ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

E-Shopping System using Text Based Steganography and Visual Cryptography

Pooja P.Deshmukh[1], M.M.Wankhade[2]

PG Student, Department of ETC, Sinhgad College of Engineering, Vadgaon (BK), Pune, Savitribai Phule Pune University, Pune India[1]

Professor, Department of ETC, Sinhgad College of Engineering, Vadgaon (BK), Pune, Savitribai Phule Pune University, Pune India[2]

ABSTRACT: E-commerce is mostly used in whole world and its uses increased day by day. There are so manymethods which are available for payment system but it must need to prevent high level of security, speed, privacy. Thecredit and debit cards security and individual information security are major issues for the customers, merchants andbanks specifically in the case of Card not Present (CNP). This paper introduced the methods are Steganography andvisual cryptography for payment procedure. Online shopping is the retrieval of product information via the Internet andissue of purchase order through electronic purchase request, filling of credit or debit card information and shipping ofproduct by mail order or home delivery by courier. Identity theft and phishing are the common dangers of onlineshopping. Identity theft is the stealing of someone's identity in the form of personal information and misuse of thatinformation for making purchase and opening of bank accounts or arranging credit cards. In 2012 consumerinformation was misused for an average of 48 days as a result of identity theft. Phishing is a criminal mechanism thatemploys both social engineering and technical subterfuge to steal consumers' personal identity data and financialaccount credentials. Payment Service, Financial and Retail Service are the most targeted industrial sectors of phishing attacks. Secure Socket Layer (SSL) encryption prevents the interception of consumer information in transit between theconsumer and the online merchant. However, one must still trust merchant and its employees not to use consumerinformation for their own purchases and not to sell the information to others. In this paper, a new method is proposed,that uses text based Steganography and visual cryptography, which minimizes information sharing between consumerand online merchant but enable successful fund transfer from consumer's account to merchant's account therebysafeguarding consumer information and preventing misuse of information at merchant side. The method proposed isspecifically for E-Commerce but can easily be extended for online as well as physical banking.

KEYWORDS: Information security; Steganography; Visual Cryptography; e-shopping

I. INTRODUCTION

Steganography is the art of hiding of a message within another so that hidden message is indistinguishable. The keyconcept behind Steganography is that message to be transmitted is not detectable to casual eye. Text, image, Video, audio are used as a cover media for hiding data in Steganography. In text Steganography, message can behidden by shifting word and line, in open spaces, in word sequence. Properties of a sentence such as numberof words, number of characters, number of vowels, position of vowels in a word are also used to hide secret message.The advantage of preferring text Steganography over other Steganography techniques is its smaller memory requirementand simpler communication. Visual Cryptography (VC), proposed by Naor et al., is a cryptographictechnique based on visual secret sharing used for image encryption. Using k out of n (k, n) visual secret sharing schemea secret image is encrypted in shares which are meaningless images that can be transmitted or distributed over anuntrusted communication channel. Only combining the k shares or more give the original secret image. Onlineshopping is the retrieval of product information via the Internet and issue of purchase order through electronicpurchase request, filling of credit or debit card information and shipping of product by mail order or home delivery bycourier. Identity theft and phishing are the common dangers of online shopping. Identity theft is the stealing ofsomeone's identity in the form of personal

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

information and misusing that information for making purchase and openingof bank accounts or arranging credit cards. In 2012 consumer information was misused for an average of 48 days as aresult of identity theft. Phishing is an illegitimate mechanism that employs both social engineering and technicalsubterfuge to steal consumers' personal identity data and financial account credentials. Payment Service, Financialand Retail Service are the most focused industrial sectors of phishing attacks. Secure Socket Layer (SSL) encryptioninhibits the interference of consumer information in transit between the consumer and the online merchant. However, one must still trust merchant and its employees not to use consumer information for their own purchases andnot to sell the information to others. In this paper, a new method is proposed, that uses text based Steganography andvisual cryptography, which minimizes information sharing between consumer and online merchant but enablesuccessful fund transfer from consumer's account to merchant's account thereby safeguarding consumer informationand preventing misuse of information at merchant side. E-shopping is used to get back product data by using internetand proceeds to purchase club to completion of electronic purchase requesting, filling of credit/debit card information..Identify theft and phishing are main issues which faced by customer, merchant and bank and these are mainly containto theft provided information and prevention of security purpose. In this paper, a new method is proposed, that appliesthe combined used of text based Steganography also, visual cryptography, which represents data managing amongstclient and online vendor however empower fruitful asset exchange from client's record.

