Secure Online Payment System Using Stegnography and Visual Cryptography

Shubham khairnar[1],Ramesh Solanki[2],

Vivekanand Education Society.

Abstract:

There rapid growth in E-Commerce market is seen 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 specifically in the case of CNP (Card Not Present). This paper presents a comparison between new approaches for providing limited information only that is necessary for fund transfer during online shopping thereby safeguarding customer data and increasing customer confidence and preventing identity theft. The method uses combined application of steganography and visual cryptography for this purpose.

Keywords: Information security, Steganography, Visual Cryptography, Online shopping, Image Security

Introduction:

Cryptography involves creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data.[1]

Information security uses cryptography on several levels. The information cannot be read with out a key to decrypt it. The information maintains its integrity during transit and while being stored. Cryptography also aids in nonrepudiation. This means that the sender and the delivery of a message can be verified.

Cryptography is also known as cryptology.

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images or layers are required to reveal the information.

The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

Steganography is data hidden within data. Steganography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data. Steganography techniques can be applied to images, a video file or an audio file. Typically, however, steganography is written in characters including hash marking, but its usage within images is also common. At any rate, steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.

Various methods in online payment using visual cryptography and stegnography:

1) **The method used in this is Algorithm Encryption Standard(AES)**

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits.[3]

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, abreach in single database can easily be contented.

2) **Ceasar cipher** is a new and simplest technique which is used for encrypting and decrypting plaintext. In ceasar cipher technique, it substitutes letters in the plaintext by shifting a certain number of places up or down the alphabet. For example, with a left shift of 4, E would be replaced by A, F would become B, and so on. [5]

Plain text: abcdefghijklmnopqrstuvwxyz

Cipher text: wxyzabcdefghijklmnopqrstuv

Formula for Encryption in Caesar cipher,

$En(x) = (x+n) \bmod 26$

Where,

x is the letter on which encryption will be done ,

n is the key by which encryption will be done, and

E is the encryption function.

Formula for Decryption in Caesar cipher,

$Dn(x) = (x-n) \bmod 26$

Where,

x is the letter on which decryption will be done ,

n is the key by which decryption will be done, and

D is the decryption function.

The result should be in between 0...25. i.e., if x+n or x-n

are not in the range 0...25, we have to subtract or add 26.

Formula for steganographic process,

Stegano_medium = cover_medium + hidden_data.

Where,

Cover_medium is the medium which is used to hide the data,

Hidden_data is the data which will be hidden,

Stegano_medium is the resultant medium of Steganography.

Its methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography

It prevents password and other confidential information from the phishing websites.

For phishing detection and prevention, we are proposing a new methodology to detect the phishing website.

3) **Encapsulation of Image Inside a Cover Image Using LSB Algorithm in a Random Fashion**

The image to be used as a cover image is obtained. In the next stage, the secret image is obtained. It determines the message type and uses the seed key to randomly select pixel

locations to encode the message within.[4] The method determines the dimension of the cover image and multiplies the dimension together to provide the number of available pixels. With the help of same random key value permutation is performed randomly to a list that includes values from 1 to the total pixel values available in a predictable and repeatable manner. Then it ensures the prevention of overwriting of message values in the cover image and can recover the secret message during the decoding stage. After that the secret message is embedded inside the cover image. The method used in this is more secure because the message is encoded across the entire image instead of left portion of the image.

4) **Stegnography and Visual Cryptography Algorithm:**

Steganography and visual Cryptography are the two methods that are used in this project. [6] The steganography technique is used to hide the OTP (generated by bank server) in the QR code. The visual Cryptography is applied on the QR Code to create the two shares/images of it. Consider the QR code generated from the OTP by steganography technique .In this QR code each pixel have 0 or 1 values of image. We are creating the two shares/images of OTP. For this we using the random matrix of 2-Dimensional.Visual Cryptography uses two transparent images. One image contain random pixels/arrays and the other image contain the secret information or Pixels/arrays. It is impossible to retrieve the secret information from one of the images. Now while creating the shares we need to do 'XORing' and while combining the shares into one we need to do 'ANDing'. firstly 1st pixel of QR code image (i.e. 0/1 value) XOR with the random generated arrays of 2-Dimensional that is (a) in Random Pixels/arrays with all the pixels/values in that arrays then new matrix is generated with that is (a') in Secret Pixels/array. If we ANDing of 1st pixel of (a) and 1st pixel of (a') we can get the original pixel in the QR code. We can retrieve the original pixels of the QR code. This implies that generated images/arrays are the correct keys. Finally all the arrays of 2*2 matrix in the Random pixels and Secret pixels are collected and merge separately in order to get the complete share 1 and share 2. The share 1 is in random array and which is sent to the merchant server (in request and response form). The share 2 is in Secret arrays and which is sent to be Client by mail.

The proposed system provides two ways authencation.
It also prevents phishing.
It uses visual cryptography to create two shares of OTP to make system more secure.

The system prevents identity theft.
It also provides security to the user personal data

Conclusion:

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. These method is related only with prevention of identity theft and customer data security. In comparison to other banking application which uses steganography and visual cryptography 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]https://www.techopedia.com/definition/1770/cryptography
[2]https://www.techopedia.com/definition/1770/stegnography
[3] Secure Online Payment System Using
Stegnography and Visual Cryptography
[4] Secure E-Pay System Using Stegnography and Visual Cryptography
[5] Secured Transaction System Using Steganography and Visual Cryptography
[6]
Online Payment System using Steganography and Visual Cryptography