SECURE E-PAY USING STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

1SARITA SWAMY, 2RESHMA GULWANI

1,2Information Technology, Ramrao Adik Institute Of Technology,Nerul,Mumbai
E-mail: 1saritawamy678@gmail.com, 2reshmagulwani@gmail.com

Abstract - There has been a tremendous growth and attraction towards the online shopping in recent time throughout the world. But on the other side we have a major task in hand to protect personal as well as banking information. After the rapid use of online transactions the rise in debit & credit card fraud and stealing the personal information is the real worry for the end users and online retailers. Also banks need to update and upgrade their security and policies to prevent this type of frauds. The intention behind this project is to improve the existing E-Commerce & online shopping retailer's application security. By using this system we can minimize the content shared between the end users and E-Commerce businesses by making sure that the funds will be transferred successfully to the retailers with encapsulating the consumer information so that such information is not misuse by the merchandise. We can achieve the introduction of CA i.e. Central Certificate Authority with application of Steganography and RG - based Visual Cryptography.

Keywords - Online Shopping, Information Security, Steganography, Visual Cryptography.

I. INTRODUCTION

Over the years no of users on internet has exponentially increased, this growth has given a big boost to online shopping. Online shopping is basically a way to check, feel and order the tons of product available for sell by the online retailers. We just need to select the product on the online retailer's website, it will generate the digital purchase order, after this we have to provide the credit or debit card details and the product you have selected will be delivered to you.

Identity theft and phishing are the major pitfall of online shopping. Phishing is an unethical way to steal the end users personal as well as banking data. Some technical professionals are used to hack this data from online retailers so that they can misuse this data. Identity theft is an act of stealing and assuming another person’s identity in order to commit fraud or other crimes like using this data for purchasing or opening new bank account.

To protect the stealing of data between end users and online merchant website we have to use Secure Socket Layer (SSL) encryption , This encryption make sure that the data will be encapsulated and tunneled in such a way that during the transfer it cannot be hacked. Still this data will be available with the retailers, so we have trust the employees of online merchandise for not sharing the data or using this data for their own use. We are proposing a new method for this.

Our technology uses text based steganography and RG-visual cryptography, this will reduce the sharing of important information such as banking and personal information. By using this we can transfer the funds in more secure way and by sharing the minimal personal information.

Fig.1. Online Payment System

1.1 Steganography

Steganography [6] technology is nothing but hiding of one message underneath the other message, by implementing this it is very difficult to distinguish the hidden message. The advantage of this type of message is that it won't be visible. We can use number of formats to hide or cover the data using steganography. Audio, Video, Text and Images are some of the formats which are popularly used. If you take the example of text steganography, there are number of ways to hide the message. By shifting the order of word & line can hide the message, by adding or removing the number of words, number of letters or number of vowels we can hide the message as well. Text steganography is widely used because of its advantage over other formats. By using Text as format the amount of memory required is very less compared to other forms and the way of communication is also simple.
1.2 Visual cryptography

Visual cryptography[15] (VC) is a encryption method where secret image is divided into sufficient number of shares based on bank schemes and then stacking those sufficient number of shares will help in revealing the secret image. This is a method which is used for protecting image based secrets. This method also does not require any computation process for decrypting the image. Suppose in (2,2) VC i.e 2 OUT OF 2 Visual Cryptography scheme Our secret image will be divided into two shares. Original image will only be reconstructed by stacking of this two shares. No information can be rebuilt by any single share. These shares will be printed on transperencies.During decryption this two shares will be stacked and secret image will be envisage by our naked eyes without any complex computation process.

II. LITERATURE SURVEY

Souvik Roya,*, P.Venkateswaranb presents a different approach to the En- glish text based steganography with Indian root In the propose method,Resources of sentences are not used ,rather attributes of English language like use of periphrases ,inflexion and fixed word order are used.This gives us ability to flexibly perform sentence creation but increases computational complexity. [10].

