Steganography and Cryptography Based Online Payment Processing System

Prof. Arun. M. Hattarge[1] Sachin Khochare[2] Nitish Ambewale[3] Sudhir Kadam[4] Atul Pandey[5]

[1]Professor

[1,2,3,4,5]Department of Computer of Engineering

[1,2,3,4,5]Dnyanganga College of Engg. & Research Narhe, Pune

Abstract— In todays world there is rapid growth of E-Commerce in Market.many people can give more preference to online shopping. In online payment processing system there is many chance of credit card or debit card fraud. Hacker can hack personal as well as account related information can hack and misuse of information such as create a fake online account and transfer a money from current account to fake account.Increasing popularity of online shopping Debit or Credit card fraud and personal information security concerns for customers and merchants specifically when card is not present, our analysis presents limited information only that is necessary for fund transfer during online shopping.This paper presents a new approach for online payment system in shopping where only minimum amount of information can send during fund transferring and safeguarding customer data,increasing customer confidence to online payment while shopping.In proposed system use new method like Text Based Steganography and Visual Cryptography to hide and secure account related information during online shopping.

Key words: Information Security, Visual Cryptography, Steganography, Online Shopping, Certified Authourity, E-Commerce, Secret Sharing, Phishing

I. INTRODUCTION

Online shopping is the retrieval of product information via the Internet and issue 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. Today's online shopping product can select and add to cart, then transfer to payment gateway

Fill personal as well as account related information and shipping product by mail order, then product can receive particular address place through delivery boy. In all this process so, many chances to fraud and misuse of account information. There is need to trust of merchant during online shopping.In existing shopping site there is need to enter more information during shopping. During payment processing sending customer data from merchant server to bank server so many chances to hack this data and misuse of them. Identity theft is the stealing of someone's identity in the form of personal information and misuse of that information for making purchase and opening of bank accounts or arranging credit cards. In 2012 consumer information was misused for an average of 48 days as a result of identity theft. Phishing is an illegitimate mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials.

Proposed system can different to existing one where only minimum amount of information can provide and successful fund transfer between consumer account to merchant account using text based steganography and visual

cryptography. In proposed system customer unique authentication password in connection to bank is hidden inside a cover text in particular image, audio, video by using text based steganography. One must still trust merchant and its employees not to use consumer now extensible to physical as well as online banking.
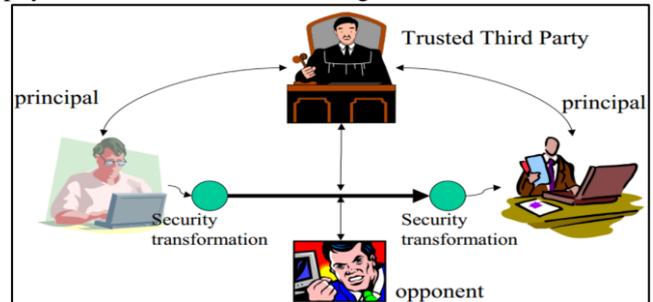

Fig. 1: Secure Data Sending System

II. STEGANOGRAPHY

In the past,People used hidden tattoos or invisible ink to convey stenographic content. Hide a secret message covering through audio, video and text file where anyone cannot access it, if any case they accept it, but don't recover an encrypted cover text. Divided share can combine only authorized user. Advantage of this method is that it require only small amount of memory and simpler to communication. The sequence of first letters of each word of the overall message spells out the real hidden message.

