A Novel Image Steganography Technique for Secured Online Transaction Using DWT and Visual Cryptography

Anitha Devi M.D
Research Scholar, Sri Siddhartha Academy of Higher Education
Tumakuru, India
anumdssit@gmail.com

K B ShivaKumar
Research Supervisor, Sri Siddhartha Academy of Higher Education
Tumakuru, India
shivakumarkb@sit.edu.in

Abstract: Online payment eco system is the main target especially for cyber frauds. Therefore end to end encryption is very much needed in order to maintain the integrity of secret information related to transactions carried online. With access to payment related sensitive information, which enables lot of money transactions every day, the payment infrastructure is a major target for hackers. The proposed system highlights, an ideal approach for secure online transaction for fund transfer with a unique combination of visual cryptography and Haar based discrete wavelet transform steganography technique. This combination of data hiding technique reduces the amount of information shared between consumer and online merchant needed for successful online transaction along with providing enhanced security to customer’s account details and thereby increasing customer’s confidence preventing “Identity theft” and “Phishing”. To evaluate the effectiveness of proposed algorithm Root mean square error, Peak signal to noise ratio have been used as evaluation parameters.

Keywords: Hacker, Identity theft, online payment system, Phishing, PSNR (Peak signal to noise ratio), RMSE (Root mean square error), Steganography and Visual Cryptography,

1. INTRODUCTION

In this era of cashless transactions, there is a rapid growth seen in E-commerce market during recent days throughout the world. With this growing popularity of online payments, information security is the major concern. With regard to Debit and credit card payments, several parameters are needed to carry out the transaction from beginning to end such as customer details, their payment card details, merchants and their POS (point of scale) payment systems related information. Hence a large amount of electronic data and currency in a digitized form is transferred through the payment system.

The main threat to security of customer’s financial information running via network could be due to either “Phishing” or “Identity theft”. Phishing is a technique to hack customer’s identity and their financial account details. Identity theft is using someone’s identity and misuse of that person’s related information for any transaction. The proposed algorithm is a novel technique with a unique combination of Steganography and Visual cryptography approach providing very limited information needed for successful online transaction and thus enhancing security to sensitive information.

Steganography is a covert communication technique, where secret information is embedded within any multimedia carrier in such a way that there is no scope for suspicion regarding secret information.
within cover media. In the proposed algorithm wavelet based steganography technique is used, in which the information is stored in wavelet coefficients of an image, instead of changing the actual pixel value information in an image. The basic idea is storing sensitive information in least important coefficients of each 4x4 Haar transformed block will not perceptually degrade the quality of image.

Visual cryptography is a popular cryptographic technique, which allows visual information (pictures, text etc) to be encrypted in such a way that decryption becomes a mechanical operation that does not a computer for authentication. Visual cryptography refers to method of sharing a secret among group of participants. Dealer provides a transparency to each one of the n users. Any S of them can see the secret by stacking their transparencies, but any S-1 of them do not gain any information regarding it. Covert image transmission technique has the potentiality of communicating sensitive information via the network securely under the inspection of an adverse censoring authority.

Images are very popular target media used in the field of steganography. In the field of digital image processing many different image file formats exist, most of them for specific applications. For these different images file formats, various steganographic algorithms exist. The existing algorithms have some disadvantages like less embedding capacity, less security and degradation in the quality of retrieved image.

2. Literature Survey

In Literature, a lot many image hiding techniques are available considering the various aspects in image security. Researchers in steganographic domain have come up with variety of schemes. A brief survey of previous related work in the area of secured online transaction is presented in this section.

M. Naor and A. Shamir [1] Proposes a secured encryption technique using visual cryptography. In this proposed algorithm input payload image is split into several shares. Minimum number of shares is required to retrieve the payload information in a lossless fashion. The secret information is retrieved by stacking all shares. The most appreciable feature of this algorithm was to have a computation less retrieval of secret information. Another important feature added in this proposed method was to generate similar looking shares, so that hacker is not doubtful looking at different shares and another additional feature added was to encode multiple pixels at a time.

Jaya, Siddharth Malik [2] et al. provides a comparison study of different existing visual cryptography methods based on various parameters like number of shares original information is split into, quality of retrieved secret information etc. Author has proposed some real time applications wherein visual cryptography technique could be applied enhancing security of secret information.

