Secured E-Payment System Using Image Steganography and Visual Cryptography

Mahsuna Abdul Sathar #1, Nimya #2, Shana #3, Vipin Goutham P #4, Geethu Bastian #5

#Students, #Asst. Professor in Computer Science and Engineering
Dept. of Computer Science and Engineering, IESCE, University of Calicut

Abstract— E-commerce (Electronic Commerce) emerged in the early 1990's and its use has increased at a rapid rate. The E-commerce has lot of advantages and disadvantages. Nowadays the main issue faced by the e-commerce is security, integrity on data and systems. Some examples of E-commerce issues are debit or credit card fraud and misuse of personal information. In this paper we are proposing a combined application of steganography and visual cryptography for creating a convenient, safe and pleasant shopping environment for consumers which offer a more secured and easiest payment option.

Keywords— Steganography, Visual Cryptography, Integrity, E-commerce, Security, Wavelet technique.

I. INTRODUCTION

E-commerce is the process by which business and consumers buy and sell goods and services through an electronic medium. E-commerce emerged in the early 1990's and its use has increased at a rapid rate. As per the growth of technology, the issues faced by the e-commerce also increased. Nowadays the main issue faced by the e-commerce is security and integrity on data and system. The consumers need to be confident and trust the provider of payment method. Some internet criminals are there who trick you into signing up and disclosing your private information by creating phishing or fraudulent websites. Customers need security all the time. In addition to it, protection of data is also essential. In recent years, cyber crimes have attracted increasing attention and in 2013, reports of stolen and leaked password have made big news. They include online credit card fraud, phishing scams and identity theft, and are increasingly common during the holiday season when online shopping drastically increases. In this paper, a new method is proposed for the security of e-payment system. This method consist of image based steganography and visual cryptography. The modern secure image steganography presents a task of transferring the embedded information to the destination without being detected by the attacker. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. Here the text is used as input because the image size is very much greater than the text. So it takes too much time for encryption and decryption. Also the decrypted image with small distortion will be accepted but in the text encryption it accepts only the decrypted text which is equal to the original text. This method allows successful fund transfer with minimal information sharing between consumer and online merchant. The proposed method is used specifically for e-commerce. But it can be extended for online as well as physical banking.

II. STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

Visual Cryptography is an encryption method used to hide information in images in such a way that it can be decrypted only when if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. Visual Cryptography uses two transparent images. It is used to encrypt the secret message that is being sent. Cryptography actually alters the message content and converts into an unreadable form. For that it uses some mathematical algorithms. The cryptographic algorithms use secret keys for encrypting as well as decrypting the data.

The word steganography is derived from the Greek words stegos and grafia which defining it as covered writing. Steganography is the science of secret communication. It is the method of encoding or embedding secret information in a manner such that the existence of the information is invisible. The information which is to be concealed is called Payload and the media where payload has to be hidden is termed as Carrier File. The medium in which the information is hidden is called the Stego-medium. Stego-key is used for hiding or encoding process to restrict detection or extraction of the embedded data. Image steganography the information is hidden exclusively in images.

III. LITERATURE SURVEY

The proposed method in paper [1] describes a new method for securing the online payment system using visual cryptography and text based steganography. The proposed text based steganography is based on Vedic Numeric Code which uses characters of English language. In Vedic numeric code, coding is based on tongue position. For assigning numbers to the letters in English alphabet the frequency of letters in English vocabulary is used. No separate importance is given to the vowels. Each letter is assigned by a number between 0-15. There are 3 users in the proposed payment method, customer, online merchant and certified authority(C A). The customer is provided by a unique authentication password related to the bank which is encrypted using text based steganography and visual cryptography. And one share obtained by this process is kept in CA’s database and other by the
customer. During online shopping the online merchant directs the customer to the certified authority portal. In this portal the customer submits his share and the merchant submit his account details. Then the CA combines the customer submitted share with its own share and obtains the original image. The CA forwards the cover text and the merchant bank details to the bank where the authentication password is recovered from the cover text. The CA then sent the customer authentication information to the merchant. When the bank receives the authentication password it will compared with the bank database and verify. If the verification is successful the fund is transferred from the customer account to the merchant account.