In text steganography message can hide by shifting line, open space, shifting word. Another published method of steganography was to put data as noise in a covering media or change the available text format and style. However, such changes attracted hackers' attention and facilitated detection of coded text. Steganography is all about creating a form of secret communication between two parties and it is a complement of Cryptography whose goal is to conceal the content of a message. Steganography uses a medium like an image, video, audio or text file to hide some information inside it in such a way that it does not attract any attention and looks like an innocent medium Steganography might be useful for secret communication in countries and regions where public use of cryptography is prohibited or restricted.
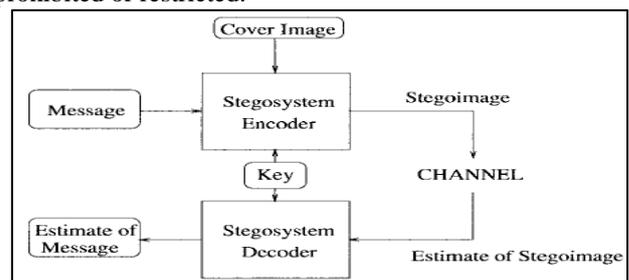

Fig. 2: Steganography System

III. VISUAL CRYPTOGRAPHY

Cryptography is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. A new method of Extended Visual Cryptography for natural images is used to produce a meaningful binary share which is predicted by Nakajima in the year 2002 presents a system which takes three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is reconstructed by printing the two output images onto transparencies and stacking them together. The use of visual cryptography is explored to preserve the privacy of an image captcha by decomposing the original image captcha into two shares that are stored in separate database servers such that the original image captcha can be revealed only when both are simultaneously available.

IV. RELATED WORKS

A related work in area of banking security based on steganography and visual cryptography. Above both systems used to minimize information sharing between consumer and online merchant and enable fund transfer from customer account to merchant account and no misuse of data. Signature based authentication system proposed in core banking but there is need to physical presence of customer. Digital signature system can be proposed by banking system and fingerprint mechanism by particular account holder. A message authentication image algorithm is proposed to protect against E-Banking fraud. Biometrics system can use to authentication system. In existing system there is no guarantee to receive data from customer account to bank database.

V. TEXT BASED STEGANOGRAPHY

Text based Steganography can use characteristic of English language like fixed word order, use periphrases for hiding data where sentence construction can easy use. In text based steganography assigning ASCII no to particular English alphabets which need to hide a secret message. Each letter has assigned a no in range 0 to 15.

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

Table 1: No Assignment

Following sentence is a cover text given below:
"My Name Is Sachin And I Am From Zeal Engg. College".

Initially encoding can be done on secret message using following encoding methods.

A. Encoding:
1) Assign an equivalent ASCII code to letter in message.
2) Convert ASCII to 8 bit binary no in a secret message.
3) Next divide 8 bit binary no to 4 bit in two parts.
4) According to 4 bit part choose suitable letter.
5) Choose a letter from particular word in secret message and construction a meaningful sentence.
6) After encryption cover text can be recover in authorize user.

B. Decoding:
Decoding is exactly opposite of a encoding process starting last step of encoding a message.

1) Collect first letter in each word of cover text message and represent it using 4 bit no.
2) Combine 4 bit binary no of cover text message and get 8 bit binary no.
3) Particular ASCII code can obtaining from 8 bit binary no in cover message.
4) According to ASCII codes assign in each letter from given no.table secret message can be recovered to cover message.

VI. RESULT

To implement text based steganography secret message is consider like:
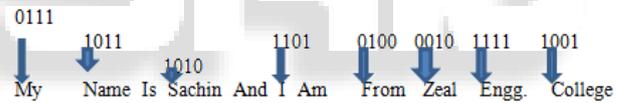Text=01111011101011010100001011111001

Fig. 3: Cover Secret Message

Drawback is to hide a large message requires a large no of word but it overcome in online banking to create a spam mail to hide banking information of particular customer.