B.Srikanth , G.Padmaja ,Dr. Syed Khasi, Dr. P.V.S.Lakshmi and A.Haritha proposed a method where signature of the applicant will be used as input and this input will be divided into number of shares depending on bank scheme.One share will be kept with the bank and all other shares based on scheme will be given to applicant.During every transaction applicant need to supply his shares.This shares are overlaped with the share present in the bank.and Authentication check is performed using correlation technique.If the correlation coefficient value is higher then authentication is succeed[11].

Souvik Roy and P.Venkateswaran Provided a new approach where limited information need to be shared for fund transfer process while doing online shopping.End users personal data is also prevented from identity theft.They have used steganography and visual cryptography for this purpose [8].

S. R. Navale , S. S. Khandagale , R. A. Malpekar , Prof. N. K. Chouhan uses a text based stegnography and RG- based Visual Cryptography to pro- pose a secure online payment system where a consumers payment information is directly sent to a payment portal and a merchant do not obtain a consumers payment information, not even in encrypted/hashed form[16].

III. COMPARATIVE ANALYSIS

3.1. Comparison

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>NAME OF PAPER</th>
<th>METHOD</th>
<th>ADVANTAGES</th>
<th>DISADVANTAGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A Text based Steganography Technique with an Indian root.</td>
<td>Vedic numeric code.</td>
<td>Flexibility and freedom for sentence creation.</td>
<td>Increases computational complexity.</td>
</tr>
<tr>
<td>2</td>
<td>Secured Bank Authentication using image Processing and Visual Cryptography.</td>
<td>Secured Bank Authentication using Image Processing and Visual Cryptography</td>
<td>This Technique shields the customer information to defend the possible forgery.</td>
<td>Need physical presence of applicant to sign an application form while opening a bank account.</td>
</tr>
<tr>
<td>3</td>
<td>Online Payment System using Steganography and Visual Cryptography.</td>
<td>Vedic numeric code and traditional visual cryptography.</td>
<td>Prevents unlawful use of customers data on merchant side.</td>
<td>Meaningless Shares are generated and transmitted over an untrusted communication channel.</td>
</tr>
</tbody>
</table>
3.2 Analysis.
We are using an Indian root technique which is a text based steganography. A very old and Indian Vedic Numeric code technique is referred to present the text based steganography. In this method English alphabets letters frequency is used with Indian Vedic Numeric Code. In this case we are not giving any special importance to the vowels as well as consonants.

Table 2: Table of letter frequency and number assignment.

<table>
<thead>
<tr>
<th>Letter</th>
<th>Frequency of letter</th>
<th>Number assigned</th>
<th>Letter</th>
<th>Frequency of letter</th>
<th>Number assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>11.2997%</td>
<td>15</td>
<td>M</td>
<td>3.9239%</td>
<td>7</td>
</tr>
<tr>
<td>A</td>
<td>8.4996%</td>
<td>14</td>
<td>N</td>
<td>6.6144%</td>
<td>11</td>
</tr>
<tr>
<td>R</td>
<td>7.1809%</td>
<td>13</td>
<td>S</td>
<td>5.7251%</td>
<td>10</td>
</tr>
<tr>
<td>I</td>
<td>7.5448%</td>
<td>13</td>
<td>L</td>
<td>4.8597%</td>
<td>10</td>
</tr>
<tr>
<td>O</td>
<td>7.1635%</td>
<td>12</td>
<td>C</td>
<td>4.1508%</td>
<td>9</td>
</tr>
<tr>
<td>T</td>
<td>6.9906%</td>
<td>11</td>
<td>U</td>
<td>3.6108%</td>
<td>8</td>
</tr>
<tr>
<td>N</td>
<td>6.6144%</td>
<td>11</td>
<td>D</td>
<td>3.3844%</td>
<td>8</td>
</tr>
<tr>
<td>S</td>
<td>5.7251%</td>
<td>10</td>
<td>F</td>
<td>3.1671%</td>
<td>7</td>
</tr>
</tbody>
</table>

Table 4: Approach for Secure Online transaction using Visual Cryptography and Text Steganography Proposed method.