A. STEGANOGRAPHY–

Steganography is the procedure of hiding a message which can hide by using image; video etc. so original message isunclear. A message can be hidden by creating meaningful sentence which uses number of words, characters andvowels, position of vowels are also used.

B. VISUAL CRYPTOGRAPHY –

In Naor said that visual cryptography is a technique which is based on visual hidden sharing used for image encryptionpurpose. Visual Cryptography contains every hidden pixels of the original binary image which is converted into foursub pixel of two hidden shared images.

II. OBJECTIVE

1. The system implemented for the payment procedure for e-shopping by combining use of applicationof Steganography and visual cryptography which maintains the data of customer secure and preventingthe misuse of data at merchant's side.
2. This method is implementing for prevention of theft and customer data security.
3. The other banking applications uses Steganography and visual cryptography basically used for personalbanking, but this method can be used for the E-Commerce with focus area on payment procedure duringe-shopping as well as personal banking.

III. RELATED WORK

A brief survey of related work in the area of banking security based on Steganography and visual cryptography ispresented in this section. A customer authentication system using visual cryptography is presented but it isspecifically designed for physical banking. A signature based authentication system for core banking is proposed but it also requires physical presence of the customer presenting the share.a combined image basedSteganography and visual cryptography authentication system for customer authentication in core banking. A messageauthentication image algorithm is proposed to protect against e-banking fraud. A biometrics in conjunction withvisual cryptography is used as authentication system. Proposed text based Steganography uses characteristics ofEnglish language such as inflexion, fixed word order and use of periphrases for hiding data rather than using propertiesof a sentence. This gives flexibility and freedom from the point view of sentence construction but itincreases computational complexity. The Steganography technique is based on Vedic Numeric Code whichcoding is based on tongue position. For applying the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Vedic code to English alphabet, frequency of letters in Englishvocabulary is used as the basis for assigning numbers to the letters in English alphabet. Number assignments ofletters are shown in table 1. No separate importance is given for vowels and consonants. Eachletter is assigned a number in the range of 0 to 15. For different frequencies, different numbers are assigned to theletters. Number assigned in range (N+0.99) % to (N+0.3) % and (N+0.2) % to (N+0.01) % is same where N is anyinteger from 0 to 11. It basically represents frequency of letters in integer form. Above number assignment method isused to maximize no of letters in a particular assigned number group which in turn gives flexibility in word choosingand ultimately results in suitable sentence construction. A brief survey of related work in the area of banking securitybased on Steganography and visual cryptography is presented in this section. A customer authentication system usingvisual cryptography is presented in but it is specifically designed for physical banking. A signature basedauthentication system for core banking is proposed in but it also requires physical presence of the customer presenting [9] the share. Proposes a combined image based Steganography and visual cryptography authenticationsystem for customer authentication in core banking. A message authentication image algorithm is proposed in toprotect against e-banking fraud [15]. A biometrics in conjunction with visual cryptography is used as authenticationsystem. No different significance is given for vowels and consonants when contrasted.