The paper [2] describes the construction of a secure banking certified authority. It introduces different schemes to safe the account: the 2 out of 3 scheme, 3 out of 3 scheme and key-share scheme. The 2 out of 3 scheme is very useful for joint account. Because out of 3 shares one share is stored in bank database and other 2 shares are kept by the applicants. To retrieve the money two applicants must be provide their own shares at a time. Otherwise the transaction will not proceed. In the 3 out of 3 scheme, the 2 shares are kept by applicants individually and one share is kept by two applicants together. So 3 out of 3 scheme is more secure. The key-share schemes introduce a key from the signatures of the applicants and makes two images independently and make the transactions individually. During transaction, overlap the scanned input share and store in the bank database. Then it will compare with the original image, if they are same transaction will done, otherwise it will not proceed. For this purpose, the paper makes four steps: Pre-processing, creation of shares, stacking, post-processing. The technique used to make the scanned image as clear and high intensity image is called pre-processing. The intensity levels of data and background are separated by using its assigned threshold value. Then the shares are created. For that the image is considered as a collection of black and white pixels. Then one share will kept by the bank database and other by the user. During transaction, stack these shares. Stacking is a process of decoding the shares or overlapping the shares. After stacking the comparison of overlapped image with the original image will take place in post-processing stage by using the correlation authentication technique. The transaction will done successfully when the two images are same. So here the proposed system provides the secure payment and the secure internet application.

The paper [3] introduces two new methods for securely transmitting a cognitive content, where in cryptography and steganography are combined to encrypt the data. One of the methods uses S-DES algorithm for securing image by converting it into a cipher text and then using steganography, conceal this text in another image. Another method directly encrypts the image by S-DES algorithm using a key image and then applying the stegnographic method. These two methods prevent the possibilities of steganalysis. In the first method that is image to text encryption, the three RGB colour intensity matrices of the image are converted to cipher text by S-DES encryption using a secret key. But in the second method i.e. image steganography the three matrices are converted to an encrypted image by using a secret image instead of converting it into cipher text.

Paper [4] proposes a new method for implementing visual cryptography on colour images using the wavelet theory. The traditional visual cryptography is only applicable for monochrome images and black and white images. The wavelet technique is used to convert the colour image into grey image. And then the halftone technique is used to convert this grey image into halftone image (single inked image). There are several techniques in the digital half toning. In this paper Floyd Error-Diffusion Filter method is used. Then the VCS model is applied on this halftone image. The share obtained by applying VCS is distributed over the participants and the decryption of the image is done by just stacking the shares.

In paper [5] a new method, Integrated Embedded Visual Cryptography is proposed in which a set of participants can recover the secret image without any cryptographic knowledge. This method is implemented by embedding random shares into meaningful covering share. The Integrated Embedded Visual Cryptography mainly consists of four faces. In the first face ‘n’ shares is generated from a secret image. Here the user must notify the no. of shares as well as the location of secret image. 2- Adding a meaningful covering image into the ‘n’ shares by providing location and name of the covering share. In the 3rd face the covering image is embedded by the VCS. Here the user must provide the name of the creating embedded share and the location of the VCS shares. In the 4th face the secret image can be reconstructed by stacking the shares.

IV. TRADITIONAL ONLINE PAYMENT SYSTEM

In traditional online shopping the consumer selects an item from the shopping site and proceeds to checkout. For that he will be directed to the payment portal. In the payment portal the consumer need to submit his or her personal information like credit card or debit card details such as card number, card holder name, type, card expiry date etc. The online shopping site may have its own payment portal or it take advantage of third party systems. So the information provided to the shopping site may be misused by the online merchant or by some third party.

V. PROPOSED SYSTEM

In the proposed system the security of online payment is achieved by introduction of central Certified Authority and combination of steganography and visual cryptography. There are mainly three users;
customer, merchant and bank. CA (certified authority) is introduced as the part of bank. When a user starts a bank account, he is provided with a user code which is in an encrypted form. In the proposed method the customer’s unique secret code will be converted into image using text to image conversion code. And also using the Vedic numeric code [1] a random number will be generated. Then by applying image steganography on it an encrypted image is generated from the combination of random numbers and image. Now a snapshot of this encrypted image is taken. From the snapshot, two shares are generated using visual cryptography. Now one share is kept in CA’s database and other is kept by the user. During online shopping the customer selects an item and adds into the cart. At the time of payment the customer just upload the share at CA’s portal and the merchant upload the account details. CA compares the uploaded share with its own share. If the two share matches, the fund is successfully transferred from the customer’s account to the merchants account, and a notification message is sent to the customer’s phone.

VI. CONCLUSION

In this paper a secured payment system for E-commerce is proposed by combining image steganography and visual cryptography. This method is concerned with the security and integrity of data and system in E-commerce. I.e. the proposed method provides a solution to avoid the misuse of data at merchant side, debit or credit card fraud etc. This method can be implemented in online shopping as well as in physical banking.

ACKNOWLEDGEMENT

It is our privilege to express our sincere gratitude to Dr. Brilly Sangeetha, Professor & Head of Dept. Computer Science Engineering, IESCE, for her constant support, encouragement and valuable suggestions throughout the work. We would also like to thank our guide Mrs. Geethu Bastian, Asst. professor in Computer Science Engineering, IESCE, for her guidance and support.

REFERENCES