Secured Data Transmission for Online payment System Using Steganography and Visual Cryptography

Harsha Rohida[1], Sonal Raghuvanshi[2], Sujit Lende[3]
[1, 2, 3] Department of Computer Engineering
[1, 2, 3] JSPM's ICOER

Abstract- *This paper presents a new approach for providing limited information only at is necessary for fund transfer during online shopping thereby safeguarding customer data and increasing customer confidence and preventing identity theft. Nowadays high-speed prosperity in E-Commerce market has been witnessed in recent time throughout the world. With ever increasing popularity of online shopping, Debit or Credit card fraud and personal information security are major concerns for customers, merchants and banks and The main motive of this project is to provide high level security in E-Commerce applications and online shopping. This project minimizes detailed information sharing between consumer and online merchant but enable successful fund transfer thereby safeguarding consumer information and preventing misuse of information at merchant's side. This is achieved by the introduction of Central Certified Authority (CA) and combined application of Steganography, Visual Cryptography and Digital Signature for this purpose.*

Keywords- Information sharing, Steganography, Visual Cryptography, Key Generation, Online shopping.

I. INTRODUCTION

Online shopping means to gain the knowledge of product and information related to that product 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 [1]. Identity theft and phishing are the common hazardous of online shopping. Identity theft is the sneak of someone's identity in the form of personal information and misusing 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 [2]. Phishing is an illegitimate mechanism that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Payment Service, Financial and Retail Service are the most focused industrial sectors of phishing attacks [3]Secure Socket Layer (SSL) encryption inhibits 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 and not to sell the information to others.

In this project, a new method is proposed, that uses text based steganography and visual cryptography, which minimizes information sharing between consumer and online merchant but enable successful fund transfer from consumer's account to merchant's account thereby safeguarding consumer information and preventing misuse of information at merchant side. The method proposed is specifically for E-Commerce but can easily be extended for online as well as physical banking. Steganography is the art of hiding of a message within another so that hidden message is indistinguishable. The key concept behind steganography is that message to be transmitted is not detectable to casual eye. Text[4], image[5], video[6], audio[9] are used as a cover media for hiding data in steganography. In text steganography, message can be hidden by shifting word and line, in open spaces, in word sequence. Properties of a sentence such as number of 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 requirement and simpler communication .Visual Cryptography (VC), is a cryptographic technique based on visual secret sharing used for image encryption. The main motive of the proposed system prescribed in this paper 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: BPCS Steganography and Visual Cryptography for safe online shopping and consumer satisfaction.(add related paper reference for steganography n v/s cryptography)[10].

The rest of the paper is organized as follows: Objective, System related works, the proposed steganography method, method of transaction in online shopping, proposed payment method, concludes the paper.

II. OBJECTIVES

The main aim of the project is to design a feasible and secure algorithm which combines the use of both steganography and cryptography with the goals of improving security, reliability, and efficiency for secret message.

III. RELATED WORK

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, then next steps is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system. And the brief survey of related work in the area of banking security based on steganography and visual cryptography is presented in this section. A customer authentication system using visual cryptography is presented in [4] but it is specifically designed for physical banking. A signature based authentication system for core banking is proposed in [5] but it also requires physical presence of the customer presenting the share. [6] proposes a combined image based steganography and visual cryptography authentication system for customer authentication in core banking. A message authentication image algorithm is proposed in [7] to protect against e-banking fraud. A biometrics in conjunction with visual cryptography is used as authentication system [8].

IV. EXISTING SYSTEM

The traditional method of online shopping involves customer or end-user selecting items online shopping portal and directing it to the payment gateway. Different payment gateways have different mechanism of storing detailed information of consumer. There have been recent high profile breaches such as in Epsilon, Sony's PlayStation Network and Heartland Payment Systems show that card holders' information is at risk both from outside and inside.

A. TRANSACTION IN ONLINE SHOPPING

In traditional online shopping as shown in Fig. 2 consumer selects items from online shopping portal and then is directed to the payment page. Online merchant may have its own payment system or can take advantage of third party payment systems such as PayPal, pay online system, Web Money and others. In the payment portal consumer submit his or her credit or debit card details such as credit or debit card number, name on the card, expiry date of the card.