Table 1: Number assignment

LETTER	NUMBER ASSIGNED	LETTER	NUMBER ASSIGMENT
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 useful for to create the meaningful sentence.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

IV. PROPOSED SYSTEM DESIGN

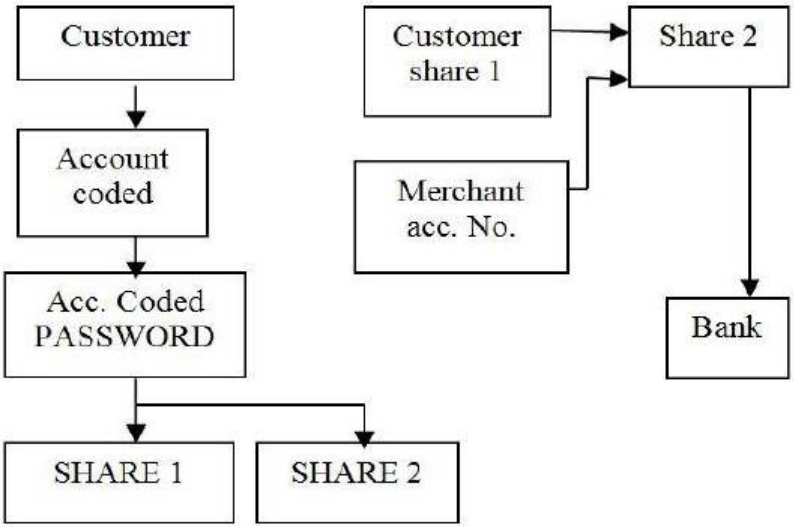


Fig.1.Block Diagram of E-retailing system

During online shopping, customer required the account number and password for payment procedure as shown in fig.1.After providing account number and password, apply text based Steganography on provided password. Password getsin two shares with one share kept by customer and other share kept by certified authority. The certified authority shareprovided to bank for check to information is right or not. After this process the merchant get new account andpassword, purchasing the product online.

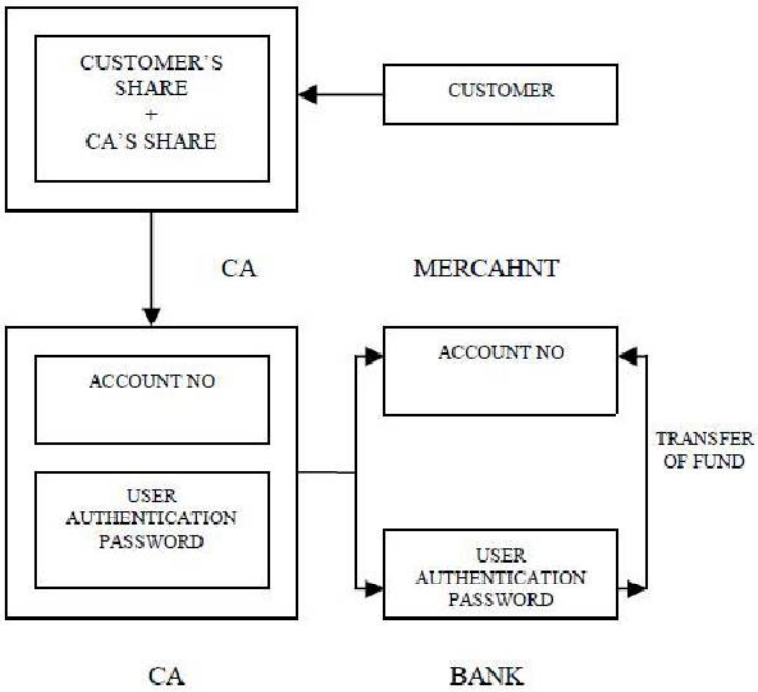


Fig .2. Proposed payment system [2]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

In the proposed framework, the data presented by the client to the online vendor is minimized by giving just least datathat will just check the installment made by the said client from its ledger. Introduction achieved by the Centralcertified authority (CA) uses the combination of Steganography and cryptography along with some information of Person provided by it. The Card Verification Value (CVV) is provided with the card which is used for e-shopping. Fig.2.shows proposed payment system.

1. Encoding Procedure-
Input: text file
Output: secret key image
Steps:
1. Each letter in the message are represented by its equivalent ASCII value and it is secret..
2. ASCII code to equivalent 8 bit binary number conversion.
3. Division of 8 bit binary number into two 4 bit binary.
4. Selection of suitable letters with number assignment according to the table corresponding to the 4 bit parts.
5. Construction of sentence according to letters as first letter as suitable word.
6. using of transformation of sentence produce emit key picture shares and shape in jpeg/bmp structure.

