International Journal of Recent Trends in Engineering & Research
ISSN : 2455-1457 Impact Factor : 3.344

Secure Online Transaction Using Text Steganography and Visual Cryptography

[1]Neha Jain,Suraj Gupta[2], Ajaykumar Prajapati[3], Manoj Verma[4]
[1]Asst.Prof.,Dept. of Computer Engineering
Shree L.R.Tiwari College of Engineering,Mumbai, India
[2,3,4]B.E. Student , Dept. of Computer Engineering
Shree L.R.Tiwari College of Engineering,Mumbai, India

Abstract— An increasing popularity of online shopping in india i.e. peoples from city and rural area have craze of online shopping. Debit or credit card fraud and personal information security are major concern for merchants, customers and banks. In this project we use a new approach for online transaction to hide the information in a securely and secure transaction. A consumer sends his payment information directly to a payment portal verifying the consumer, allows the transaction and sends a payment receipt to the appropriate merchant .we will use the text steganography and visual cryptography to secure online transaction to protect consumer data from hacker and an internet susceptibilities.

Keywords— Payment Portal; Steganography; Online shopping; Visual Cryptography.

I. INTRODUCTION

Online shopping is a form of electronic commerce which allows consumers to directly buy goods or services. Online shopping has grown in popularity over the years, mainly because people find it convenient and easy to bargain shop from the comfort of their home or office. The concept of e-commerce is, however, not just limited to buying and selling of goods. It also includes the entire purchase process of developing, marketing, vending, supplying, servicing and paying for products and services.Payment system and protocol have been developed, with the development of e-commerce. The current payment system consists of merchants, consumers and transaction portals such that a merchant receives a consumer's payment information and forwards it to a payment portal to process the payment. This, however, exposes a consumer's payment information to risks, because a merchant can save the consumer's payment information in either plain or encrypted form and may misuse it later. It is also possible that a merchant's server, through which a consumer's payment information is forwarded to a payment portal, is compromised and the merchant is unaware of it.

We propose a payment method that does not send consumer payment information to merchants and allows only payment portal to deal with it. Payment portal are secure and reliable, because they comply with the standard data security rules and communicate with banks and credit card companies using the most secure methods and technologies. To strengthen data security, the implemention of a new payment portal scheme is introduced along with visual cryptography & steganography in our proposed online payment system.

A. Steganography

Steganography[3] is the process of masking sensitive information in any media to transfer it securely over the underlying unreliable and insecure communication network. In text Steganography, message can be hidden by shifting word and line, in open spaces, in word succession. Attributes of a conviction such as number of phrases, number of characters, num of vowels, location of vowels in a word are also used to hide private message. The advantage of choosing text Steganography over other Steganography

techniques is its smaller memory requirement and simpler communication.

B. Visual Cryptography

Visual cryptography[7] (VC) is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Visual cryptography (VC), proposed by Naor and Shamir, is a method for protecting image-based secrets that has a computation-free decryption process. In the (2, 2) VC scheme each secret image is divided into two shares such that no information can be reconstructed from any single share. Each share is printed in transparencies. The decryption is achieved by stacking the two shares and the secret image can be visualized by naked eye without any complex cryptographic computations.

II. EXISTING SYSTEM

The Exiting payment system consists of merchants, consumers and transaction portals such that a merchant receives a consumer's payment information and forwards it to a payment portal to process the payment. This, however, exposes a consumer's payment information to risks. It is Possible that a merchant's server, through which a consumer's payment information is forwarded to a payment portal, is compromised.

At present most of the banking system uses One Time Password(OTP) as a security measures in credit card payment system in online shopping. Some application uses captcha images to avoid automated program from hacking the secret codes. One Time Password is a secure system which will generates 4 digit or 6 digit random numbers and send to the authorized user's Mobile phone whenever they are plan to make the payment through credit card in online. One copy of OTP is stored in server and user is requested to enter the received OTP. When user types OTP, then the input OTP is compared with stored OTP in server if both are matching, Transaction process move further else it will produce error message.

A. Drawbacks

- Online shopping is happing in Internet and OTP will send to user mobile, Both are different channel.
- Sometimes mobile signal is Weak, the user may not get the OTP.
- There is always time delay in SMS deliver in Peak hours because of big queue in SMS gateway.
- OTP has a life cycle of 5 minutes, After that it is Useless. So that if you get OTP after 5 minutes then it has no importance.

