ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

E-Retailing System Using Steganography And Visual Cryptography: A Survey

Pooja P. Deshmukh*, Prof. M.M.Wankhade**

*ME Student, Sinhgad College of Engineering, Pune, Maharashtra, India

**Dept. of ENTC, Sinhgad College of Engineering, Pune, Maharashtra, India

ABSTRACT: E-Commerce is rapid growth in seen in present time in whole world and uses increased at a rapid rate.The international presence of Internet has been drawing millions of users towards computer and the common trends of using these networks as a new field of conducting the business process in stimulating the demands for proper payment methods. There are so many methods which are available for payment system but it must need to prevent high level of security, speed, privacy. With Increasing the Demand of e-Shopping through Home, The Debit /credit card fraud and individual information security are major issues 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

In e-commerce a rapid growth is obtained by increasing popularity in recent time so that main issues faced is security and integrity on data and system .For this purpose the customers need to build confidence and trust on provider for payment procedure .The most accepted payment mode is today's world debit/credit in the payment mode. It is very convenient procedure for online shopping purchasing the products .When consumer purchase the product and add it to go-cart and go for further payment procedure . So that time consumer need to fulfil their personal information like account number, cvv etc. However, these same technologies also make life easier for cybercriminals by offering them new and easy ways to steal users' money. For accepting payment system the merchandiser need to have access on online payment portal. The online payment portal is a service provider that is integrated with the credit card .also it transfers the related information between the merchant and the payment system.
The typical online payment process has the following stages:
1. Customer submits the payment information to the merchant like their personal information account number provide on debit card etc
2. The merchant submits the payment information to the online payment portal
3. The online payment portal submits the payment to the payment processor.
4. The payment processor authorizes the payment and responds to the payment portal.
5. The payment portal responds back to the merchant.
6. The merchandiser responds back to the consumer showing if the online payment was successful or not and take right action against it.

In real life, fraudulent Transaction are scattered with transactions and simple pattern matching techniques are not often sufficient to detect those frauds acc irately. To prevent this fraud use the combine application of text based stenography and visual cryptography for remove frauds and to preventing identity theft and phishing are the common problems for shopping

MOTIVATION -
Internet is very rapidly growing at an extremely fast pace and estimated that create a new web page every minute. It is easy to use, efficiency and quickness, search engines. The international presence of Internet has been drawing millions of users towards it. It is a challenging atmosphere to software engineers who work to create vast software for vast

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

market world. It burst the online market; the E-Commerce software needs to process the payment transactions efficiently, more securely and with less communication. The payment information can be taken as private financial data that should be transferred using the most secure methodologies. This paper discusses the various types of methods employed to incorporate security into electronic payment systems.

II. LITERATURE REVIEWS

In Mrs. D. Murugeswari, Kn.Sangeethahas derived that a high-speed prosperity in E-Commerce market has been witnessed in recent time throughout the world. In rapid time the population demand the e-shopping which increases the problem in debit/credit card fraud and individual information are major concern for customer and bank. The main purposed of this project is to provide high level security in E-Commerce applications and e- shopping.

Fig .1.Example of Steganography

In S. Roy, P. Venkateshwaran said that Steganography is the process which a secret message can hide by transmitting in a media which can use text, image, video, audio etc. In text Steganography, the message can hide by shifting the characters, converting it into ASCII values, converted into binary form and formatting it to a new sentence etc. it requires small memory and it is simpler in communication. Figure 1 shows an example of Steganography.