2. Transaction in online shopping –

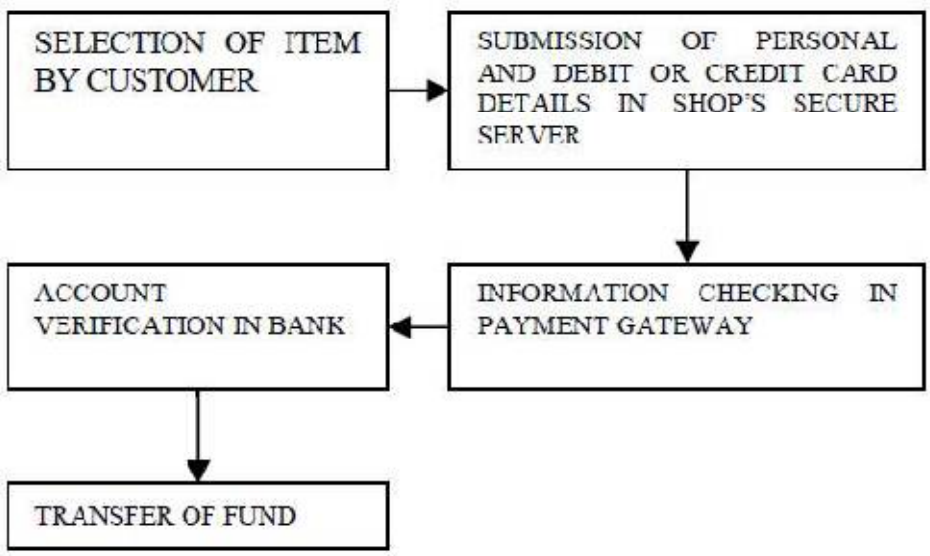


Fig 3. Payment procedure [1]

The payment procedure is given in figure 4. In payment gateway procedure the customer has to submit their credit ordebit details like name, card's number which gives on credit card and debit card etc.

A. Customer Authentication: Customer's unique password is provided by the bank which is hidden inside in a covertext by using text based Steganography method. The information like account no of the user is connected with merchantis placed above the cover text in its secret form. Now two shares are obtained and one share is kept by the customer andthe other share is kept by certified authority (CA).

B. Certification Authority (CA) Access –
During the time of e-shopping when the selection of particular item is done and it is added, the select payment gatewayoption of merchant will direct the customer to certified authority (CA) gateway. In gateway, both seller and merchantcan submit their shares. Later when their respective shares are received the CA performs a combine operation

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

were itsown share will be combined with the shopper share to obtain original value of share. Presently CA, send trader accountsubtle elements which is in spread content structure to the bank where client confirmation secret key is recuperatedfrom the spread content shipper account points of interest, spread content are sent to the bank where client verificationdata is sent to the vendor by CA. After accepting client verification secret word, bank matches it with its own particulardatabase and subsequent to advocating client, exchanges reserve from the client record to the submitted seller'saccount.

