International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

OPS: -A Review on Data Hiding using Steganography & Visual Cryptography

Aqeel Salman Azez
Univ. college of humanities in Al najaf Al a'shraf master of computer science (information system)
MSC(IS), Email : aqeelsalman8@gmail.com

ABSTRACT

A Rapid Growth in E-Commerce is seen in late time all through the world. The Increasing Growth of International interconnected PC systems and the pervasive patterns of utilizing these systems as another field of leading the business process in animating the requests for new installment routines. There are such a variety of strategies which are accessible for installment however it must accomplish abnormal state of security, velocity, protection, decentralization and must take a shot at global level for electronic trade to be acknowledged by the Consumer and Business. With Increasing the Demand of Shopping Online through Home, The Debit or charge card misrepresentation and individual data security are significant sympathy toward the clients, shippers and banks particularly on account of CNP. This paper studies the best in class in installment innovations and representations rising advancements.

Keywords- CNP-Card Not Present

I. INTRODUCTION

Trade is the most real part of any human progress. Enhancing Commerce can bring success into all fragments of society. In today's reality there have been real changes to the trade business. The most critical of it is the presentation of PCs into the trade business. Computerization of business has taken the world by a tempest. There are critical upgrades in the ranges of starting offer of items, setting requests, making installments, and exchange of stores. This has prompted a vastly improved worldwide economy and better expectations for everyday comforts for all.

The prevalence of internet shopping is developing step by step. As per an ACNielsen study led in 2005, one-tenth of the world's populace is shopping on the web. Web shopping is the recovery of item data by means of the Internet and issue of procurement request through electronic buy solicitation, filling of credit or check card data and transportation of item via mail request or home conveyance by messenger [1].Identity robbery and phishing are the normal threats of web shopping.

Data fraud is the taking of somebody's character as individual data and abuse of that data for making buy and opening of ledgers or masterminding charge cards. Phishing is a criminal system that utilizes both social designing and specialized subterfuge to take shoppers' close to home personality information and budgetary record qualifications. In second quarter of 2013, Payment Service, Financial and Retail Service are the most focused on mechanical parts of phishing assaults [2]. Attachment Layer (SSL) encryption keeps the capture attempt of shopper data in travel between the buyer and the online trader.

Notwithstanding, one must in any case trust trader and its workers not to utilize customer data for their own particular buys and not to offer the data to others Internet is developing at an amazingly quick pace. It has been evaluated that there is another page consistently.

The convenience, productivity and snappiness, web crawlers and worldwide vicinity of Internet has been drawing a great many clients towards it. The limitless business sector opportunity on the Web implies a testing air to programming designers who work behind the screen to get things going on the Web. With the blasting online business sector, the E-Commerce programming needs to handle the exchanges effectively, all the more safely and with lesser correspondence delays. The installment data contains private money related information that ought to be exchanged utilizing the most secure approachs. This paper examines the different strategies utilized to join security into electronic installment frameworks.

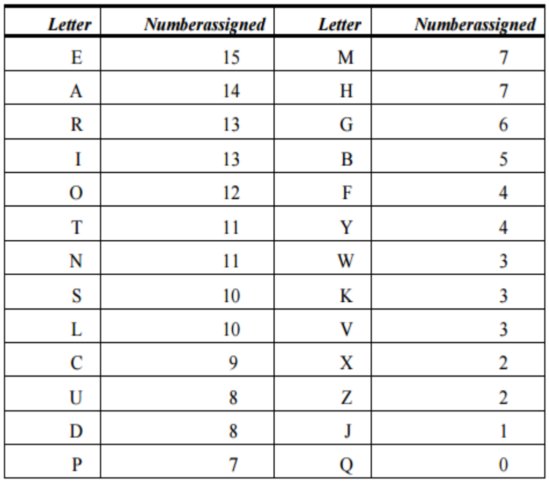
II. PAYMENT SYSTEM USING STEGNOGRAPHY AND VISUAL CRYPTOGRAPHY

Proposed content based steganography utilizes attributes of English dialect, for example, expression, settled word request and utilization of periphrases for concealing information as opposed to utilizing properties of a sentence as in [9], [10], [11]. This gives adaptability and flexibility from the point perspective of sentence development however it increments computational unpredictability.

