International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 4, June 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Online Payment System using Steganography and Visual Cryptography

Vishnu Anil

PG Scholar, School of CS & IT, Jain (Deemed-to-be-University), Bengaluru, Karnataka, India

ABSTRACT

A galloping expansion in E-commerce market has been marked lately across worldwide. Constantly progressive vogue of online purchase, debit or credit card fraud and personalized data security are the most significant distress for the customers, merchants and banks particularly in the case of CNP (Card Not Present). This Report bestows a new approach for delivering only the finite and precise information that is essential for fund transfer over online purchasing thereby safeguarding the customer data and accelerating customer confidence and averting identity theft. And this method applies a merged application of steganography and visual cryptography for this purpose.

KEYWORDS: *Information security; Online shopping; Steganography; Visual Cryptography*

How to cite this paper: Vishnu Anil "Online Payment System using Steganography and Visual Cryptography" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-4, June 2020, pp.12-15, URL: www.ijtsrd.com/papers/ijtsrd30841.pdf

IJTSRD30841

I. INTRODUCTION

Online purchasing is the repossession of product information through the internet and consequence 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. Identity theft and phishing are the general hazard of online purchasing. Identity theft is the looting of someone's identity in the form of personal information and abuse of that information for making purchase opening of bank accounts or arranging credit cards. In 2012 buyer data was abused for a normal of 48 days because of data fraud. Phishing is a criminal system that utilizes both social engineering and electronic subterfuge to take purchasers individual information and financial account credentials. In second quarter of 2013, Payment Service, Financial and Retail Service are the most focused industry of phishing attack. Secure Socket Layer (SSL) encryption prevents the capture attempt of purchaser data in travel between the buyer and the online trader. In any case, one should at present trust vendor and its workers not to utilize buyer data for their own buyings and not to sell the data to other people.

In this paper, a new technique is proposed, that utilizes text based steganography and visual cryptography, which limits data sharing among shopper and online dealer however empower effective fund transfer from shopper's record to dealer's record accordingly defending purchaser information and preventing abuse of data at trader side. The strategy proposed is explicitly for E-Commerce yet can without much of a stretch be reached out for online just as physical banking.

II. STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

Steganography is the specialty of covering up of a message inside another with the goal that concealed message is undefined. The key idea driving steganography is that message to be transmitted isn't distinguishable to easygoing eye. Text, Image, Audio, Video are utilized as a cover media for concealing information in steganography. In text steganography, message can be covered up by moving word and line, in open spaces, in word succession. Properties of a sentence, for example, number of words, number of characters, number of vowels, position of vowels in a word are additionally used to share secret message. The benefit of favoring content steganography over other steganography methods is its littler memory necessity and simpler communication.

Visual Cryptography (VC) is a cryptographic strategy dependent on visual secret sharing utilized for picture encryption. Utilizing k out of n (k, n) visual secret sharing plan a secret picture is scrambled in shares which pictures have no meaning that can be transmitted or appropriated over an untrusted correspondence channel Just consolidating the k offers or more give the first secret picture.

III. RELATED WORK

A concise review of related work in the zone of banking security dependent on steganography and visual cryptography is introduced in this segment. A client verification system utilizing visual cryptography is there yet it is mainly intended for physical banking. A signature based verification framework for core banking is proposed however it additionally requires physical presence of the client introducing the share. Visual cryptography validation framework for client authentication in core banking. A message authentication picture algorithm is proposed to ensure against e-banking fraud. A biometrics related to visual cryptography is utilized as an authentication system.

IV. PROPOSED TEXT BASED STEGANOGRAPHY METHOD

Proposed content based steganography utilizes attributes of English language, for example, expression, fixed word request and use of periphrases for hiding information instead of utilizing properties of a sentence. This gives adaptability and opportunity from the point perspective on sentence development yet it increments computational complexity.

The steganography procedure depends on Vedic Numeric Code in which coding depends on tongue position. For applying the Vedic code to English letter set, frequency of letters in English vocabulary is utilized as the reason for assigning out numbers to the letters in English letter set. Number assignments of letters are appeared in table 1. No different significance is given for vowels and consonants as analyzed.

Each letter is alloted a number in the scope of 0 to 15. For various frequencies, various numbers are assigned out to the letters. Number assigned out in range (N+0.99) % to (N+0.3) % also, (N+0.2) % to (N+0.01) % is same where N is any whole number from 0 to It essentially represents to frequency of letters in whole number structure. Above number assignment strategy is utilized to amplify no of letters in a specific appointed number group which in turn gives adaptability in word picking and eventually brings about reasonable sentence development.

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

TABLE1. Number Assignments

A. Encoding steps:

- Each letter in secret message are represented to its equivalent ASCII code
- ASCII code is converted into 8 bit binary number
- This 8 bit binary number is dived it into two 4 bit
- Selecting the needed letter from the table according to the 4 bit part
- Selecting the first letters from the words and creating a relevant sentence
- Avoiding adverb, pronoun etc in coding helps with flexibility in forming sentence
- Encoding doesn't rely on case sensitivity

B. Decoding Steps:

- Selecting the first letter of each word of the message and relating to the 4 bit number
- To get the 8 bit number these 4 bit numbers are merged
- From 8 bit numbers ASCII codes are obtained
- Secret message is recovered from the ASCII code

C. Result

To implement the above content based steganography technique, a secret message is used.

