Cheating Prevention in E-payment System using Visual Cryptography

Ms. Shital B Patel[1] & Dr. Vinod L Desai[2]
[1]Research Scholar, RK University, Kastubadham, Rajkot
[2]Assistant Professor, Department of Computer Science, Gujarat Vidyapith, Ahmedabad

Received: August 26, 2018 Accepted: October 16, 2018

ABSTRACT *In recent years E-commerce enlarged a tremendous growth in the world. A day by day growing popularity of online shopping, debit or credit cards, phishing and personal information. Security is the main concern of customers, merchants and banks. A Having used the online transaction quickly, debit and credit card fraud and the consolidation of personal information are a real problem for the customer. Online retailers must also modernize their banks and adhere to their security and policies to limit this type of fraud. The objective behind this proposal is to enhance the existing E-commerce and online shopping retailer's application security. By using this system we can reduce the content shared between the end users and E-commerce business by making sure that the money will be transferred successfully to the retailers with encapsulating the customer information so that such information is not misuse by the merchandise. In this paper we have proposed new approach for secure online payment system using Visual Cryptography (VC).*

Keywords: *Online shopping, E-commerce, E-payment, Visual cryptography, shares.*

1. INTRODUCTION

The process of buying products through web browser referring E-shopping instead of using mortar stores. No of users on internet has exponentially increased a day by day, this growth has given a big expansion to online shopping. Online shopping is basically a process to check, feel and order the large number order of product available for sell by the online retailers. We just need to select the product on the online retailer's website, it will generate the digital purchase order, after this we have to provide the credit or debit card details and the product you have selected will be delivered to you by mail order or home delivery by courier [1].

E-payment system is an alternative explanation provided to customer to have cashless transaction in returns to the services/purchase done. Simply we can say that e-payment is a device by which customer can make Online Payments for his/her purchase of valuable items or services without
physical transfer of cash and cheques, irrespective of time and location. It is the basis of online payments and on-line payment system development is a higher form of electronic payments. It makes electronic transaction available 24*7 using internet network to support ecommerce [2].

Identity theft and phishing are the major drawback of online shopping. Phishing is an unprofessional way to steal the end users personal as well as banking data. Some technical professionals are used to hack this data from online retailers so that they can misuse this data. Identity theft is an act of stealing and assuming another person's identity in order to commit fraud or other crimes like using this data for purchasing or opening new bank account.

To protect the stealing of data between end users and online merchant website we have to use Secure Socket Layer (SSL) encryption , This encryption make sure that the data will be encapsulated and tunneled in such a way that during the transfer it cannot be hacked. Still this data will be available with the retailers, so we have trust the employees of online merchandise for not sharing the data or using this data for their own use. We are proposing a new method for this.

In this paper, Proposed method uses visual comprehension by textual bases, access to at least information and communication between clients and members of the commission. If this information is protected by the customer and by the user, it is also provided by the customer information. The proposed content is particularly interesting for e-commerce, but it is widely extended for online banking.

The rest of the paper is organized as follows: Section II gives brief description of visual cryptography. Section III contains literature survey. Section IV presents the current methodology for e-payment was actually done. Section V provides proposed payment method. Section VI concludes the paper.

2. VISUAL CRYPTOGRAPHY

Naor and Shamir suggested a new idea of visual cryptography (VC) in 1994 [3]. Visual cryptography, a developing cryptography method, uses the features of human visualization to decode the encrypted images. It involves neither cryptography information nor difficult calculation. For protecting purpose, it also protect that hackers cannot identify any hints about a secret image from separate cover images. The essential knowledge is to dividing the data into n parts recognized as the shares. Only when a appreciate amount of shares are stacked composed will human eyes identify the image content.

Visual cryptography protect secrets inside the images. Image is distributed into several shares and later decode without any computation. This decoding is done by overlapping the shares which will expose the secret image or text by the human visual system. At the beginning of the model which was established involves of a cipher text and a page of transparency [8]. The initial text is recover by overlapping the transparency with the key bygone the cipher text. More recent, this model is enlarged with k from a secret sharing pattern, where secret sharing is a method where secret shares are scattered between the participants. Thus, the secret can only publish when an appropriate number of shares are stacked together. The (k, n) secret sharing scheme exposes a secret image only when k or more than k shares are arranged. But share less than k will not expose any information.

In secret sharing method used combination of black and white pixels in image and text. These white and black pixels show in n converted version called shares. Each shares contains of a collection of black and white subpixels. Examine visual cryptographic scheme:

White pixel always produces one black and white subpixel after superimposing however loss pixel results two blacks subpixels. When shares are stacked collected, if the number of subpixel is more than stable threshold then that pixel is measured as “on” if it less then stable threshold it is measured as “off”. It represent in Figure.2.