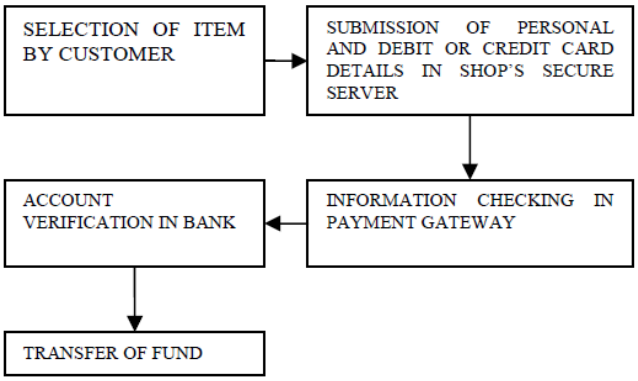

Fig. 2. Transaction in online shopping.

Details of information sought from shopper vary from one payment gateway to another. For example, payment in IRCTC website requires Personal Identification Number (PIN) when paying using debit card whereas shopping in Flipkart or Snapdeal requires Visa or Master secure code. In addition to that merchant may require a Card Verification Value code, CVV (CVV2 for Visa, CVC2 for MasterCard), which is basically an authorizing code in CNP transactions. According to the PCI Data Security Standard [20], merchants are prohibited from storing CVV information or PIN data and if permitted card information such as name, card number and expiration date is stored, certain security standards are required. However recent high profile breaches such as in Epsilon, Sony's PlayStation Network and Heartland Payment Systems show that card holders' information is at risk both from outside and inside. A solution can be forcing merchant to be a PCI complaint but cost to be a PCI complaint is huge and the process is complex and time consuming [21] and it will solve part of the problem. One still has to trust the merchant and its employees not to use card information for their own purposes.

B. DRAWBACK OF EXISTING SYSTEM

In the traditional system mentioned above, customer is not sure whether his PIN No and CVV No is sent to the merchant. One still has to trust the merchant and its employees to use card information for their own motives. This representation doesn't show high level security. In these traditional systems, there is no additional non-functional requirement of phishing mechanism which can be harmful and might lead to employment of social engineering and technical subterfuge. Thus, in the proposed system mentioned later in

this paper would ensure better security and satisfaction of consumer or other transaction stakeholders.

V. PROPOSED SYSTEM

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. Now one share is kept by the customer and the other share is kept in the database of the certified authority. During shopping online, after selection of desired item and adding it to the cart, preferred payment system of the merchant directs the customer to the Certified Authority portal. In the portal, shopper submits its own share and merchant submits its own account details. Now the CA combines its own

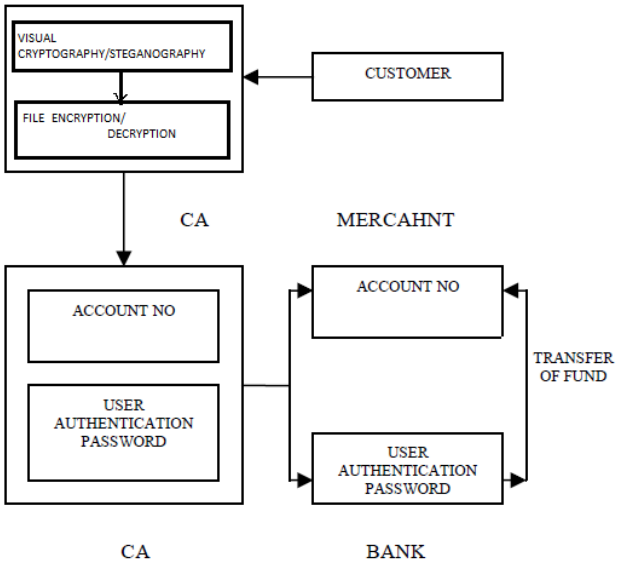

Fig. 3. Proposed payment method

Share with shopper's share and obtains the original image. From CA now, merchant account details, cover text are sent to the bank where customer authentication password is recovered from the cover text. Customer authentication information is sent to the merchant by CA. Upon receiving customer authentication password, bank matches it with its own database and after verifying legitimate customer, transfers fund from the customer account to the submitted merchant account. After receiving the fund, merchant's payment system validates receipt of payment using customer authentication information.