<table>
<thead>
<tr>
<th>Approach for Secure Online transaction using Visual Cryptography and Text Steganography Proposed method.</th>
<th>Text Steganography using ASCII code and Realized Visual Cryptography</th>
<th>Customer privacy is prevented from CA as well as Merchant. No secret key is used while creating shares</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-Processing</td>
<td>Share 1</td>
<td>Share 2</td>
</tr>
<tr>
<td>Pre Processed Image</td>
<td>Stacking</td>
<td>Post Processed Image</td>
</tr>
<tr>
<td>Sharing</td>
<td>Stacked Image</td>
<td>Original Image</td>
</tr>
</tbody>
</table>

Secured Bank Authentication using Image Processing and Visual Cryptography. In our project, Applicants signature is treated as the input parameter, which is processed and splits into number of share. Now the number of shares will be totally dependent on the scheme which bank follows. Out of all the share one copy of share will be kept by the bank to store in their database for checking and processing other copies will be given to the end user. Every end user has to produce the copy of his share during every transaction he made. Now for checking purpose this share will be overlapped with the share of bank which is present in banks database. After this authentication & authorization will be completed by correlation technique. If the correlation coefficient value is on higher side, that means the authentication is done successfully.

Fig.5. Text Based Steganography Result

Fig.6. Signature Authentication Process

IV. PROPOSED SYSTEM

4.1 Proposed System
Our solution will share the minimum information to the online retailers, as will only verify the payments made by the end user to the banks. In this way the vital information regarding the bank details and personal information can be hide successfully. To achieve this we have introduce CA i.e. Central Certified Authority and merge its application with steganography and visual cryptography. By using this only information that will be available with merchant will be in the form account number related to the debit or credit card. This information will be authorized and authenticated by the customer only. This process in briefly showed in fig. 7. By using our proposed method, with the help of bank end user will generate the authentication password which will be a hidden inside the cover text by steganography method. End users authentication information i.e. his account number is placed above the cover text in the original form. In this way snapshot of both the text is taken. Now one share of the snapshot is kept with the end user while the other share is shared with Central Certified Authority. Now once you done with the shopping and selecting the desired product under cart end user will be directed to CA portal. After this CA will match its own share with the end users share and get the original image. Now CA will forward merchant account number with cover text to the bank where the end users authentication password will be recovered from the text. Once the bank receives the details from the CA it will try to match the details with the available details with the banks. Once bank confirms that the data has been matched it will transfer the funds from End user account to the merchant account. Once the merchant receives the payments it will provide the end user with the receipt. The only issue is CA does not know to which bank the combined share should be forwarded. We can eliminate this by appending 9 digit routing or transit number of bank with the end users bank details.
The proposed system includes 2 techniques:
1. Algorithm for Steganography using ASCII Code

4.1.1 Algorithm for Steganography using ASCII Code

Encoding Steps:
1. Take input from user in the text form.
2. Each letter is represented by its ASCII code.
3. The ASCII code will be represented in 8 bit binary number.
4. This 8 bit number is further divided into two parts 4 bit each.
5. Every part of this number will be assigned with 0 to F hex code. Then further this will be used to select the corresponding suitable words in the table shown below:

Decoding Steps:
1. Now it will take the word of cover message, it will represent that word with suitable number from the table given below.
2. Every number will be assigned a binary number of 4 bits.
3. The combination of these two adjacent 4 bit numbers will create the new 8 bit number.
4. Now, this new 8 bit number will be used to identify the ASCII code.
5. After this process we have obtained a ASCII code.
6. Which will recover the secret message which customer has given to bank.