The stegano graphy procedure is taking into account Vedic Numeric Code [12] in which coding is in light of tongue position. For applying the Vedic code to English letters in order, recurrence of letters in English vocabulary [13] is utilized as the premise for doling out numbers to the letters in English letters in order. Number assignments of letters are demonstrated in table 1. No different significance is given for vowels and consonants when contrasted with [14].

Every letter is allocated a number in the scope of 0 to 15. For distinctive frequencies, diverse numbers are doled out to the letters. Number relegated in extent (N+0.99) % to (N+0.3) % and (N+0.2) % to (N+0.01) % is same where N is any whole number from 0 to 11. It fundamentally speaks to recurrence of letters in whole number structure. Above number task technique is utilized to boost no of letters in a specific doled out number gathering which thus gives adaptability in word picking and at last results in suitable sentence development.

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

Encoding Steps

 Representation of every letter in mystery message by its proportionate ASCII code Conversion of ASCII code to proportionate 8 bit paired number Division of 8 bit twofold number into two 4 bit parts Choosing of suitable letters from table 1 relating to the 4 bit parts Meaningful sentence development by utilizing letters got as the first letters of suitable words. Omission of articles, pronoun, relational word, qualifier, was/were, is/am/are, has/have/had, will/might, and would/ought to in coding procedure to give adaptability in sentence development. Encoding is not case touchy

Deciphering Steps

First letter in every expression of spread message is taken and spoke to by relating 4 bit number. 4 bit paired quantities of consolidated to get 8 bit number. ASCII codes are acquired from 8 bit numbers. Finally mystery message is recouped from ASCII codes

Result

To actualize the above content based steganography technique, a mystery message is considered. Assume it is "content". Content = 0111010001100101011111000001110100 Result of encoding is d

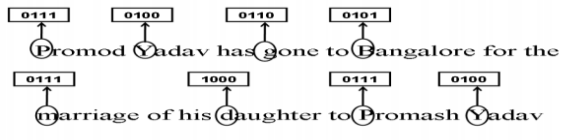

0111
0100
0110
0101
Promod Yadav has gone to Bangalore for the
0111
1000
0111
0100
marriage of his daughter to Promash Yadav

Fig 1. Result of Encoding

III. PAYMENT METHOD

In the proposed arrangement, data put together by the client to the online dealer is minimized by giving just least data that will just check the installment made by the said client from its financial balance. This is accomplished by the presentation of a focal Certified Authority (CA) and consolidated use of steganography and visual cryptography. The data got by the vendor can be as record number identified with the card utilized for shopping. The data will just accept receipt of installment from credible client. In the proposed technique, client one of a kind verification secret word in association with the bank is covered up inside a spread content utilizing the content based steganography system as said above. Client confirmation data (account no) regarding shipper is set over the spread content in its unique form.

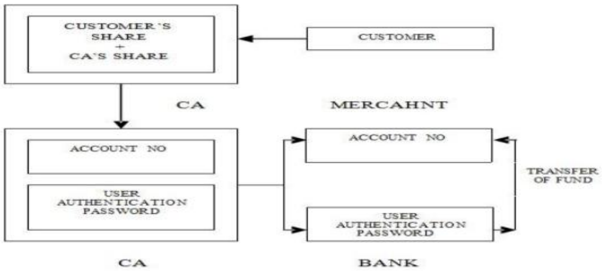

CUSTOMER'S SHARE + CA'S SHARE
CUSTOMER
CA
MERCAHNT
ACCOUNT NO
USER AUTHENTICATION PASSWORD
ACCOUNT NO
TRANSFER OF FUND
USER AUTHENTICATION PASSWORD
CA
BANK

Fig 2. Proposed payment method

Presently one offer is kept by the client and the other offer is kept in the database of the confirmed power. Amid shopping on the web, after choice of coveted thing and adding it to the truck, favored installment arrangement of the shipper guides the client to the Certified Authority entrance. In the entrance, customer presents its own offer and shipper presents its own particular record points of interest. Presently the CA joins its own offer with customer's offer and acquires the first picture. From CA now, dealer record points of interest, spread content are sent to the bank where client confirmation secret key is recouped from the spread content. Client confirmation data is sent to the vendor by CA. After accepting client verification secret word, bank matches it with its own particular database and in the wake of checking true blue client, exchanges store from the client record to the submitted dealer record. In the wake of getting the trust, dealer's installment framework accepts receipt of installment utilizing client validation data.