A. Implementation

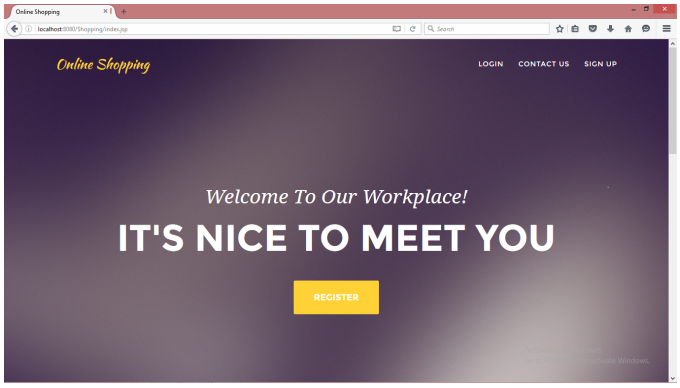

Fig ::It is the first page of Online Shopping System

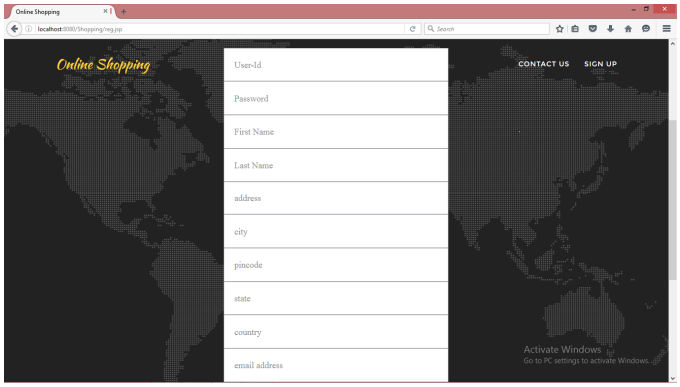

Fig: It's the Registration page of Online Shopping System.

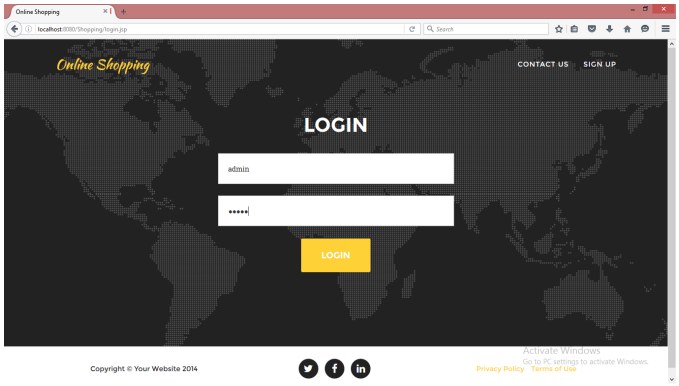

Fig :It is the login page of Online Shopping System

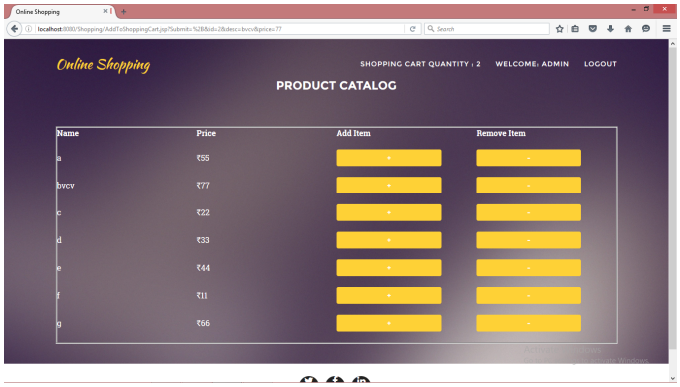

Fig :In these page, various items can be purchased and can be added to the shopping cart

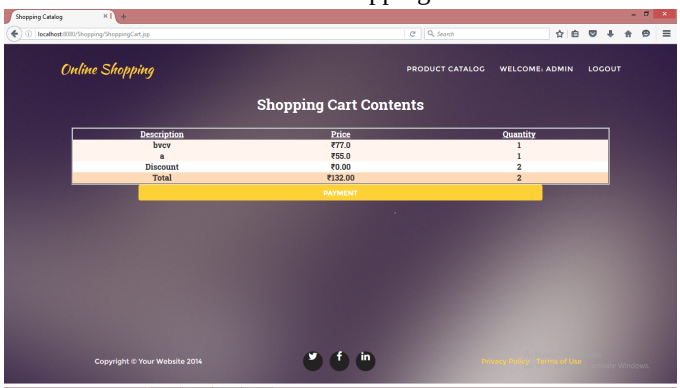

Fig :After purchasing one or more items ,the link gets connected to the payment page