VII. EXISTING PAYMENT PROCESSING SYSTEM IN ONLINE SHOPPING

In today's online shopping customer can login into particular shopping site then selects item from online shopping portal and add to cart. After this next goes to payment gateway and enter a personal as well as credit card information can checking by payment gateway, after this particular bank can verify account details of customer and after verifying bank can successful fund transfer from customer account to merchant account.
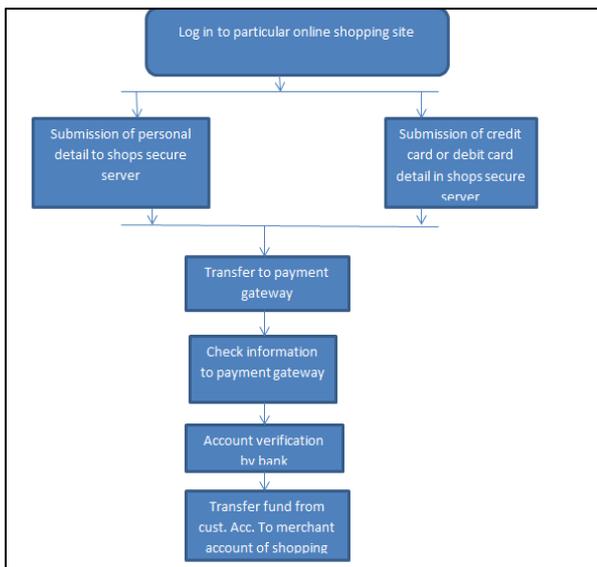
Fig. 4: Existing Online Payment System

Flipcart require a personal identification no to pay using debit card.other online shopping site like snap deal, amazon, e-bay, Jabong require a card verification value code. In existing payment system when consumer can enter his personal information to shopping site server, this time so many chances to break the security and customer data can go anywhere and payment cannot done successful. Many time online site merchant can misuse of customer information and make during payment, merchant's payment system requires directing 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.

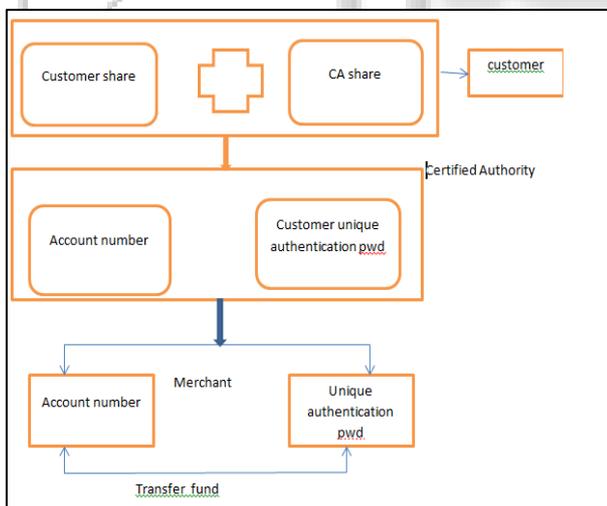VIII.   PROPOSED ONLINE PAYMENT PROCESSING SYSTEM

Fig. 5: Proposed Payment Processing System

In proposed online payment processing system only minimum amount of information can be provide and successful amount transfer between customer account to merchants account and safeguarding information using steganography and visual cryptography. Merchant can identify an amount receive in his account can be in form of account no related to card used by online shopping.

In proposed system unique authentication password is hidden inside cover text using text based steganography. Take a snapshot of this text divide it into two part like share1 and share2.Now both of two share, one share is kept to customer and remaining share kept by certified authourity.In payment gateway merchant directs customer to CA portal.in this portal customer submits its own share and merchant need to submits its account details. After done all this CA can combine its own share and customers share to recover an original image. Now CA can send this original cover text image to bank server where bank can recover a customer authentication password from cover text, then bank match customer details to his database and transfer a fund from customer account to merchant account.Customer cannot direct to merchant. After payment can receive shopping site merchant validate payment slip to CA sending customer authentication information.

If "Sachin" is customer authentication password and account number is Acc_no=12542020105
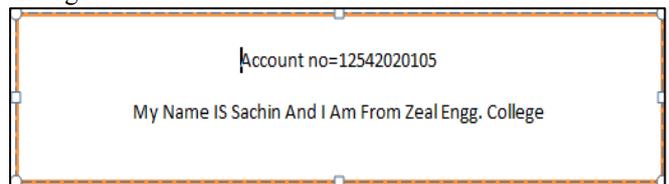Cover text="My Name Is Sachin and I Am from Zeal Engg. College"