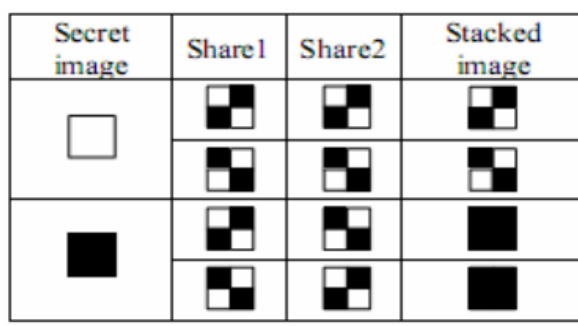

Fig. 1. Construction of (2, 2) VC

3. LITERATURE SURVEY

V Hemanth, M Shareef and K S Ranjith [4] in “Anti-Phishing uses Visual Cryptography” in this paper they received result for anti-phishing with the use of visual cryptography. Online banking system use visual cryptography for enhancing security. By implementing visual cryptography method the phishing attack can be exclude. Analyze how to phishing attacks arise and how to determine an E-mail is blackmail.

B.Srikanth, G.Padmaja, Dr. Syed Khasi, Dr. P.V.S.Lakshmi and A.Haritha proposed a method where signature of the applicant will be used as input and this input will be divided into number of shares depending on bank scheme. One share will be kept with the bank and all other shares based on scheme will be given to applicant. During every transaction applicant need to supply his shares. This shares are overlapped with the share present in the bank. And Authentication check is performed using correlation technique. If the correlation coefficient value is higher than authentication is succeeded [6].

Souvik Roya, P.Venkateswaranb presents a different approach to the English text based steganography with Indian root In the propose method, Resources of sentences are not used ,rather attributes of English language like use of periphrases ,inflection and fixed word order are used. This gives us ability to flexibly perform sentence creation but increases computational complexity [5].

Souvik Roy and P.Venkateswaran Provided a new approach where limited information need to be shared for money transfer process while doing online shopping. End users personal data is also prevented from identity theft. They have used steganography and visual cryptography for this purpose [8].

S. R. Navale, S. S. Khandagale, R. A. Malpekar, Prof. N. K. Chouhan uses a text based steganography and RG-based Visual Cryptography to pro-pose on secure online payment system where a consumer the payment information will be sent directly to a payment portal and dealers are not receiving a consumer payment information, also encrypted / hashed form[9].

3.1. Comparative Analysis

In this paper we compare different method that work on online transaction so comparison see in below table 1.

Table 1: Comparison

Sr. No.	Name of Paper	Method	Advantages	Disadvantages
1	A Text based Steganography technique with an indian root.	Vedic numeric code.	Flexibility and Freedom for sentence creation	Increases computational complexity.
2	Authorization of the medical bank of the process of image processing and visual representation.	Authorization of the medical bank of the process of image processing and visual representation.	This technique shield the customer information to defend the possible forgery.	Need physical presence of applicant to sign an application from while opening a bank account.
3	Online Payment System using Steganography and Visual Cryptography.	Vedic numeric code and Traditional Visual Cryptography.	Prevents unlawful use of customer's data on merchant side.	Meaningless shares are generated and transmitted over an untrusted communication channel.
4	Approach for Secure online transaction using Visual Cryptography and Text Steganography (Proposed Method).	Text Steganography using Ascii code and RG based Visual Cryptography.	Customer privacy is prevented from CA as well as Merchant. No pixel expansion while creating shares.	Lower Visual Quality.

4. CURRENT METHODOLOGY

In current scenario, there are mainly 3 entities involved namely Customer or Client, Merchant server and Bank Server. The task of Customer or Client is to first make an account at merchant server. Client needs to fill username, password, e-mail address, residential address, credit card details and other confidential information in order to login to merchant site.

After login is successful, Client will select product which he/she wants to purchase. After making a request to purchase a product, Merchant server will send this information to Bank server. In turn Bank server will send OTP to Client in order to authenticate the request raised by

Client. At client side OTP is validated and purchase order is placed. This OTP is valid till 10 mins.