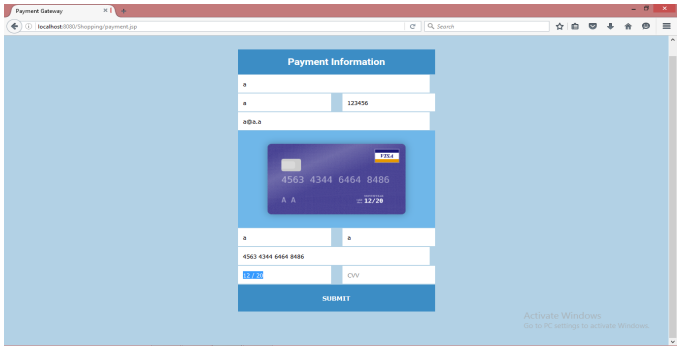

Fig: After entering the payment gateway, the important details are filled by the customer and it is represented in an animated way

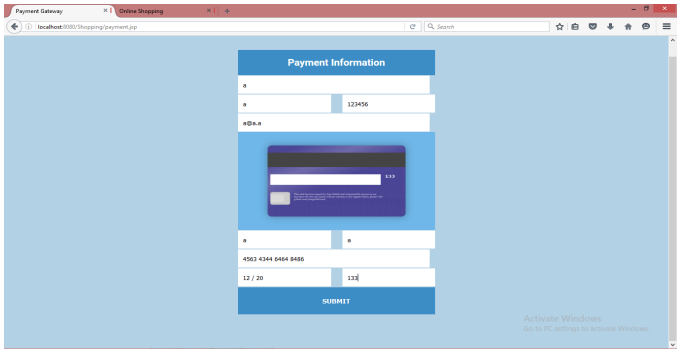

Fig: After entering the payment gateway, the important details are filled by the customer and it is represented in an animated way

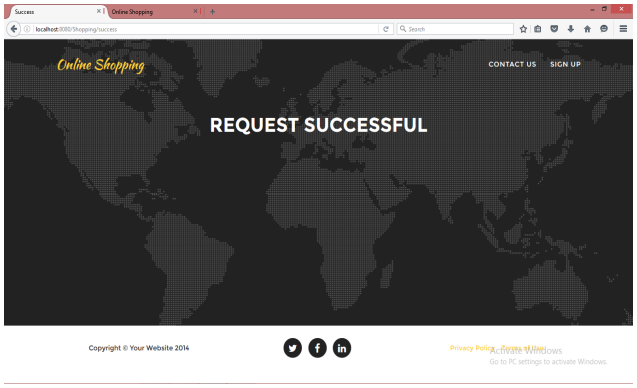

Fig :After filling the information the request is successful

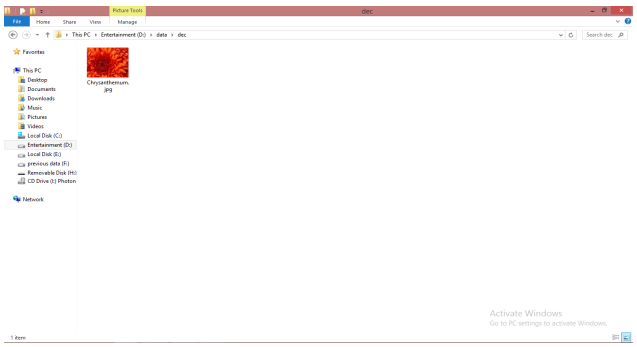

Fig :These is the random image taken for steganography

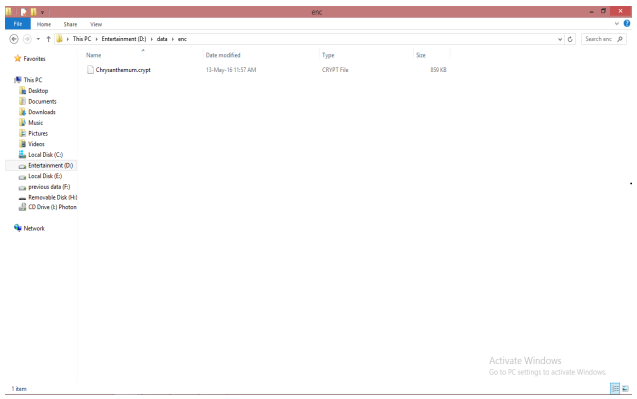

Fig :When payment is done successfully, and encrypted file is automatically generated