Results:
1) Secret Password = sarita.
2) Convert it into 8 bit ASCII code : s = 01110011 , a= 01100001 , r = 01110010 , i = 01101001 , t = 01110100 , a = 01100001.
3) 8 bit binary number is then divided into two 4 bits parts. s = 01110011 , a= 01100001 , r = 01110010 , i = 01101001 , t = 01110100 , a = 01100001.
4) Now , 4 bit binary will be in range of 0 to 15 For eg : 0111 = 7 , 0011 = 3 , 0110 = 6 , 0001 = 1 , 0111 = 7 , 0010 = 2, 0110 = 6 , 1001 = 9 , 0111 = 7 ,0100 = 4 , 0110 = 6 , 0001 = 1.
5) Perform word assignment from table.
7 = MY, 3 = DOG, 6 = TO, 1 = DEAR, 7 = MY, 2 = HOW, 6 = TO, 9 = YOU, 7 = MY, 4 = PRINCE, 6 = TO, 1 = DEAR.

6) Encrypted Password = MY DOG TO DEAR MY HOW TO YOU MY PRINCE TO DEAR.

4.1.2 Algorithm for RG-Based Visual Cryptography

Naor and Shamir’s proposed technique has a drawback of multiplying the every share of pixel to 4 times of original pixel. Which leads to increase in size of the pixel as well as the increase in amount of space required to save that pixel as it will occupy 4 times more space. This technique results in more time utilization as it has to encrypt and decrypt the more number of pixels. Also transferring this high memory pixels through network is also time consuming. To rectify this Kafri and Keren came up with new technology which does not multiply the pixels using the random grid. This technique receives the original input image and convert this to number of cipher-grids, cipher-grids does not give any information about the original image. But it comes with the solution as it does not require pixel multiplication. By using this we can save the time for encrypting and decrypting the image by retaining the original size of image. This technique was introduced by Kafri and Keren in 1987. After doing number of tests it was found out that the Kafri and Keren technique has given better output compared to any other similar technique.

Algorithm:
Step 1: Generate R1 as a random grid.
Step 2: for (each pixel R1 [x, y], 1 ≤ x ≤ w and 1 ≤ y ≤ h) do
Step 3: R1[x, y] = randpixel(0, 1)
Step 4: for (each pixel B[x, y], 1 ≤ x ≤ w and 1 ≤ y ≤ h) do
Step 5: if(B[x, y] = 0) R2[x, y] = R1[x, y] else R2[x, y] = R1[x, y].
Step 6: output(R1, R2).

4.1.3 Advantages

1. By using this process if there is security breach at the database level of retailer, we can rest assure that the end users personal or banking information is not affected. This also protect the unethical use of end users personal or banking information at the website of retailer.

2. In addition more security can be achieved by fourth party Central Certifying Authority (CA). This will enable the end user with more secured fund transfer as the number of parties and security level will be increased.

3. We are using Steganography in such a way that even the Central Certifying Authority (CA) will not be able to understand the authentication password of the end user. So by this we provide more security to the end user.

4. The communication between the Central Certifying Authority (CA) and end users bank will be completed with the help of secured mailing service so that this code can be protected from wrong use.

5. There is always a possibility of the database being hacked or compromised since the end user data is forwarded to number of parties.

CONCLUSIONS

Hence we can conclude that, by using the existing method while doing shopping through online retailer’s website there is always a possibility of intrusions & information leakage. During the said process vital information like bank details & end users personal data can be hacked and misused. To
Secure E-Pay using Steganography and Visual Cryptography

... protect the end users data and make the financial transactions more secure we are proposing this system. In which through CA end users payment information will be provided to payment portal rather than sharing it with merchants website. For this approach we need the support of trusted third party know as Central Certified Authority with text steganography and RG-visual cryptography. CA authorized and authenticate the identity of end user by combining share1 and share2 text images before payment is processed. The Combined approach of Text steganography and RG-visual cryptography with CA will ensure end user with information privacy and protect data from being misused.Hence by using this combined approach in our proposed payment system, it has been proved secure and protects customers payment details being hacked by network intruders or attackers.

REFERENCES


Proceedings of WRFER International Conference, 07th May, 2017, Pune, India