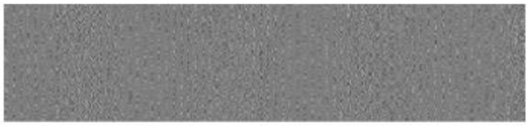


Fig. 3 : Share 1 kept by customer

Fig. 4: Share 2 kept by CA

Hidden Markov Model

We can Add Additional Level of Security through Hidden Markov Model. Well model will be utilized to figure out deceitful access of Credit card. The Average Transaction of Card Holder will be recorded which is continually going excessively checked at the season of exchange. On the off chance that the Transaction is crossing the edge furthest reaches of normal exchange the Transaction will be dealt with as fake exchange and the Security Questions will be asked before conferring exchanges.

IV. ALGORITHMS

4.1 BPCS (Bit-Plane Complexity Segmentation) Steganography algorithm

The calculation can be portrayed in brief strides as takes after [2].

a) Convert the bearer picture (of any document position) from PBC (Pure Binary Code) to CGC (Canonical Gray Code) framework and in png group.

b) Perform the histogram investigation.

c) After that bit-plane investigation is performed.

d) Perform size-estimation i.e. compute the spots where we can store the emit picture.

e) Perform bit plane many-sided quality division on picture i.e. install discharge obstructs into transporter picture.

f) After installing mail that picture to another client.

g) For separating the implanted picture performs desteganography which is precisely inverse to steganography.

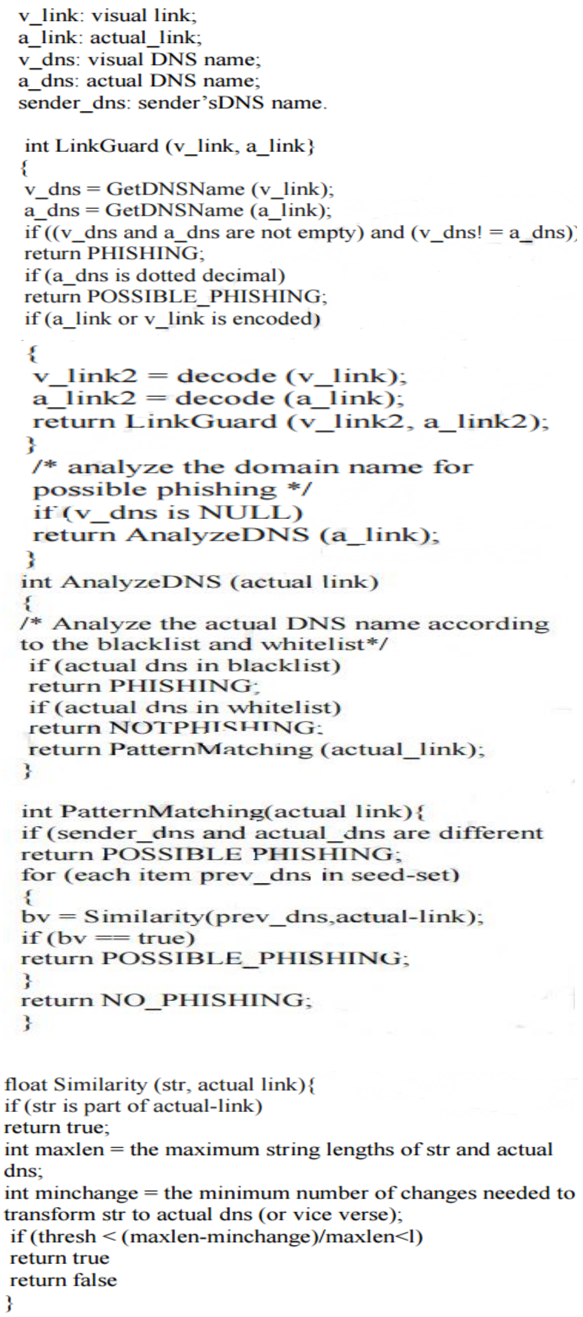
4.2 Visual Cryptography Algorithm

Visual cryptography is a sort of cryptography which permits the visual data to be scrambled in a manner that their unscrambling can be performed by human visual framework. Each mystery pixel of the first paired picture is changed over into four sub pixel of two offer pictures and recuperated by straightforward stacking procedure. This is proportional to utilizing the intelligent OR operation between the shares [4].