STAR = 01110011 01110100 01100001 01110010

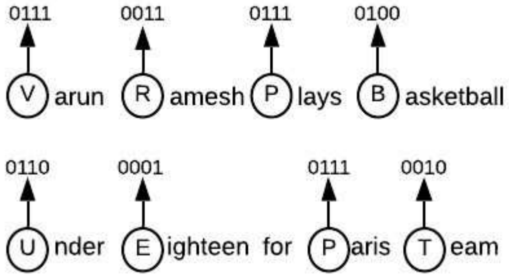

Fig.1. Cover message

D. Drawback

In conclusion to hide 4 letter word,8 words are essential eliminating the words that are additional to furnish adaptability in sentence exposition. So to conceal a large message, this strategy entail no. of words and generates complexity in sentence exposition. Downside of this strategy can be used in its upside by applying it to online banking to generate spam mail to conceal one's banking information.

V. TRANSACTION IN ONLINE SHOPPING

In conventional online shopping, shoppers choose things from an online shopping gateway and afterward is coordinated to the payment page. Online traders may have their own payment framework or can take advantage of third party payment frameworks, for example, Paypal, GooglePay, Paytm, PhonePay and others. In the payment portal purchasers present their credit or debit card details, for example, credit or debit card number, name on the card, expiry date of the card.

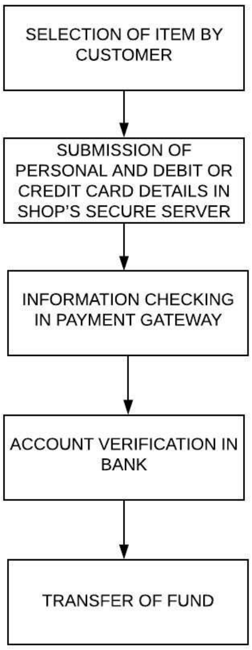
SELECTION OF ITEM BY CUSTOMER
SUBMISSION OF PERSONAL AND DEBIT OR CREDIT CARD DETAILS IN SHOP'S SECURE SERVER
INFORMATION CHECKING IN PAYMENT GATEWAY
ACCOUNT VERIFICATION IN BANK
TRANSFER OF FUND

Fig.2. Transaction in online shopping

Details of information looked for from customers fluctuate from one payment gateway to another. For instance, payment in airtel siterequires a Personal Identification Number (PIN) when paying, utilizing a debit card though shopping in Amazon or Flipkart requires Visa or Master secure code. Notwithstanding that shipper may require a Card Verification Value code, CVV (CVV2 for Visa, CVC2 for MasterCard), which is essentially an authorizing code in CNP exchanges. According to the PCI Data Security Standard , vendors are precluded from storing CVV information or PIN information and if card information, for example, name, card number and termination date is stored, certain security norms are required. Anyway recent high profile breaches such as in Adobe, Dubsmash and eBay show that card holders' data is in danger both from outside and inside. A solution can be compelling traders to be a PCI grumbling yet cost to be a PCI protest is tremendous and the procedure is time consuming and complex and it will take care of part of the issue. One despite everything needs to have trust in the trader and its representatives not to utilize card data for there own purposes

VI. PROPOSED PAYMENT METHOD

In the proposed arrangement, data put together by the client to the online trader is limited by giving just least data that will just confirm the installment made by the said client from its financial balance. This is accomplished by the presentation of a Central Certified Authority (CA) and consolidated utilization of steganography and visual cryptography. The data got by the merchant can be an account number related with the card utilized for shopping. The data will just approve receipt of payment from an authentic client. The procedure appears in Fig.3.

In the proposed strategy, client unique confirmation password in association with the bank is covered up inside a text utilizing the textbased steganography technique as referenced in area IV. Client validation information (account no) regarding dealer is set over the cover text in its unique structure. Presently a preview of two writings is taken. From the preview picture, two offers are created utilizing visual cryptography.

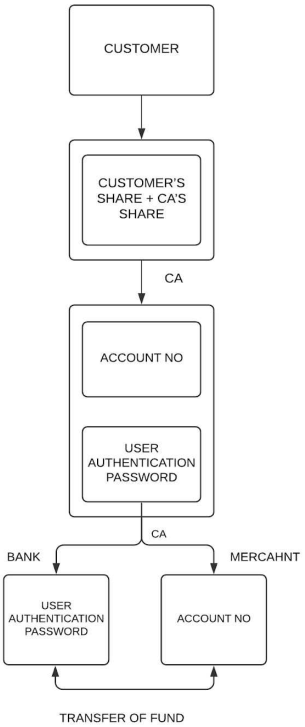
CUSTOMER
CUSTOMER'S SHARE + CA'S SHARE
CA
ACCOUNT NO
USER AUTHENTICATION PASSWORD
CA
BANK
MERCAHNT
USER AUTHENTICATION PASSWORD
ACCOUNT NO
TRANSFER OF FUND

Fig.3. Proposed payment method

Presently one share is kept by the client and the other share is kept in the database of the certified authority. During shopping online, after selecting wanted thing and adding it to the cart, favored payment arrangement of the dealer coordinates the client to the Certified Authority portal. In the portal, customer presents its own offer and the dealer presents its own account subtleties. Presently the CA joins its own offer with customer's shares and gets the first picture.