Chetana Hegde, Manu S et al.[3] has developed a method of encrypting the signature of an authenticated customer and then splitting it into several shares. Number of split shares is dependent on scheme chosen by the corresponding bank. When two different shares are created, one of the shares is kept in bank database and other is maintained at customer end. The customer needs to submit his/her share during transactions. His/her share is combined with share at the bank to retrieve authenticated signature. The evaluation parameter used in this algorithm is correlation factor.

Sowmya Suryadevara, Rohaila Naaz et al. [4] proposes an authentication technique using tongue biometric applying visual cryptography technique. Three dimensional images of tongue is maintained at database in bank. High resolution picture of authenticated customer is maintained in database. These images are initially preprocessed and later it is made more secured by using visual cryptography technique.

Shivendra Katiyar, Kullai Reddy et al. [5] has developed an algorithm, for authentication in a voting system. This algorithm makes use of optical character recognition technique to read the secret information required to authenticate the voter hidden inside a cover image. This secret information could be finger print impression. After authentication the voter will be allowed to vote.
3. Proposed Model

The System implementation starts by taking a snapshot of consumer related payment information. The picture information is hidden inside a carrier image using steganography technique applied to image. Now on a resulting stego image visual cryptography technique is applied to generate two shares. One of the share is maintained at consumer end and other share is kept in the database maintained at the certified authority.

While doing online transaction the customer submits his/her own share and the concerned merchant submits its own account details. Now the certified authority puts its own share with consumer’s share and obtains the original image. From the certified authority, the merchant account details and the carrier image are sent to the bank where customer’s authentication is recovered from the carrier. Customer’s authentication information is sent to merchant by certified authority. After receiving secret information related to customer authentication, bank matches with its database and after verifying, transfers the fund.

Proposed Algorithm:
Step1: Take a snapshot of secret information. Apply Huffman encoding technique to secret information in the form of an image as shown in below flow chart. Huffman coding is based on the frequency of occurrence of symbols (pixel values of a image). This method uses less number of bits to encode the information that appears quite frequently.

Fig1: Huffman Encoding Technique applied on payload image.
Fig2: Block Diagram of Steganography process

Step2: Select the cover image to hide payload image information. Apply Haar based discrete wavelet transform to compress it. Initially decompose the signal into wavelet coefficients. As a next step, apply threshold value to modify wavelet compression to another sequence and then apply quantization and entropy coding for compression of data.

Step3: Once the compressed image is obtained, the Huffman encoded secret image information is embedded into the compressed carrier image.

Step4: After embedding the secret information, the inverse DWT is applied to reconstruct the picture information in spatial domain and then stego signal is obtained.

Step5: As a next step apply visual cryptography technique on stego image. But visual cryptography works only on binary image. Hence Digital half toning is used to convert the grey scale image into binary format. After obtaining the binary image, shares are created by making use of visual cryptography technique. Now two shares are obtained which can be stored in two separate databases.

Fig3: Visual cryptography process

Fig4: Digital halftoned images
Step 6: Next step is extraction of secret information; here we make use of two shares generated in the previous step. To obtain the combined image we make use of XOR bit operation between two shares. Next on the stacked image, haar based DWT technique is applied to convert the image from time domain to frequency domain.

Step 7: As a last step, apply Huffman decoding, which is exactly the reverse of Huffman encoding to obtain secret information.

4. Simulation Results

Fig5: Block diagram of Extraction Process.

Fig6: GUI1 considering logo as a secret information and Customer’s image being cover image

Fig7: GUI1 considering logo as a secret information
The above graphical user interfaces demonstrate the lossless recovery of secret information. The tabulated results prove that the proposed algorithm using DWT and visual cryptography combination provides better PSNR and MSE values as compared to existing algorithm using DCT. PSNR and MSE are the evaluation parameters used to evaluate the effectiveness of the proposed algorithm.

