International Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume III, Issue IV, April- 2016

SECURE E-PAYMENT USING LSD BASED STEGNOGRAPHY AND VISUAL CRYPTORAPHY

SREYA PRAKASH
M-TECH , DEPT OF CSE
Malabar Institute of Technology,
Anjarakandy.
sreyaprakash0@gmail.com

RIJIN I K
HOD, DEPT OF CSE
Malabar Institute of Technology,
Anjarakandy.
rijinik@gmail.com

Abstract— An e-commerce payment system facilitates the acceptance of electronic payment for online transactions. credit cards have become one of the most common forms of payment for e-commerce transactions .The problem of misusing the data related to the debit card and credit card is increasing wide spreadly. This paper presents a new method for providing limited information that is necessary for fund transfer during online shopping. It safeguards customer data and increases customer confidence and also helps preventing identity theft. This is achieved through the combined application of lsb based steganography and visual cryptography for this purpose. A new end–host based anti- phishing algorithm called LinkGuard algorithm is proposed to detect phishing website.
Keywords— Information security; Steganography; Visual Cryptography; Online shopping;

I. INTRODUCTION

Online shopping is the process whereby consumers directly buy goods or services from a seller in real-time, without an intermediary service, over the Internet . It is a form of electronic commerce. Identity theft and phishing are the common dangers of online shopping. Identity theft is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss. Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels. phishing attacks are very common in the 2nd quarter of 2013 and the most targeted industrial sectors are Payment Service, Financial and Retail information can be reconstructed from any single share. Each share is printed in transparencies. The decryption is achieved by stacking the two shares and the secret image can be visualized by naked eye without any complex cryptographic computations.

In text based stegnography[1], In result to hide 4 letter word, 8 words are required excluding the words that are added to provide flexibility in sentence construction. So to hide a large message, this technique requires large no of words and creates a complexity in sentence construction. In this paper, a new method is proposed, that uses lsb based steganography and visual cryptography.

II. STEGANOGRAPHY

The LSB is the lowest significant bit in the byte value of the image pixel. The LSB based image steganography [2]embeds the secret in the least significant bits of pixel values of the cover image (CVR). In conventional LSB technique, which requires eight bytes of pixels to store 1byte of secret data but in proposed LSB technique, just four bytes of pixels are su_cient to hold one message byte. Rest of the bits in the pixels remains the same.

III. VISUAL CRYPTOGRAPHY

Visual cryptography (VC) is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image. Visual cryptography (VC), proposed by Naor and Shamir[3], is a method for protecting image-based secrets that has a computation-free decryption process. In the (2, 2) VC scheme each secret image is divided into two shares such that no information can be reconstructed from any single share. Each share is printed in transparencies. The decryption is achieved by stacking the two shares and the secret image can be visualized by naked eye without any complex cryptographic computations.

IV. RELATED WORK DONE

A short-lived study of related work in the area of banking security based on steganography and visual cryptography is presented in this division. A consumer authentication system using visual cryptography and steganography is presented in but it is precisely designed for physical banking. A signature based authentication system for core banking is proposed in but it also requires physical presence of the consumer presenting the share. proposes a combined image based steganography and visual cryptography authentication system for consumer authentication in core banking. A message authentication image algorithm is proposed in to protect against e-banking fraud. A biometrics in conjunction with visual cryptography is used as authentication system .

International Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume III, Issue IV, April- 2016

V. PROPOSED LSB BASED STEGANOGRAPHY METHOD

The Least Significant Bit (LSB) is one of the main techniques in spatial domain image Steganography.The LSB is the lowest significant bit in the byte value of the image pixel The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in its col-ors will be indistinguishable from the original by a human being, just by looking at it. In conventional LSB technique, which requires eight bytes of pixels to store 1byte of secret data but in proposed LSB technique, just four bytes of pixels are su_cient to hold one message byte. Rest of the bits in the pixels remains the same.

1. Conversion of image to matrix

In the conversion process of image to matrix we convert the input cover image into matrix values which is stored in a text file. Firstly an image is read from computer, the original image is in the form of RGB which is converted into grey image. The grey image is resized to a particular size of 256*256. Each image has intensity values for every pixel, here these intensity values are stored into a text file. Figure 1.1 shows the cover image used. In the figure 1.2, the intensity values of cover image obtained during the conversion of image to matrix is represented.

Figure 1.1 : Cover Image

2. Embedding process

After completion of image to matrix the next step is to embed a message into an image. The image obtained during this process is called as steganoembed image. The message is embedded into the intensity values of image obtained during image to matrix conversion. The intensity values of the embedded image are as shown in the figure 2.1 and stegano image in figure 2.2.

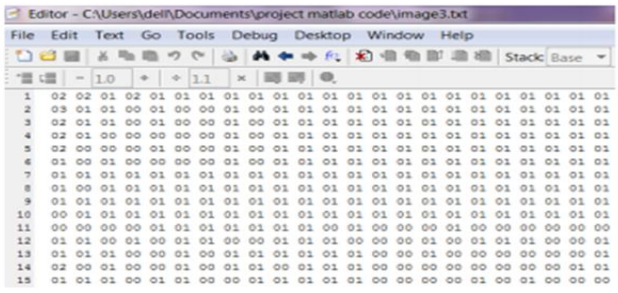

Figure 1.2 : Intensity values of Cover image

Figure 1.3: Secret Image

3. Conversion of matrix to image

In this stage intensity values are converted back to image. The image obtained has message embedded into it. The cover image and the image obtained here have to be identical. Hence the objective of Steganography is satisfied.