When Client is logged in, sensitive information such as credit card details can be captured by attacker or the site can be a phishing website.

e ISSN 2348 –1269, Print ISSN 2349-5138
Cosmos Impact Factor 4.236

Fig. 2. Current Methodology of Online Payment System

5. PROPOSED SYSTEM

In order to purchase any goods customer needs to fill his/her confidential details at Merchant site but Customer doesn't know whether merchant is genuine or not. So In proposed e-payment method will share minimum information to the merchant. The proposed method includes three main characters for online transactions: customer, bank, merchant or retailer. Before purchasing online, the customer must open a bank account by providing his personal details to the bank. When customer open account in bank, bank will give a private key and this private key divided into two shares. One share will keep bank in its database and other share will give to the customer. The version is created by applying visual cryptography to a snapshot of text containing the customer's account number and debit and credit card information. By using these shares customer can perform secure e-shopping. In Figure 3, Figure 4, Figure 5 and Figure 6 See how the share is generated and the customer sees his / her personal information when the shares overlap.

Account no: 00261001003311
Name: Patel Shital
City: Ahmedabad

Fig. 3. Snapshot account no and Personal Information

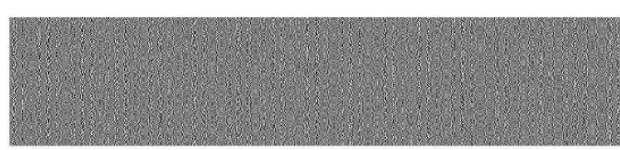

Fig. 4. Share 1 kept by customer.

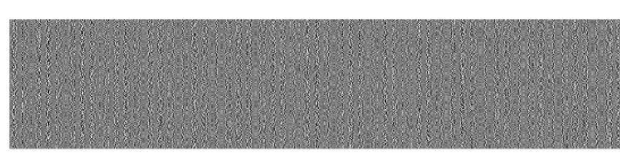

Fig. 5. Share 2 kept by Bank.

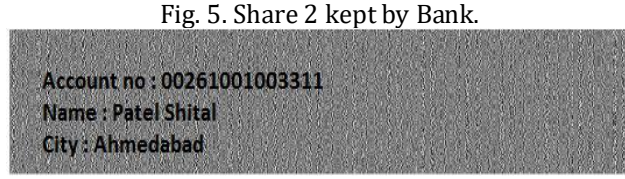

Fig.6 overlapping of share 1 and share 2.

Figure.7 represent steps that needed in proposed system.

In proposed method first customer open account in bank after bank will generated private key and that key will divided into two shares. One share given to customer and second share keep bank in its database. When customer do online shopping he/she select item and add to cart then last they perform epayment. Customer send his/her personal information to Merchant and merchant will send that personal information to bank. Bank have overlapping share1 and share2 and get personal information and bank verify that information then finally payment has processing.