Consider a monochrome image I of size m×n. Let Noise approximation be K. Mean square error (MSE) and Peak signal to noise ratio (PSNR) is calculated as shown below.

\[ \text{MSE} = \frac{\sum_{m,n} (I(m,n) - K(m,n))^2}{m \times n} \]  

\[ \text{PSNR} = 10 \log_{10} \left( \frac{\text{MAXI}}{\text{MSE}} \right) \]

Here, MAXI is the pixel value with maximum magnitude. If the pixels are represented using 8 bits, then the maximum pixel value is 255. Ideal PSNR value for lossy compression technique applied to images and video ranges between 30 to 50 dB. If the pixel value is represented by using 16 bits there is a visible improvement in the quality of retrieved image and its PSNR ranges from 60 to 80 dB. The range of acceptable loss in wireless transmission system ranges from 20 to 25 dB.

### 5 Conclusion

The Proposed algorithm is a new and unique approach providing very limited information that is needed for shopping online and thereby providing greater security to customer’s account details and thereby enhancing security to online transactions. The effectiveness of the algorithm is evaluated using evaluation parameters like PSNR and MSE. From the experimented results, it is found that there is appreciable increase in PSNR value as well as greater reduction in the MSE as compared to existing techniques which use Discrete cosine transform applied on cover image to hide secret information. Better PSNR could be achieved with 16 bit coding for each pixel to represent information.
References

1. “Visual cryptography,” M. Naor and A. Shamir, Advances in Cryptography: EUROCRYPT’94, LNCS, vol. 950, pp. 1–12, 1995.
2. “Novel Authentication System Using Visual Cryptography,” Jaya, Siddharth Malik, Abhinav Aggarwal, Anjali Sardana, Indian Institute of Technology Roorkee, India.
3. “Secure Authentication using Image Processing and Visual Cryptography for Banking Applications,” Chetana Hegde, Manu S, P Deepa Shenoy, Venugopal K R, L M Patnaik Department of Computer Science and Engineering University Visvesvaraya College of Engineering, Bangalore University, Bangalore 560 001, India.
4. “Visual Cryptography Improvises the Security of Tongue as a Biometric in Banking System” Sowmya Suryadevara, Rohaila Naaz, Shweta, Shuchita Kapoor, Anand Sharma, Computer Science Dept. Mody Institute of Technology Laxmangarh, Rajasthan, India.
5. “Online Voting System Powered By Biometric Security Using Steganography,” Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi Department of Computer Science and Engineering Indian Institute of Technology Guwahati, India – 781039.
6. “A Tutorial Review on Steganography,” Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, University of Calcutta, Computer Science and Engineering Department, Heritage Institute of Technology, Anandapur, Kolkata – 700107.
7. “Multilayer Information Hiding -A blend of Steganography and Visual Cryptography,” Jithesh k, Dr. A V Senthil Kumar, Department of Computer Science, Hindustan College of Science & Commerce, Coimbatore-641006, Tamil Nadu.
8. “Evaluation of Huffman and Arithmetic Algorithms for Multimedia Compression Standards,” Asadollah Shahbahrami, Ramin Bahrampour, Mobin S. Rostami, Mostafa Ayoubi Mobarhan, Department of Computer Engineering, University of Guilan, Rasht, Iran.
9. “Image Compression Using Discrete Wavelet Transform,” Bhonde Nilesh, Shinde Sachin, Nagmode Pradip, D.B. Rane.
10. “Protection of Confidential Color Image Information Based on Reversible Data Hiding Technique (PCCIRT)” Anitha Devi M.D, Dr K.B. ShivaKumar, International conference on computing and network communications (CoCoNet’15), Dec 16-19, 2015.

First Author:

Anitha Devi M.D received her master degree in Digital Electronics and Communication from VTU Belgaum, Karnataka, India in the year 2006. She is currently pursuing her PhD degree in the field of Image processing and Steganography at SSAHE University Tumkur, Karnataka, India. She is working as assistant professor in the department of Electronics and Communication, SSIT, Tumkur since 2006 till date. Her research interests include Data hiding techniques and Image Processing.
Second Author:

K.B. Shiva Kumar received the PhD degree from Fakir Mohan University, ODISHA, India in 2012. He is currently Professor and Head of Telecommunication Engineering Dept at SSIT, Tumkur, Karnataka, India. His research interests include Steganography, Image Processing and Communication.