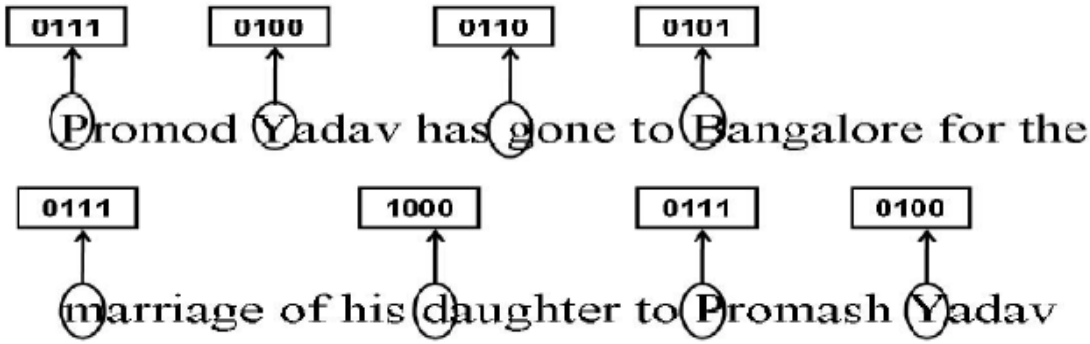
3. Decoding Procedure

Input: two secret key images
Output: original secret key image
Steps:
1. First letter is represented by its equivalent 4 bit binary number for each first letter of message.
2. 4 bit binary numbers are combined to get 8 bit binary number.
3. 8 Bit binary numbers are used to get ASCII code values.
4. ASCII code values are used to get secret shares.
5. Finally, Original secret key is obtained.

VI. SIMULATION AND TESTING RESULTS

1. Result

To actualize the above content based Steganography technique, a mystery message is considered. Assume it is "content".
Content = 01110100011001010111100001110100



Customer selects the order and filled the personal information like account no., CVV. Fig.5. shows the payment gateway window.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

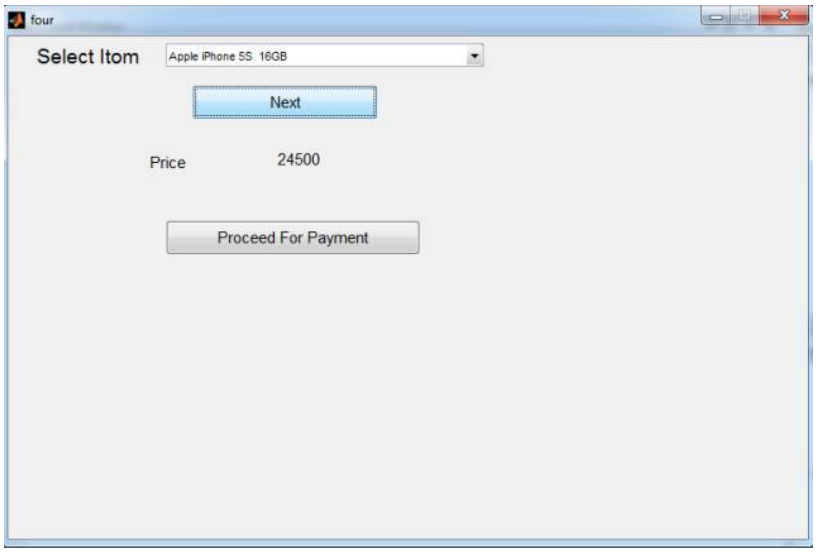


Fig 5. Payment gateway window

When the scheme is executed in MATLAB R2015 version is displayed. The snapshot is taken when first teganography and visual cryptography is used. Fig 5 shows the result of after applying steganography by using GUI.