III.RELATED WORK

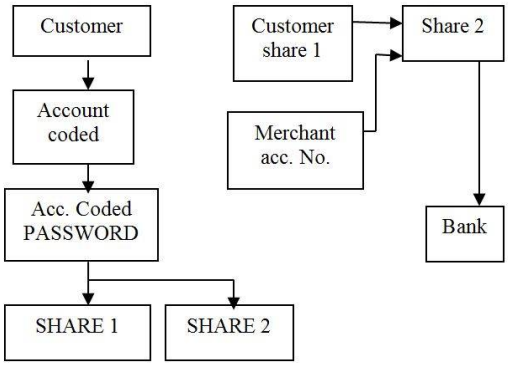


Fig 2 Block diagram of e-retailing

1. PROPOSED SYSTEM –

In the proposed system, the information submitted by the customer which required minimum information which will help to verify the payment system which said by to the online merchant is minimized by providing only minimum information that will only verify the payment system it said by customer its account . This information fulfilled by a central certified authority (CA) and combined used application of Steganography and visual cryptography. The introduction was achieved by a Certified Authority (CA) and use of applications of Steganography and visual

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Cryptography. The information is given by the merchant can be in the form of account number or cvv related to the card used for online shopping. Fig .3.shows proposed payment system.

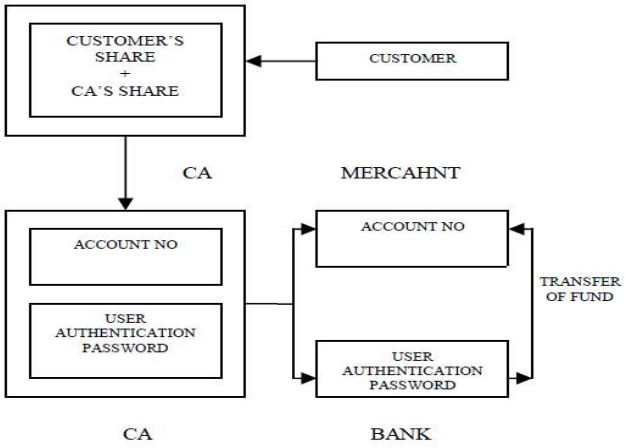


Fig.3. Payment procedure [1]

2. Text based Steganography –

In these, the message can be hidden by shifting word and line, converted into ASCII and then binary for getting meaningful sentence. It also hide the phrases, characters and vowels .

3. Visual Cryptography –

In Naor said that visual cryptography is a cryptographic technique which based on visual secret sharing used for image encryption. Visual Cryptography is contains every secret pixel of the original binary image is converted into four sub pixel of two secret share images and it is recovered by simple stacking process.

Encoding Procedure-
Input: text file
Output: secret key image

Steps:

1. Representation of each letter in secret message by its equivalent ASCII code.
2. Conversion of ASCII code to equivalent 8 bit binary number.
3. Divide 8 bit binary number into two 4 bit part
   A. Choosing of suitable letters number assignment table corresponding to the 4 bit parts.
   B. Meaningful sentence construction by using letters which first letter is suitable for words is get.
4. Using of conversion of sentence generate secrete key image shares and form in jpeg/bmp form.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Table 1: 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

This table shows the number assignment table which is used to create the meaningful sentence.

TRANSACTION IN ONLINE SHOPPING -

Firstly consumer selects items from online shopping portal and then it is directed to the payment gateway. Online shipper may have its own particular instalment framework or can exploit outsider instalment frameworks, for example, PayPal, pay online framework, Web Money and others. In payment gateway procedure the consumer submit his or her credit details like name, credit or debit card number which gives on credit card etc.

A. Customer Authentication: Customer unique authentication password is connected to the bank which is hidden inside in a cover text using the text based Steganography method and the information like account no is connected with merchant is placed above the cover text in its master form. Now an informal photograph of two texts is taken. From the informal photograph image, two plowshares are generated using visual cryptography. Now one plowshare is kept by the customer and the other plowshare is kept in the database of the certified authority (CA).

B. Certification Authority (CA) Access -

During shopping online, after selection of desired item and adding it to the cart, select payment system of the merchant directs the customer to the Certified Authority (CA) gateway. In the gateway, both shopper and merchant can submit their own shares. After providing the own shares CA performs that combine its own share with shopper's share to obtains original share image. Presently CA, send vendor account points of interest which is in spread content structure to the bank where client verification secret word is recouped from the spread content dealer account subtle elements, spread content are sent to the bank where client confirmation data is sent to the shipper by CA. After accepting client confirmation secret key, bank matches it with its own particular database and in the wake of advocating client, exchanges store from the client record to the submitted vendor account. In the wake of getting the asset, trader's instalment framework accepts receipt of instalment utilizing client confirmation data.