VI. ALGORITHMS

A. Key Generation Algorithm

The algorithm can be described in concise steps as follows:

- Setup (1_; n): executed by the data owner to setup an account on an untrusted server. On input a security level parameter 1_ and the number of cipher text classes n (i.e., class index should be an integer bounded by 1 and n), it outputs the public system parameter, which is omitted from the input of the other algorithms for brevity.

- KeyGen: executed by the data owner to randomly generate a public/master-secret key pair (pk; msk).

- Encrypt (pk; i;m): executed by anyone who wants to encrypt data. On input a public-key pk, an index i denoting the cipher text class, and a message m, it outputs a cipher text C.

- Extract (msk; S): executed by the data owner for delegating the decrypting power for a certain set of cipher text classes to a delegatee. On input the master secret key msk and a set S of indices corresponding to different classes, it outputs the aggregate key for set S denoted by KS.

- Decrypt (KS; S; i; C): executed by a delegatee who received an aggregate key KS generated by Extract.
- On input KS, the set S, an index i denoting the cipher text class the cipher text C belongs to, and C, it outputs the decrypted result m if i 2 S.

B. STEGANOGRAPHY

- Text-Based Steganography: It makes use of features of English Language like inflexion, fixed word order and use of periphrases for hiding data rather than using properties of a statement. BPCS Steganography: The information hiding capacity of a true color image is around 50%. A sharpening operation on the dummy image increases the embedding capacity quite a bit. Randomization of the secret data by a compression operation makes the embedded data more intangible. The steganography program for each user is easy. It further protects against eavesdropping on the embedded information. It is most secured technique and provides high security.

VII. 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.
- Can be integrated with any system.
- More secured than alternative.
- It prevents unlawful use of customer information at merchant's side.
- 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.
- Presence of a fourth party, CA, enhances customer's satisfaction and security further as more number of parties are involved in the process.
- Since customer data is distributed over 3 parties, a breach in single database can easily be contented.

VIII. CONCLUSION

In this paper, a payment system for online shopping is proposed by combining text based steganography and visual cryptography [4][5]&[6] that provides customers data privacy and prevents misuse of data at merchant's side. The method is concern only with prevention of identity theft and customer data security. In comparison to other banking application which uses steganography and visual cryptography [4] [5] & [6] 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

[1] Jihui Chen, Xiaoyao Xie, and Fengxuan Jing, "The security of shopping online," Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), vol.9, pp.4693-4696, 2011.

[2] Javelin Strategy & Research, "2013 Identify Fraud Report,"https://www.javelinstrategy.com/brochure/276

[3] Anti-Phishing Working Group (APWG), "Phishing Activity TrendsReport, 2013."

[4] Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography," Proceedings of 2011 World Congress on Information and Communication Technologies, pp. 1181-1186, Mumbai, India, 2011.

[5] 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, pp. 65-72, Chennai, India, 2008.

[6] S.Premkumar, A.E.Narayanan, "New Visual Steganography Scheme forSecure Banking Application," Proceeding of 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 1013 – 1016, Kumaracoil, India, 2012.

[7] K. Thamizhchelvy, G. Geetha, "E-Banking Security: Mitigating OnlineThreats Using Message Authentication Image (MAI) Algorithm,"Proceedings of 2012 International Conference on Computing Sciences (ICCS), pp. 276 – 280, 2012.

[8] 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.

[9] Daniel Gruhl, Anthony Lu, Walter Bender, "Echo Hiding," Proceedings of the First International Workshop on Information Hidding, pp. 293-315, Cambridge, UK, 1996.

[10] J.C. Judge, "Steganography: Past, Present, Future," SANS Institute, November 30, 2001.