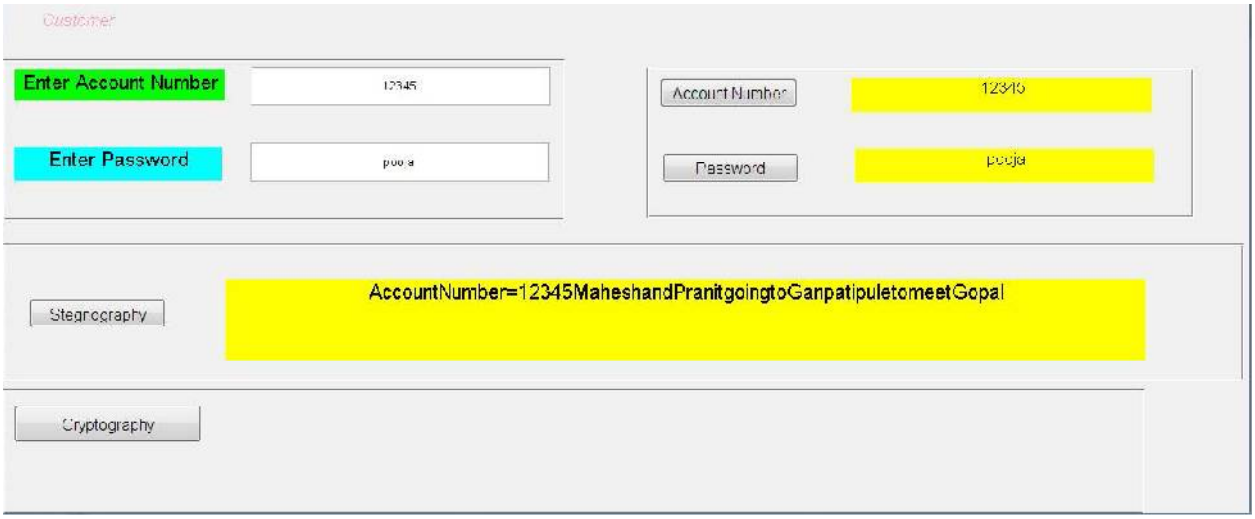


Fig 6.Result of encryption

2. Cases Obtained

Snapshot account no and cover text [1]

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

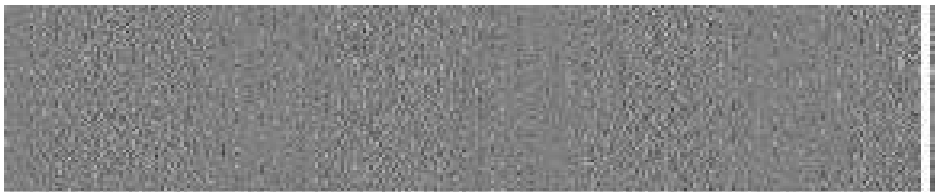
Share 1 kept by customer [1]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

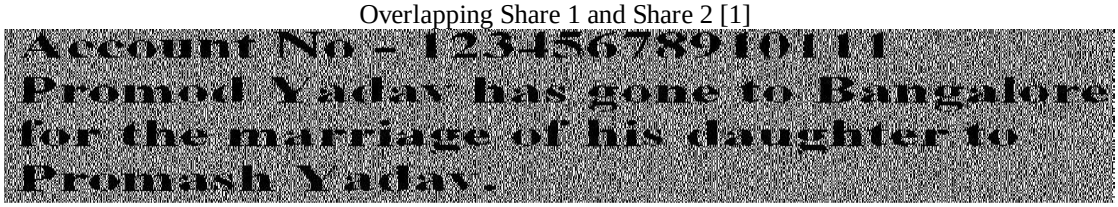
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016



Share 2 kept by CA [1]

Overlapping Share 1 and Share 2 [1]



The below figure shows the main result which obtained after applying visual cryptography.