III. PROPOSED METHODOLOGY

The proposed system prescribed in this project is to handle applications that require a high level of security, such as E- Commerce applications, core banking and internet banking. This can be done by using combination of two applications: Text Steganography and Visual Cryptography for safe online shopping and consumer satisfaction. Online shopping is generally considered as 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.

In the proposed solution, information submitted by the customer to the online merchant is minimized by providing only minimum information that will only verify the payment made by the said customer from its bank account. This is achieved by the introduction of a central Certified Authority (CA) and combined application of steganography and visual cryptography. The information received by the merchant can be in the form of account number related to the card used for shopping. The information will only validate receipt of payment from authentic customer.

In the proposed method, customer unique authentication password in connection to the bank is hidden inside a cover text using the text based steganography method. Customer authentication information (account no) in connection with merchant is placed above the cover text in its original form.

Now a snapshot of two texts is taken. From the snapshot image, two shares are generated using visual cryptography.

In our proposed system of online shopping, user logs in and enters into the online store to view the products. When he/she adds the item to the cart, he/she will be entering the card no and unique authentication password. This

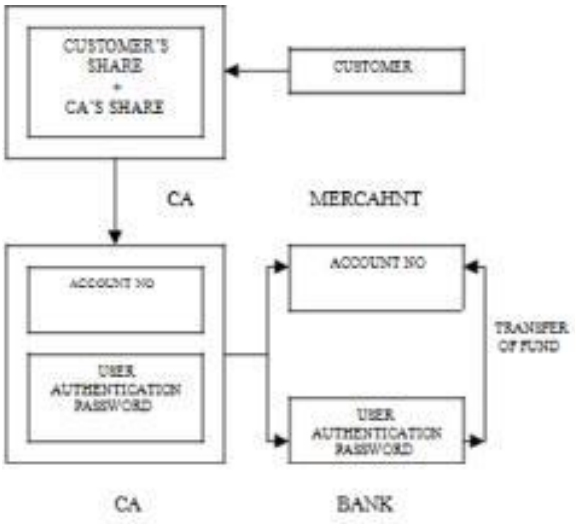

Fig. 1. Proposed payment system

information will be created as a stego or stegno image using BPCS Steganography. 2-out-2 algorithm of visual cryptography will create two shares out of the stegno image. (Customer's share and CA's share). CA browses user's share and generates the card no which is sent to the bank so as to extract the customer's PIN (de-steganography). Finally fund will be transferred from the bank to the merchant.

A. Steganography Algorithm

Encoding Steps :

- Representation of each letter in secret message by its equivalent ASCII code.
- Conversion of ASCII code to equivalent 8 bit binary number.
- Division of 8 bit binary number into two 4 bit parts.
- Choosing of suitable letters from table 1 corresponding to the 4 bit parts.
- Meaningful sentence construction by using letters obtained as the first letters of suitable words.
- Omission of articles, pronoun, preposition, adverb, was/were, is/am/are, has/have/had, will/shall, and would/should in coding process to give flexibility in sentence construction
- Encoding is not case sensitive.

Decoding Steps :

- First letter in each word of cover message is taken and represented by corresponding 4 bit number.
- 4 bit binary numbers of combined to obtain 8 bit number.
- ASCII codes are obtained from 8 bit numbers.
- Finally secret message is recovered from ASCII codes.

TABLE I. NUMBER ASSIGNMENT

Lesser	*\itttlheir U.'f.'fil'/Tl'J*	*Lester*	*Atithket* untJlW
t	*]5*	M	*7*
A	14	H	*7*
R	13	*(i*	6
I	]j	*B*	*5*
0	12	F	*4*
T	11	Y	*4*
N	11	W	*3*
S	*ID*	K	*3*
L	*LD*	V	*3*
C	*9*	*X*	*2*
u	*S*	*z*	*2*
D	*s*	*J*	L
F	*7*		0

B. Visual Cryptography Algorithm

- Visual cryptography is a type of cryptography which allows the visual information to be encrypted in such a way that their decryption can be performed by human visual system.
- Every secret pixel of the original binary image is converted into four sub pixel of two share images and recovered by simple stacking process. The two apparently random images can now be combined using an exclusive-or (XOR) to re-create the original image.

IV. RESULTS AND ANALYSIS

The customer unique authentication password in connection to the bank is hidden inside a cover text using the text based steganography. Customer authentication password i.e. account no. in connection with merchant is placed above the cover text in its original form. now a snapsort of two texts is taken shown in Fig. 2, two share are generated using visual cryptography.one share is kept by the constomer as shown in Fig. 3,other share is kept in the database of CA as shown in Fig. 4, now CA combines its own share with constomer share to obtain the original image. which helps to check that customer is Authenticate or not.