Decoding procedure –

Input: two secret key images

Output: original secret key image

Steps:

1. First letter in every expression of spread message is taken and spoke to by comparing 4 bit number.
2. 4 bit binary numbers of combined to obtain 8 bit number.
3. ASCII codes are obtained from 8 bit numbers.
4. Finally, secret message is recovered from ASCII codes.
5. Original secret key is obtained.

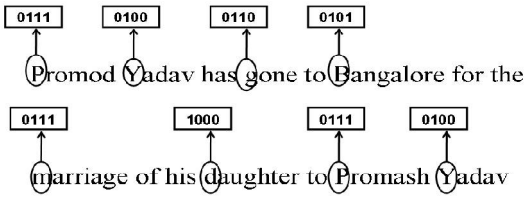
ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Result-
To execute the above substance based Steganography system, a puzzle message is considered. Accept it is "content".
content = 01110100011001010111100001110100



MODELLING:–

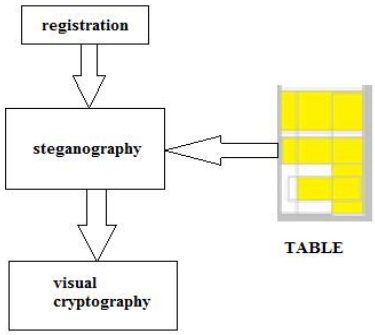


Fig 4.block diagram of modelling

IV. EXPERIMENTALWORK

CASES OBTAINED –

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

Snapshot account no and cover text.[1]

Share 1 kept by customer[1]

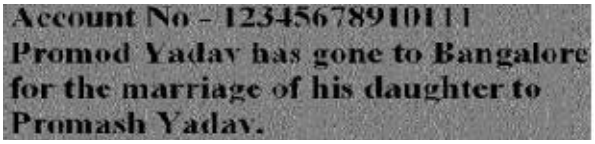
Share 2 kept by CA[1]

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016



Overlapping Share 1 and Share 2[1]

Hidden Markov Model

We can Add Extra Level of Security through Concealed Markov Model. Gee model will be utilized to discover deceitful access of Charge card. The Normal Exchange of Card Holder will be recorded which is continually going excessively checked at the season of exchange. In the event that the Exchange is intersection the edge furthest reaches of normal exchange the Exchange will be dealt with as fake exchange and the Security Inquiries will be.

REFERENCES

[1] V.Lokeswara Reddy and T. Anusha "Combine Use of Steganography and Visual Cryptography for Online Payment System" International Journal of Computer Applications (0975 – 8887) Volume 124 – No.6, August 2015
[2] Souvik Roy1 and P. Venkateswarant "Online Payment System using Steganography and Visual Cryptography" IEEE Students' Conference on Electrical, Electronics and Computer Science of2014
[3] Jihui Chen, XiaoyaoXie, and Fengxuan Jing, "The security of shoppingOnline," Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), vol. 9, pp. 4693-4696, 2011
[4] Javelin Strategy & Research, "2013 Identify FraudReport, https://www.javelinstrategy.com/brochure/276.
[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] M. Naornd A. Shamir, "Visual cryptography," Advances in Cryptograhy: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.
[7] ChetanaHegde, S. Manu, P. DeepaShenoy, 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.
[8] Jaya, Siddharth Malik, AbhinavAggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography," Proceedings of 2011 World Congress on Information and Communication Technologies.
[9] KalavathiAlla, 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.
[10] Bharati Krishna Tirthaji, "Vedic Mathematics and its Spiritual Dimension," Motilal Bansari Publishers,1992.