eye. Text, image, video, audio are utilized like a cover media for hiding data in steganography [1]. In text steganography, message could be hidden by shifting word and line, in open spaces, in word sequence. Qualities of the sentence for example quantity of words, quantity of figures, quantity of vowels, and position of vowels in short will also be accustomed to hide secret message. The benefit of preferring text steganography over other steganography techniques is its smaller sized memory requirement and much easier communication. Only mixing the k shares or even more provide the original secret image.

2. PREVIOUS STUDY:

A person authentication system using visual cryptography is presented but it's particularly created for physical banking. A signature based authentication system for core banking is suggested it requires physical existence of the client presenting the proportion. A note authentication image formula is suggested to safeguard against e-banking fraud. A biometrics along with visual cryptography can be used as authentication system.

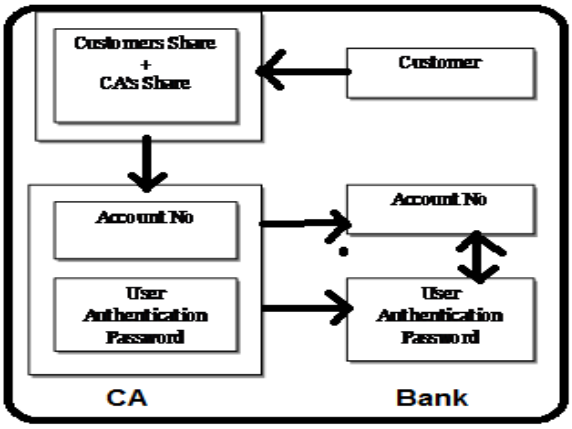

Fig.1.Proposed system

3. PROPOSED MODEL:

The steganography technique is dependent on Vedic Number Code by which coding is dependent on tongue position. Suggested text based steganography uses characteristics of British language for example inflexion, fixed word order and employ of periphrases for hiding data instead of using qualities of the sentence [2]. This provides versatility and freedom in the point look at sentence construction however it increases computational complexity. For using the Vedic code to British alphabet, frequency of letters in British vocabulary

can be used because the grounds for assigning figures towards the letters in British alphabet. Each letter is assigned several in the plethora of to fifteen. For various frequencies, different figures are allotted to the letters. It essentially represents frequency of letters in integer form. Encoding: 1. Representation of every letter secretly message by its equivalent ASCII code. 2. Conversion of ASCII code to equivalent 8 bit binary number. Division of 8 bit binary number into two 4 bit parts. 3. Selecting of appropriate letters from table 1 akin to some bit parts. 4. Significant sentence construction by utilizing letters acquired because the first letters of appropriate words. 5. Omission of articles, pronoun, preposition, adverb, was/were, is/am/are, has/have/had, will/shall, and would/should in coding tactic to give versatility in sentence construction. 6. Encoding isn't situation sensitive. Decoding: 1. First letter in every word of canopy message is taken and symbolized by corresponding 4 bit number. 2. 4 bit binary figures of combined to acquire 8 bit number. 3. ASCII codes are acquired from 8 bit figures. 4. Finally secret message is retrieved from ASCII codes. In lead to hide 4 letter word, 8 test is needed excluding the language which are put into provide versatility in sentence construction. To hide a sizable message, this method requires large no of words and helps to create a complexity in sentence construction. Drawback to this method may be used in the advantage by making use of it to internet banking to produce junk e-mail mail to cover one's banking information. In traditional shopping online, consumer selects products online shopping portal after which is forwarded to the payment page. Online merchant might have its very own payment system or can engage in 3rd party payment systems for example PayPal, pay online system, Web Money yet others. Within the payment portal consumer submit their debit or credit card details for example debit or credit card number, name around the card, expiry date from the card. Information on information searched for from shopper change from one payment gateway to a different. For instance, payment in IRCTC website requires Personal Identification Number (PIN) when having to pay using bank card whereas shopping in Flipkart or Snapdeal requires Visa or Master secure code. However recent much talked about breaches for example in Epsilon, Sony's Ps Network and Heartland

Payment Systems reveal that card holders' details are in danger both from outdoors and inside. One continues to have to believe the merchant and it is employees to not use card information in order for their own purposes. Within the suggested solution, information posted through the customer towards the online merchant is minimized by supplying only minimum information which will only verify the payment produced by the stated customer from the banking account. This is done by the development of a main Certified Authority (CA) and combined use of steganography and visual cryptography. The data received through the merchant could be by means of account number associated with the credit card employed for shopping. Within the suggested method, customer unique authentication password in link with the financial institution is hidden in the cover text while using text based steganography method [3]. Customer authentication information (account no) regarding the merchant is positioned over the cover text in the original form. During shopping on the web, after choice of preferred item and adding it towards the cart, preferred payment system from the merchant directs the client towards the Certified Authority portal. Customer authentication details are delivered to the merchant by CA. Upon receiving customer authentication password, bank matches it using its own database after verifying legitimate customer, transfers fund in the customer account towards the posted credit card merchant account [4]. After finding the fund, merchant's payment system validates receipt of payment using customer authentication information. However, CA doesn't know that bank to forward the coverage text acquired from mixing two shares. It may be solved by appending 9 digit routing or transit quantity of bank with customer authentication information. Security Threat: During payment, merchant's payment system requires to direct the patron to CA's portal but fraudulent merchant may direct shopper to some portal much like CA's portal but of their own making and acquire customer own share. To avoid this kind of phishing attack, a finish-host based approach could be implemented for recognition and protection against phishing attack [5].

3. CONCLUSION:

The technique is worried just with protection against id theft and customer data security. Within this paper, a repayment system for

shopping online is suggested by mixing text based steganography and visual cryptography that gives customer data privacy and prevents misuse of information at merchant's side. Compared to other banking application which utilizes steganography and visual cryptography, are essentially requested physical banking, the suggested method does apply for E-Commerce with focus area on payment during shopping online in addition to physical banking. Suggested text based steganography uses characteristics of British language for example inflexion, fixed word order and employ of periphrases for hiding data instead of using qualities of the sentence. This provides versatility and freedom in the point look at sentence construction however it increases computational complexity.

REFERENCES:

[1] 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.

[2] Daniel Gruhl, Anthony Lu, Walter Bender, "Echo Hiding," Proceedings of the First International Workshop on Information Hidding, pp. 293-315, Cambridge, UK, 1996.

[3] Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography," Proceedings of 2011 World Congress on Information and Communication Technologies, pp. 1181-1186, Mumbai, India, 2011.

[4] 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.

[5] 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.