Secure Communication in Online Payment
Reshma Rajendran¹, Amrutha V. Nair²
M.Tech Student¹, Assistant Professor²
Department of Electronics and Communication Engineering
Sree Buddha College of Engineering, Elavumthitta, Kerala, India

Abstract:
E-Commerce has witnessed a gigantic growth nowadays throughout the world. Electronic payment systems let the government, businesses and financial institutions to offer their customers with wide variety of payment options. In the case of CNP debit or credit card fraud and personal information security are the major issues of online shopping. If the website is insecure, the risk on submitting one’s banking information increases. The hackers are able to steal one’s identity and clean out the bank accounts. A new approach is presented based on providing limited but necessary information necessary for fund transfer. The proposed method involves the combined application of steganography, visual cryptography and LSB encryption. The method uses text as well as image steganography, the method of visual cryptography convert the cover message into meaningless images which then embedded into a cover image using LSB encryption, so that it can be transmitted through an unreliable communication channel.

Keywords: E-Commerce, Steganography, Visual Cryptography, CA, Phishing

1. INTRODUCTION

E-Commerce is defined as trading or facilitating trading of products or services using electronic medium. There are different categories of E-Commerce: i) B2B-Companies doing business with each other. ii) B2C-Business to general public, using shopping cart software. iii) C2B-Customer posts a project with a set budget online and companies bid on the project. and iv) C2C-Individuals can buy and sell their goods. Online shopping belongs to the category of B2C and C2C. It involves online transfer of funds. The major problems associated with online fund transfer are:

- Phishing
- Identity Theft

Phishing attack is done by sending a fake mail tends the user to open an attachment or click on a link. Once the user gives up any sensitive information, it can be used to breach your employers system or compromise you identity. Identity theft is the purpose use of someone else identity. The solution is to provide only constrained information during online payment. New encryption method is proposed, aimed to increase the customer confidence by safeguarding customer information to prevent identity theft.

It involves the combined application of steganography, visual cryptography and LSB encryption. The method uses text as well as image steganography, the method of visual cryptography convert the cover message into meaningless images which then embedded into a cover image using LSB encryption, so that it can be transmitted through an unreliable communication channel.

In section 2 we describe transaction in online shopping and in section 3 we present the existing transaction method. In section 4 included introductions to steganography and visual cryptography. In section 5 we describe LSB encryption. In section 6 we describe proposed algorithm.

In section 7 we describe our experimental results. In section 8 we present conclusions.

2. TRANSACTION IN ONLINE SHOPPING

In online shopping the customer picks items from the online shopping portal and gets directed to the payment page. The merchant may have own payment system or may take the service of a third party. In the payment portal, the customer submit the debit card details such as card number, cardholder name, Card Verification Value Code and the card expiry. Though, an OTP is involved, the card holder information is at risk both from inside and outside, it’s clear from the recent high profile breaches such as in Epsilon.

Figure 1. Transaction in Online Shopping

In online shopping the customer picks items from the online shopping portal and gets directed to the payment page. The merchant may have own payment system or may take the service of a third party. In the payment portal, the customer submit the debit card details such as card number, cardholder name, Card Verification Value Code and the card expiry. Though, an OTP is involved, the card holder information is at risk both from inside and outside, it’s clear from the recent high profile breaches such as in Epsilon.

3. EXISTING METHOD

In the existing method it involves a central certified authority (CA). The information submitted by the customer to the online merchant is minimum and is only sufficient to verify that the payment is made. The information received by the merchant is in the form of account number.
The customer unique password related to the bank is encrypted using text based steganography. The encrypted information is merged with the cover text and a snapshot is taken. From the snapshot image, two shares are generated one of the share is stored in CA database, the other is provided to the customer. During online shopping the payment portal direct the customer to the CA. CA retrieve the encrypted information, by combining the shares. From CA, merchant account number and user authentication password encrypted by cover text send to the bank. Upon receiving the information bank matches it with its own database, after verifying the customer is legitimate, transfers the fund.

4. STEGANOGRAPHY & VISUAL CRYPTOGRAPHY

Steganography is the art of hiding a message within another so that the hidden message is indistinguishable [1]. The key idea is the message become undetectable to casual eye. It can be used in conjunction with visual cryptography. The cover media in steganography can be text, image, audio or audio for hiding data. The advantages of text steganography are its smaller memory requirement and simpler communication. Steganography is difficult to detect, if not impossible, to reveal. A cryptographic technique based on visual secret sharing is defined as visual cryptography. A secret image is encrypted in shares (meaningless images) that are distributed over the unreliable communication medium. The secret can only be retrieved when sufficient number of shares is combined. The interesting feature of visual cryptography is that it is perfectly secure and a very simple mechanism for decoding the secrets. One of the disadvantage is the decryption process is lossy. Contrast is important for visual cryptography, because the clarity of the recovered secret is determined by human visual system.

5. LSB ENCRYPTION

One of the main techniques in spatial domain image steganography is Least Significant Bit Encryption. The LSB based steganography method embeds the secret in the LSB pixel values of the cover image. It is based on the fact that the level of precision in common image formats is very much greater than that perceivable by the average human vision. Therefore, an image altered with slight variations in its color will be indistinguishable by a human being. The share1 and share2 are embedded into the cover image by choosing the image plane, where it can be embedded. The plane is chosen by taking the average of pixel values of a particular position and the pixel value of a plane which is greater, is selected as LSB encryption pixel.

6. PROPOSED ALGORITHM

6.1 Bank Server
- Enter the User Authentication Password.
- Generate the encoded text (text steganography).
- Load the coded text into the Visual Cryptographic Module.
- Generate two shares (Visual Cryptography).
- Select the cover image into which the shares are to be embedded.
- LSB Encryption.
- Two Stego shares are generated (for CA as well as the customer).

6.2 Central Authority
- When transaction phase initiated the shares are retrieved from the stego shares.
- Shares are then combined to generate the coded text.
- Finally the coded text sent by CA is decoded by the bank server.
- Thus Customer authentication Password is retrieved.

7. EXPERIMENTAL RESULTS
Figure 5. Combining the Shares at CA

8. CONCLUSION

A payment system for online shopping is proposed. It is based on the combined use of steganography, visual cryptography and LSB encryption. The method is concerned with prevention of identity theft and aimed at customer data security. The result shows that the quality of cover image is retained up to 90% of the original cover image. Unless the algorithm is known to the intruder the, the decryption is highly impossible.

9. ACKNOWLEDGEMENT

I would like to express profound gratitude to our Head of the Department, Prof. Cherian Schariah, for his encouragement and for providing all facilities for my work. I express my highest regard and sincere thanks to my guide, Asst. Prof. Ms. Amrutha V Nair, who provided the necessary guidance and serious advice for my work.

10. REFERENCES


AUTHOR PROFILE

Reshma Rajendran received B-Tech degree in Electronics and Communication Engineering from M.G University, Kerala at Sree Buddha college of Engineering in 2014. And now she is pursuing her M-Tech degree in Communication Engineering under APJ Abdul Kalam Technological University in Sree Buddha college of Engineering. Amrutha V Nair is working as Assistant Professor in department of Electronics and Communication, Sree Buddha college of Engineering, Elavumthitta, Pathanamthitta.