From CA now, shipper account details, cover text are sent to the bank where client validation password is recovered from the cover text. Client validation information is sent to the dealer by CA. After getting client confirmation password, bank matches it with its own database and after confirming the genuine client, moves fund from the client account to the submitted trader account. In the wake of getting the fund, trader's payment system approves receipt of payment utilizing client authentication information.

The issue is that CA doesn't know to which bank to forward the spread content acquired from consolidating two shares. It can be understood by attaching 9 digit routing or transit number of bank with client authentication information. if "star" is client novel confirmation secret word and account no of client is 12345678901012, for example picture of cover text and account no is appeared in Fig.4 and resultant shares by the utilization of visual cryptography on snapshot are Fig.5 and Fig.6. Fig.5 shows share 1 kept by client and Fig.6 shows share 2 kept by CA. Fig.7 shows the aftereffect of combining share 1 and share 2.

text 12345

Fig.4. Snapshot account no and cover text.

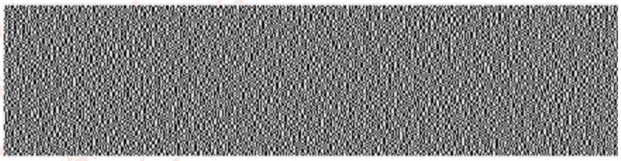

Fig.5. Share 1 kept by customer.

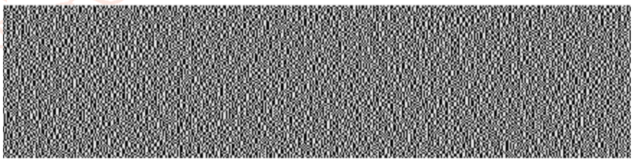

Fig.6. Share 2 kept by CA.

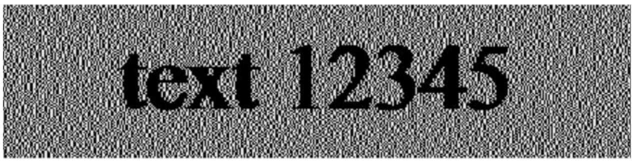

Fig.7. Overlapping of share 1 and share 2

A. Advantage

- Proposed strategy limits client data sent to the online shipper. So if there should be an occurrence of a break in trader's database, client doesn't get effected. it additionally forestalls unlawful utilization of client data at trader's side.
- Presence of a fourth party, CA, improves client's fulfillment and security further as progressively number of parties are engaged with the procedure.
- Use of steganography guarantees that the CA doesn't

know the client authentication password in this manner keeping up client privacy.

- cover text can be sent as email from CA to bank to abstain from rising doubt.
- Since client information is circulated more than 3 gatherings, a break in single database can undoubtedly be contented.

B. Security Threat

During payment, vendor's payment system requires to guide the customer to CA's gateway however fraud vendor may guide customer to a gateway like CA's gateway however of its own creation and get hold of client own share. To prevent this kind of phishing attack, an end-host based methodology can be executed for detection and prevention of phishing attack.

C. Method Extension

The payment system can likewise be extended to physical banking. Shares may contain client picture or signature in addition for client authentication password. In the bank, clientpresents its own share and client physical signature is approved against the signature acquired by joining client's share and CA's share alongside approval of client confirmation password. It prevents misuse of stolen card and stops ill-conceived client.

VII. CONCLUSIONS

In this paper, a payment system for online shopping is proposed by consolidating text based steganography and visual cryptography that gives client information protection and prevents misuse of information next to merchant. The strategy is concerned just with avoidance of identity theft and client information security. This can be used in other online payment methods, like online shopping where payment area can be focused also physical banking.

REFERENCES

[1] https://en.wikipedia.org/wiki/Visual_cryptog raphy

[2] http://users.telenet.be/d.rijmenants/en/visual crypto.htm

[3] https://www.computer.org/csdl/proceedings-article/sadfe/2010/4052a025/12OmNxE2mT s

[4] https://www.oxforddictionaries.com/words/ what-is-the-frequency-of-theletters-of-the-al phabet-in-english.

[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] 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.

[7] 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

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

[9] 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.

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

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

[12] 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.

[13] 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.

[14] Javelin Strategy & Research, "2013 Identify Fraud Report," https://www.javelinstrategy.com/brochure/2 76.

[15] 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.

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

[17] 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.

[18] Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report, 2013," http://docs.apwg.org/reports/apwg_trends_report_q2 _2013 .pdf.

[19] J. C. Judge, "Steganography: Past, Present, Future," SANS Institute, November 30, 2001.

[20] 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.