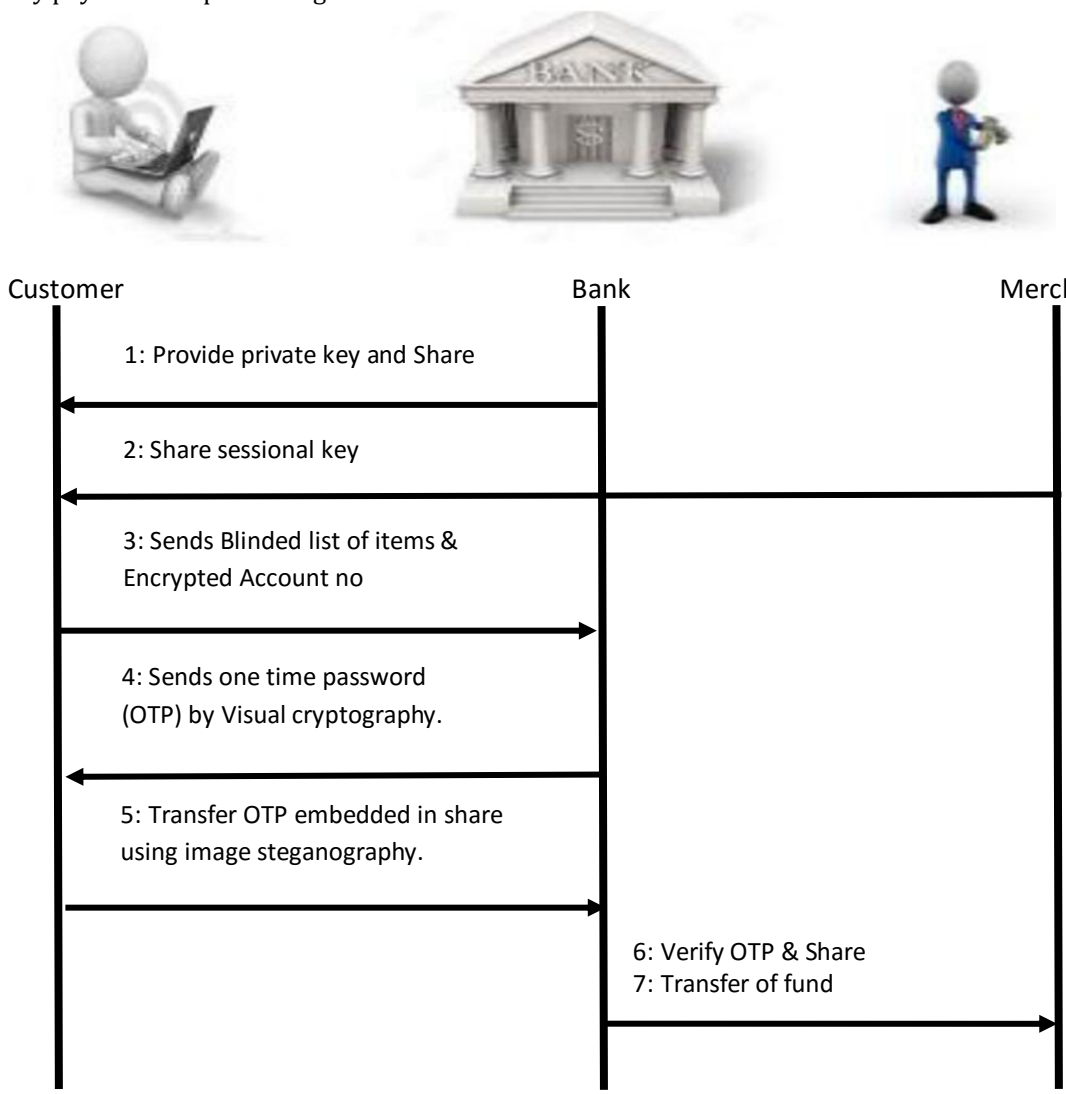

Fig.7 Steps in Proposed System

6. CONCLUSION

With the increasing cashless world, problems of secure transactions get up. Because of that, to help the customer while doing shopping through online retailer's website there is always a possibility of intrusions & personal information escape. During the said process vital information like bank details and customer personal information can be hacked and misused. Proposed method is presented to protect customer from phishing website and avoid misuse of the credentials. Hence the system will provide more secure online transactions by using visual cryptography.

REFERENCES

1. R Bramhechar, D Patil, "A Survey Paper on Online Payment System using Steganography and Visual Cryptography with Hidden Markov Model," IJMTER, pp. 61-66 , July 2015.
2. Arele, Anshu, and Vikas Sejwar. "A Survey on E-Payment using Quantum and Visual Cryptography." International Journal 8, no. 5 (2017).

3. Shital Patel, Dr.V.L.Desai (2016) —Comparative Study and Analysis of Halftone Visual Cryptography via Error Diffusion‖ in IJARCSSE Vol.6, Issue 1.
4. Rajendra, A. B., & Sheshadri, H. S. (2013, August). Visual Cryptography in Internet Voting System. In Innovative Computing Technology (INTECH), 2013 Third International Conference on (pp. 60-64). IEEE.
5. Devi, K. S., Srinivasan, P., Vaishnave, M. P., & Arutperumjothi, G. (2017). Secure E-Pay System Using Steganography and Visual Cryptography. World Academy of Science, Engineering and Technology, International Journal of Mathematical, Computational, Physical, Electrical and Computer Engineering, 11(7), 286-289.
6. W Ashadeep Kaur, Rakesh Kumar, Kamaljeet Kainth, "Review Paper on Image Steganography" ,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 6, June 2016 ISSN: 2277 128X.
7. Sandhya N, Jyoti Rao (March-2014). A Brief Introduction of Visual Cryptography. International Journal of Engineering Research & Technology.
8. Renner, R., & Cirac, J. I. (2009). de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. Physical review letters, 102(11), 110504.
9. R. Navale1 , S. S. Khandagale2, R. A. Malpekar3, Prof. N. K.Chouhan4,"Approach for Secure Online transaction using Visual Cryptography Text Steganography",International Journal of Engineering Research Technology (IJERT) ISSN:2278-0181 Vol. 4 Issue 03, March-2015 894.
10. Roy, S., & Venkateswaran, P. (2014, March). Online payment system using steganography and visual cryptography. In Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students' Conference on (pp. 1-5). IEEE.
11. Kumar, B., Brahme, S., Suman, S., Phatak, K., & Pawar, A. M. (2017). ONLINE SECURE PAYMENT SYSTEM USING CAPTCHA AND VISUAL CRYPTOGRAPHY. International Education and Research Journal, 3(1).