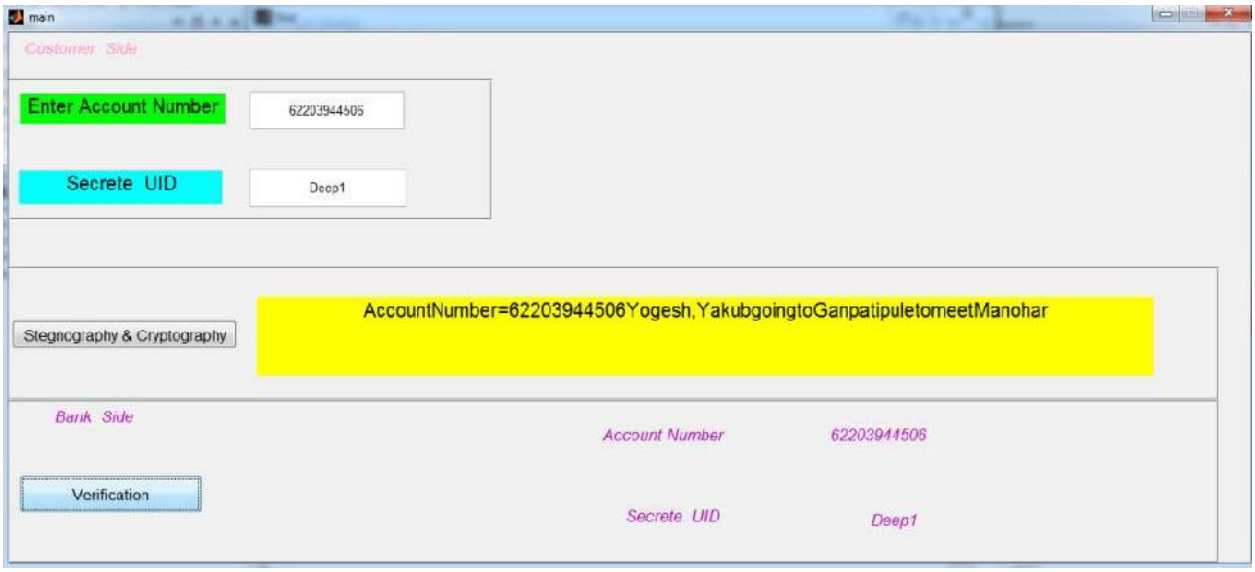


Fig 7.Result shows of decryption

VII. CONCLUSION

In this paper, the system proposed the payment procedure for e-shopping by combining use of application of Steganography and visual cryptography which maintains the data of customer secure and preventing the misuse of data at merchant's side. This method is implementing for prevention of theft and customer data security. The other banking

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

applications uses Steganography and visual cryptography basically used for personal banking, but this method can be used for the E-Commerce with focus area on payment procedure during e-shopping as well as personal banking.

REFERENCES

[1]Souvik Roy1 and P. Venkateswarant "Online Payment System using Steganography and Visual Cryptography" IEEE Students' Conference on Electrical, Electronics and Computer Science of2014
[2] 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
[3] Jihui Chen, XiaoyaoXie, and Fengxuan Jing, "The security of shopping Online," Proceedings of 2011 International Conference on Electronic andMechanical Engineering and Information Technology (EMEIT), vol. 9, pp. 4693-4696, 2011.
[4] Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, "Techniques for Data Hiding," IBM Systems Journal, Vol.35, Nos. 3 & 4, pp. 313-336, 1996.
[5] Jaya, Siddharth Malik, AbhinavAggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography," Proceedings of 2011 World Congress on Information and Communication Technologies.
[6] Bharati Krishna Tirthaji, "Vedic Mathematics and its Spiritual Dimension," Motilal Bansari Publishers,1992.
[7]http://oxforddictionaries.com/words/what-is-the-frequency-of-theletters- of-the-alphabet-in-english.
[8] 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.
[9]Javelin Strategy & Research, "2013 Identify Fraud Report, https://www.javelinstrategy.com/brochure/276
[5] J. Chen, T. S. Chen, M. W. Cheng, "A New Data Hiding Scheme in Binary Image," Proceeding of Fifth International Symposium on MultimediaSoftware Engineering, pp. 88-93, 2003.
[6] 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.
[7] Daniel Gruhl, Anthony Lu, Walter Bender, "Echo Hiding," Proceedings of the First International Workshop on Information Hidding, pp. 293-315, Cambridge, UK, 1996.
[8] Walter Bender, Daniel Gruhl, Norishige Morimoto, A.Lu, "Techniques for Data Hiding," IBM Systems Journal, Vol. 35, Nos. 3 & 4, pp. 313-336, 1996.
[9] K. Bennet, "Linguistic Steganography: Surevey, Analysis, and Robustness Concerns for Hiding information in Text," Purdue University, CeriasTech Report 2004—2013.
[10] J.C. Judge, "Steganography: Past, Present, Future," SANS Institute, November 30, 2001.
[11] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptograhy: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.
[12] Jaya, Siddharth Malik, AbhinavAggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography," Proceedings of 2011 World Congress on Information and Communication Technologies, pp. 1181-1186, Mumbai, India, 2011.
[13] 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, pp. 65-72, Chennai, India, 2008