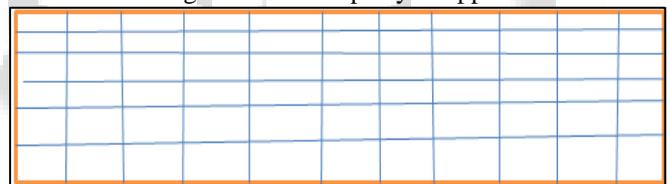Fig. 6: Snapshot of Acc_No and Cover Text

Fig. 7: Share1 Kept By Shopper

Fig. 8: Share2 Kept By CA

IX.   ADVANTAGE

- Easy fund transfer without any threat of hacking.
- Minimum amount of information can sent to merchant, so in case if merchant account can break or database can break, customer doesn't get any affect.
- Including fourth party, CA enhancing customer satisfaction to security about customer data.
- Use of steganography CA cannot get information like unique authentication password to maintain customer privacy.
- Cover text can be sent in form of email from CA to bank to avoid rising suspension

X.   CONCLUSION

In this paper a online payment processing system can propose a combine text based steganography and visual cryptography. Using both this techniques only minimum amount of information can send and fund transfer. Providing customer data privacy and prevent misuse of data at merchants site. According to related information many core

bank use a steganography and cryptography application for physical banking but our system can apply for E-Commerce which focus on online shop as well as Physical banking. Providing a security of customer data at online shopping and increasing popularity to online shopping.

REFERENCES

[1] Souvik Roy and P.Venkateshwaran "Online Payment System Using Steganography and Cryptography" at 2014 IEEE students conference on electrical, electronics and computer science.

[2] Sana Shiva and A.Hari Teja "Secure E-Marketing using Steganography and Emergence of Cryptography "in Jan 2015 at International Journal Of computer science and mobile computing.

[3] S.R.Khonde, Dheeraj Agarwal and Shrinivas Deshmukh" Online Payment System using BPCS Steganography and Visual Cryptography" at International science and research in 2012.

[4] Gokul.M,Shriram.K.Vasudevan,Umeshbabu.R and Deepak Kartik "Hybrid Steganography using Visual Cryptography and LSB Encryption Method" at International Journal of computer Application in dec.2012

[5] Ratnakirti Roy, Suvamoy Changder,Anirban Sarka and Narayan Debnath "Evaluating Image Steganography Techniques: Future research challenge at IEEE 2013.

[6] Jihui chen, Xiaoyao Xie and Fengxuan "The Security of Shopping online" Proceeding of 2011 international conference on electric and mechanical Engineering.

[7] G.Pavitra,D.S.John,Deva Prasanna "Countering Phishing Threat using Visual Cryptography" in international journal of science and research in march ,2013.

[8] J.C.Judge "Steganography: past, present, future" SANS institute nov,2001.

[9] M.Naor and A.Shamir "Visual Cryptography, Advance in Cryptography" EUROCRYPT.94, LNCS, vol.950, 1995.

[10] Javelin Strategy and research,"2013: Identify Fraud Report",http://www.javelinstrategy.com/broucher/276.

[11] Khadija Kaousar M A "Trio Framework For Secure Online Transaction Using Visual Cryptography" at international journal of science and research publications in May, 2013.

[12] Archana.B.Dhole and Prof.Nitin.J.Janwe "An Implementation of Algorithm in Cryptography in Image" at international journal of scientific and research publications in March,2013.

[13] P.S.Revenkar, Anisa Anjum, W .Z.Gandhare "Survey of Visual Cryptography Schemes" at international journal of security and its application in Apr,2010.

[14] Mrs.D.Murugeshwari, KN.Sangeeta, M.Srivani "Secure E-pay using Text based Steganos and Visual Cryptography" at international journal of engineering research and general science in jan,2015.

[15] Dr. Nidhal K. El Abbadi "New Algorithm for Text In Text Steganography" at Kufa University, Iraq.

[16] Uma Mehata "Multi-Part Data Hiding In Audio Steganography" at international journal of advance research in computer engineering and Technology in oct, 2014.