Account No - 12345678910111 Promod Yadov has none to Bangalore lor the marriage of his daughter to Promash Yadav.

Fig. 2. Snapshot account no. and cover text

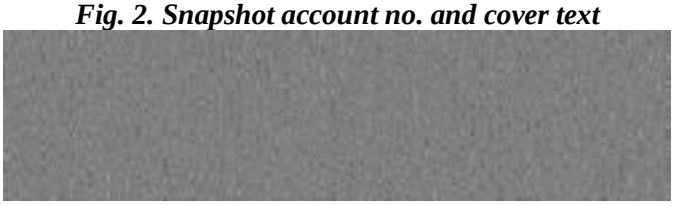

Fig. 4. Share 2 kept by CA.
Fig. 3. Share 1 kept by customer.

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

Fig. 5. Overlapping of share 1 and share 2.

A. Advantages

- Proposed method minimizes customer information sent to the online merchant. So in case of a breach in merchant's database, customer doesn't get affected. It also prevents unlawful use of customer information at merchant's side.
- Presence of a fourth party, CA, enhances customer's satisfaction and security further as more number of parties are involved in the process.
- Usage of steganography ensures that the CA does not know customer authentication password thus maintaining customer privacy.
- Cover text can be sent in the form of email from CA to bank to avoid rising suspicion. Since customer data is distributed over 3 parties, a breach in single database can easily be contented.

V. CONCLUSIONS

In this paper, a payment system for online shopping is proposed by combining text based steganography and visual cryptography that provides customer data privacy and prevents misuse of data at merchant's side. The method is concerned only with prevention of identify theft and customer data security. In comparison to other banking application which uses steganography and visual cryptography [4, 8, and 9], are basically applied for physical banking, the proposed method can be applied for E-Commerce with focus area on payment during online shopping as well as physical banking.

REFERENCES

i. U.Naresh, U.Vidya Sagar, C.V. Madhusudan Reddy , " Intelligent Phishing Website Detection and Prevention System by Using Lin Guard Algorithm," in Proc. IOSR, 2013. Vol. 14(Issue 3), pp 28-36.
ii. Souvik Roy, P.Venkateswaran, "Online Payment System using Steganography and Visual Cryptography," Proceedings of IEEE Students' Conference on Electrical, Electronics and Computer Science,2014.
iii. Pranita P. Khairnar, Prof. V. Ubale, " Steganography Using BPCS technology,"in Proc. International Journal Of Engineering And Science , May 2013. Vol.3(Issue 2),pp 08-16.
iv. S.Premkumar, A.E.Narayanan, "New Visual Steganography Scheme for Secure Banking Application," Proceeding of 2012 Internat ional Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp.1013 - 1016, Kumaracoil,India,201.
v. Jihui Chen, Xiaoyao Xie, and Fengxuan Jing, "The security of shoppingOnline," Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology
vi. (EMEIT), vol. 9, pp. 4693-4696, 2011. Javelin Strategy & Research, "2013 Identify
vii. FraudReport,https://www.javelinstrategy.com/brochure/276.
viii. Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, "Techniques for Data Hiding," IBM Systems Journal, Vol.35, Nos. 3 & 4, pp. 313336, 1996.
ix. M. Naor nd A. Shamir, "Visual cryptography," Advances in Cryptograhy: EUROCRYPT'94, LNCS, vol. 950, pp. 1-12, 1995.
x. 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

xi. Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography," Proceedings of 2011 World Congress on Information and Communication Technologies.
xii. C. Pautasso, T. Heinis, and G. Alonso, "Autonomic resource provisioning for software business processes," Information and Software Technology
xiii. S. Suryadevara, R. Naaz, Shweta, S. Kapoor, "Visual cryptography improvises the security of tongue as a biometric in banking system," Proceedings of 2011 2nd International Conference on Computer and Communication Technology (ICCCT), pp. 412 - 415, 2011.
xiv. S. Suryadevara, R. Naaz, Shweta, S. Kapoor, "Visual cryptography improvises the security of tongue as a biometric in banking system," Proceedings of 2011 2nd International Conference on Computer and Communication Technology (ICCCT), pp. 412 - 415, 2011.
xv. Kalavathi Alla, 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.
xvi. N. Laranjeiro and M. Vieira, "Towards fault tolerance in web services compositions," in Proc. of the workshop on engineering fault tolerant systems.