4.3 Link Guard Algorithm

Connection Guard lives up to expectations by investigating the contrasts between the visual connection and the genuine connection. It additionally computes the likenesses of a URI with a known trusted site [3].

The accompanying wordings are utilized as a part of the calculation.



```
v_link: visual link;
a_link: actual_link;
v_dns: visual DNS name;
a_dns: actual DNS name;
sender_dns: sender'sDNS name.

 int LinkGuard (v_link, a_link}
 {
 v_dns = GetDNSName (v_link);
 a_dns = GetDNSName (a_link);
 if ((v_dns and a_dns are not empty) and (v_dns! = a_dns))
 return PHISHING;
 if (a_dns is dotted decimal)
 return POSSIBLE_PHISHING;
 if (a_link or v_link is encoded)

 {
  v_link2 = decode (v_link);
  a_link2 = decode (a_link);
  return LinkGuard (v_link2, a_link2);
 }
  /* analyze the domain name for
  possible phishing */
  if (v_dns is NULL)
  return AnalyzeDNS (a_link);
 }
int AnalyzeDNS (actual link)
 {
/* Analyze the actual DNS name according
to the blacklist and whitelist*/
 if (actual dns in blacklist)
 return PHISHING;
 if (actual dns in whitelist)
 return NOTPHISHING;
 return PatternMatching (actual_link);
}

int PatternMatching(actual link){
if (sender_dns and actual_dns are different
return POSSIBLE PHISHING;
for (each item prev_dns in seed-set)
{
bv = Similarity(prev_dns,actual-link);
if (bv == true)
return POSSIBLE_PHISHING;
}
return NO_PHISHING;
}


float Similarity (str, actual link){
if (str is part of actual-link)
return true;
int maxlen = the maximum string lengths of str and actual
dns;
int minchange = the minimum number of changes needed to
transform str to actual dns (or vice verse);
 if (thresh < (maxlen-minchange)/maxlen<l)
 return true
 return false
}
```

V. RELATED WORK

Jaya ,Sidhart Malik, AbhinavAggarwal, Anjali SardanaPraposed A client verification framework utilizing visual cryptography [3] yet it is particularly intended for physical managing an account. ChetanaHegadem, S. Manu, P. DeepaShenoy, K.R.Venugopal,L.M.Patniak proposed A mark based verification framework for center saving money [4] yet it additionally requires physical vicinity of the client introducing theshare. K. Thamizhchelvy, Q. Geetha Praposed A message verification picture calculation is pin [5] to ensure against e-keeping money misrepresentation. S.Suryadevara,R. Naaz, Shweta, S kapoor proposed A biometrics in conjunction with visual cryptography is utilized as verification framework [6]. Ghosh and Reilly [7] have proposed Mastercard extortion recognition with neural system. They have constructed a discovery framework, which is prepared on a huge example of named Visa account exchanges. These exchanges contain case extortion cases because of lost cards, stolen cards, application misrepresentation, fake extortion, mail-request extortion, and non got issues (NRI) frauds. Chiu and Tsai [8] have proposed Web administrations and information mining methods to set up a community oriented plan for extortion location in the managing an account industry. With this plan, taking an interest banks offer learning about the misrepresentation designs in a heterogeneous and dispersed environment. To set up a smooth channel of information trade, Web administrations strategies, for example, XML, SOAP, and WSDL are used. The issue with the vast majority of the aforementioned methodologies is that they require marked information for both veritable, and in addition false exchanges, to prepare the classifiers. Getting this present reality misrepresentation information is one of the most concerning issue connected with charge card extortion location. Likewise these methodologies can't identify new sorts of extortion for which marked information is not accessible.

VI. CONCLUSION

In this paper, we propsed an installment framework for internet combining so as to shop content based Steganography and visual cryptography that gives client information protection and anticipates abuse of information next to merchandiser. The processing is involving just with aversion of wholesale fraud and client information security. In comparing to other saving money application which utilizes Steganography and visual cryptography are fundamentally connected for the physical managing an account, the proposed system can be connected for the ECommerce with center territory on installment amid web shopping and additionally physical keeping money.

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