4. Extraction process

In this process we extract the message which was embedded during embedding process. At first declare a message byte, here the size of the message is 8 bits. Read a pixel from the array starting from address=0.Extract the LSB and replace the i th bit in the message byte where i =1 to 8 Address=address=1. When i =8, a byte is extracted. Repeat for extracting next byte.

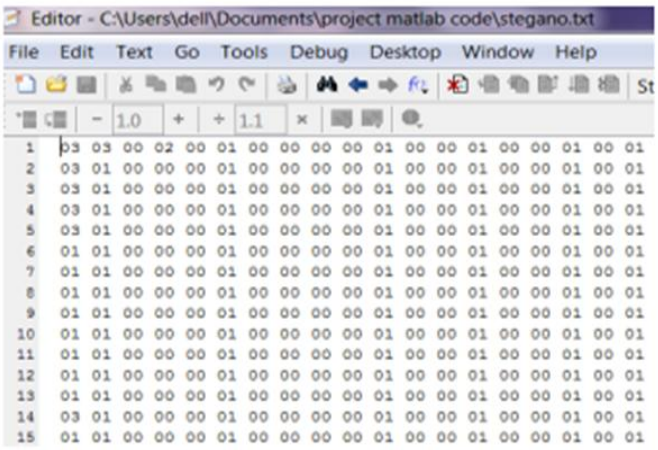

Figure 2.1: Intensity values of Stegano-image

Figure 2.1: Stegano Image

VI. Link Guard Algorithm

Link guard algorithm is used to detect phishing mails. phishing mails are called hyperlinks .A hyperlink has a structure as follows.
<a href=”URI” >Anchor text <a >

where URI (universal resource identifiers) provides the necessary information needed for the user to access the networked resource and Anchor text is the text that will be displayed in users Web browser .The content of the URI will not be displayed in users Web browser .The algorithm is as follows:

```
v link: visual link;
a link: actual link;
v dns: visual DNS name;
a dns: actual DNS name;
sender dns: senders DNS name.
int LinkGuard (v link, a link )
{
v dns = GetDNSName (v link );
a dns = GetDNSName (a link );
 if ( (v dns and a dns are not
 empty ) and (v dns != a dns ) )
 return PHISHING;
 if (a dns is dotted decimal )
 return POSSIBLE PHISHING;
 if (a link or v link is encoded )
{
 v link2 = decode (v link );
a link2 = decode (a link );
 return LinkGuard (v link2, a link2 );
}
if (v dns is NULL )
return AnalyzeDNS (a_link);
 }
 int AnalyzeDNS (actual link)
 {
return PHISHING;
if (actual dns in whitelist)
return NOTPHISHING;


return PatternMatching (actual_link);
 }
int PatternMatching(actual link)
{
 if (sender_dns and actual_dns are different)
 return POSSIBLE PHISHING;
for (each item prev_dns in seed-set)
{
 bv = Similarity(prev_dns,actual-link);
 if (bv == true)
 return POSSIBLE_PHISHING;
 }
 return NO_PHISHING;
}
float Similarity (str, actual link) {
 if (str is part of actual-link)
 return true;
int maxlen = the maximum string lengths of str and actual dns;
int minchange = the minimum number of changes needed to transform str to
actual dns (or vice verse); if (thresh < (maxlen-minchange)/maxlen<l)
 return true
 return false
 }
```

VII. Proposed System

In the proposed method, customer unique authentication password in connection to the bank is hidden inside a cover text using the lsb 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. During shopping online shopper submits its own share in the CA’s portal and merchant submits its own account details. CA browses user’s share and generates the card no which is sent to the bank so as to extract the customer’s PIN (de-steganography). Finally fund will be transferred from the bank to the merchant.

Conclusion

In this paper, I present a payment system for online shopping combining lsb based steganography and visual cryptography that provides customer data privacy and prevents misuse of data at merchants side. The method is concerned only with prevention of identity theft and customer data security. The proposed method can be applied for E-Commerce with focus area on payment during online shopping as well as physical banking. A new end–host based anti-phishing algorithm called LinkGuard algorithm is proposed to detect phishing website.

References :

[1] Sandip Roy and P Venkateswaran. Online payment system using steganography and visual cryptography. In Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students’ Conference on. IEEE, 2014.
[2] Shilpa Gupta, Geeta Gujral, and Neha Aggarwal. Enhanced least significant bit algorithm for image steganography. IJCEM International Journal of Computational Engineering & Management, 15(4):40–42, 2012.
[3] Moni Naor and Adi Shamir. Visual cryptography. In Advances in CryptologyEUROCRYPT’ 94, pages 1–12. Springer, 1995.
[4] Radhika .D. K Champakamala .B.S, Padmini.K. Least significant bit algorithm for image steganography. International Journal of Advanced Computer Technology (IJACT), 2013.