International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 06 | June-2018 www.irjet.net p-ISSN: 2395-0072

# Secure Online Payment System Using Steganography and Visual Cryptography

**Sangita Yadav[1], Priyanka Parui[2], Dr.Murlidhar Dhanawade[3]**

[1,2] *Student in Dept. of MCA,NCRD's Sterling Institute of Management Studies,Navi Mumbai,Maharashtra,India*
[3] *Professor Dept. of MCA,NCRD's Sterling Institute of Management Studies,Navi Mumbai,Maharashtra,India*

---

**Abstract -** *There rapid growth in E-Commerce market is seen in recent time throughout the world. In increase of shopping on online portals, Credit or Debit card fraud and personal data security are bigger involvement for merchants, banks and customers specifically in the case of card not present. This paper presents various ways for providing limited data only that is necessary for money transfer during online shopping , thereby assuring customer information and preventing identity theft and increasing customer confidence. The technique used in this is the combined application of steganography and visual cryptography.*

***Key Words***: **Information security[1], Steganography[2], Visual Cryptography[3], Online shopping[4], Image Security[5]**

## 1. INTRODUCTION

Cryptography is a part of creating written or generated codes that allow information to be kept secret. Cryptography changes the data which is hard to read for an unauthorized user, acknowledge it to be transfer without approved entities decoding it back into a format which is easy to read thus the information remain unchanged[1].

Information security uses cryptography on various levels. The information or data cannot be read without a key to decrypt it. The data which is stored it maintains its integrity during transferring and while being stored. Non repudiation in cryptography is basic factor and it also supports them. It means that both sender's and receiver's delivery of message are being verified. Cryptography is also known as cryptology.

The special encryption technique which is Visual Cryptography is used 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 not possible to fetch secret data from either of the images. Two transparent images are essential to maintain the data, the easy way to implement Visual Cryptography is to print both layers onto a transparent sheet.

Steganography is data hidden within data. Steganography is an encryption method that can be work with the cryptography as an extra-secure technique where it protects customer's data.
This method can be used to work with videos, an audio file or images. Basically steganography is however written in characters including hash marking and its within images is also common. At any proportion, steganography protects from pirating copyrighted materials as well as support in unauthorized viewing.

### 1.1 Various methods in online payment using visual cryptography and steganography:

#### 1.1.1 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 consist of list of linked operations, some of which involve substitution of inputs by particular outputs (substitutions) and others include shuffling of bits everywhere (permutation).

Impressively, AES carry out all its computation on bytes rather than bits [3].

Suggested method minimizes customer information sent to the online merchant. So in case of a barrier in merchant's database, customer's database doesn't get changed. It also provides unauthorized use of customer data at merchant's side.

In existence of a fourth party, CA improve customer's fulfilment and security further as more number of parties are included in the process.

Method of steganography assure that the CA does not know customer authentication password thus protect customer privacy.

Cover text can be sent in the form of email from CA to bank to neglect increasing doubt.

Since customer information is shared among 3 parties, a barrier in single database can be easily satisfied.

#### 1.1.2 Ceasar cipher

It 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) mod 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) mod 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.

### 1.1.3 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.

### 1.1.4 Steganography and Visual Cryptography Algorithm:

Steganography and visual Cryptography are the two methods that are used in this project.

The steganography technique is used to hide the OTP (generated by bank server) in the QR code. The visual Cryptography is tested on the QR Code to generate 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 generating 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 data or Pixels/arrays. It is not possible to fetch the secret data from one of the images. Now while generating 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 combined 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 authentication.

It also prevents phishing.

It needs visual cryptography to create two shares of OTP to protect system.

The system prevents identity theft.

It also gives security to the user personal data.

## 3. CONCLUSION

By combination of text based steganography and visual cryptography that implement customer data privacy and avoid misuse of data at merchant's side. A payment system for online shopping is planned. These method is related only with prevention of identity theft and customer data security. In contrast to other banking application that uses steganography and visual cryptography are basically tested for physical banking, the proposed technique can be tested for E-Commerce with focus area on payment during physical banking

## REFERENCES

[1] https://www.techopedia.com/definition/1770/cryptography

[2] https://www.techopedia.com/definition/1770/stegnography

[3] Aarti Ramdas Gavali ,"Secure Online Payment System Using Steganography and Visual Cryptography", Volume 6, ISSN 2321 3361

[4] Swati Akolkar,Secure E-Pay System Using Steganography and Visual Cryptography,Volume 3, ISSN : 2348 – 6090

[5] Doshi Ruchali, Secured Transaction System Using Steganography and Visual Cryptography ,Volume 6, ISSN 2321 3361

[6] Priyanka More,Online Payment System using Steganography and Visual Cryptography ,Volume 3, ISSN (O): 2349-7084