World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:11, No:7, 2017

Secure E-Pay System Using Steganography and Visual Cryptography

K. Suganya Devi, P. Srinivasan, M. P. Vaishnave, G. Arutperumjothi

***Abstract*—**Today's internet world is highly prone to various online attacks, of which the most harmful attack is phishing. The attackers host the fake websites which are very similar and look alike. We propose an image based authentication using steganography and visual cryptography to prevent phishing. This paper presents a secure steganographic technique for true color (RGB) images and uses Discrete Cosine Transform to compress the images. The proposed method hides the secret data inside the cover image. The use of visual cryptography is to preserve the privacy of an image by decomposing the original image into two shares. Original image can be identified only when both qualified shares are simultaneously available. Individual share does not reveal the identity of the original image. Thus, the existence of the secret message is hard to be detected by the RS steganalysis.

***Keywords*—**Image security, random LSB, steganography, visual cryptography.

I. Introduction

STEGANOGRAPHY has its origin from a Greek word meaning "concealed writing". It is a way to hide secret information in cover image pixels in such a way that it cannot be detected by Human Visual System (HVS) [1], and none can detect its existence without the intended sender and receiver. Carrier object, secret data and steganographic algorithm are the three major components of steganography. Generally, introducing a secret key and cryptographic algorithm has always become mandatory for increasing the security levels. Steganography can be incorporated for providing security in many applications, viz. online voting, transmission of top-secret data, online banking, and safe circulation of secret documents among defense organizations. On the other hand, steganography could also be very iniquitous, e.g. terrorists and criminals use steganography for their communication and inject viruses and trojan horses.

A. Classification of Steganography

The carrier object used for embedding the secrets can be images, text, videos, audios, or network protocol packets. Based on the type of carrier object used, steganography is classified into five types. if the text is used as a carrier, it is called text steganography. Similarly, if audio is used for hiding secret messages, we call it audio steganography, and so on. The types of steganography are:

a. Audio steganography
b. Image steganography
c. Video steganography
d. Text steganography
e. Network steganography

B. Classifications of Steganographic Techniques

Various approaches can be employed in the classification of steganographic techniques. One classification is based on the carrier object that is used at the time of embedding the secret data into the carrier object. Another classification approach [1] is to categorize them on the basis of cover modification in the process of hiding secret information. Using the second approach, we could classify steganographic techniques into two broad domains.

1.Spatial Domain Techniques

In this technique, a direct change is incorporated in the carrier object (text, audio, etc.) in order to hide secret data. Though this technique has advantages of having high payload and involves less changes in the carrier object, they are vulnerable to even simple attacks like cropping, scaling, rotating, compression, etc. Some of the techniques that belong to spatial domain are:

a. Least Significant Bit (LSB)
b. Gray-Level Modification (GLM)
c. Pixel Value Differencing (PVD)
d. Edges based Embedding (EBE)

2.Transform Domain Techniques

In the transform domain technique, the carrier object (image, video, etc.) is first transformed from spatial domain to transform domain. After that, its frequencies are used to hide the secret data, and again, the carrier object is transformed to spatial domain. Though these techniques have advantages of having lower payload, they have robustness against statistical attacks. Some of the techniques that belong to transform domain are:

a. Discrete Wavelet Transform Technique (DWTT)
b. Discrete Fourier Transform Technique (DFTT)
c. Discrete Cosine Transform Technique (DCTT)

In this paper, we have chosen color image as a carrier object because it contains more redundant bits. Also, color images provide more pixels to increase the payload capacity.

C. Image Processing

Image processing is a form of signal processing for which

F. K. Suganya Devi is with the Department of CSE, University College of Engineering Panruti, Tamilnadu, 607106 India (e-mail: ssuganya.ucep@ gmail.com).

S. P. Srinivasan is with the Department of Physics, University College of Engineering Panruti, Tamilnadu, 607106 India (e-mail: sril35@ gmail.com).

T. M. P. Vaiyshnavi and P. Arutperumjothi are with the Department of CSE, University College of Engineering Panruti, Tamilnadu, 607106 India (e-mail: vaishnnave03@gmail.com, apjothi131@gmail.com).

input is an image, such as photograph or video frame. The output can either be an image or a set of features or characteristics related to the input image. Mostly, all the image-processing techniques treat the input image as a two-dimensional signal and then apply standard or well-known signal processing techniques to it.

D. Visual Cryptography

Visual cryptography is a cryptographic technique which involves encryption of the input image by dividing it into some shares, and on the other side, for decryption some or all the shares of the encrypted image, they are used for overlapping to get back the original image. Visual Cryptography Scheme (VCS) is a kind of secret sharing scheme [2] that focuses on sharing secret images. The idea behind the proposed visual cryptography model is to split a secret image, which separately reveals no information other than the size of the secret image, into two random shares (printed on transparencies). Similarly, to reconstruct the secret image, the two shares will be stacked. The underlying operation for this technique is logical OR operation.

Various visual cryptography applications are as follow:

1) Biometric security
2) Watermarking
3) Steganography
4) Printing and scanning applications
5) Bank customer identification

Types of visual cryptography:

1) Halftone visual cryptography
2) Color visual cryptography
3) Visual Cryptography with Perfect Restoration
4) Multiresolution Visual Cryptography
5) Progressive Multiresolution Visual Cryptography

II. Literature Review

Right from its start (by ancient Greeks in 484-425 BC), many technical, linguistics, and modern steganographic techniques [2] have been developed and used for steganography, each having their own advantages and disadvantages. Though some of the techniques seem to have high payload capacity with good imperceptibility depending upon the carrier object for hiding secret data (spatial domain techniques), they are more vulnerable to attacks. Other techniques are more robust against statistical attacks but they have lower payload capacity. So, always there exists a trade-off between these three factors, i.e. payload, imperceptibility and robustness. As an example, a few techniques of steganography and visual cryptography are discussed below.

LSB is the basic technique used for steganography in which the least significant bit of carrier image pixels is replaced with bits of secret message. To clarify the concept of LSB method, let us consider an example,

Byte that must be hidden:
01101010

Cover message bytes:
10001001
10011000
01100111
00101000
10001111
01000110
01110101

Now, the LSBs of cover image are modified according to the secret message byte:

Decimal Binary:
01101010
10001000
10011001
01100111
00101000
10001111
01000110
01110101
10011000

In the above technique, only the LSB bits vary so that it would not show any significant difference in the cover image.

A secure technique [3] has been proposed where they have hided secret data in the LSBs of cover image pixels in a cyclic manner at random. The secret bits are embedded in cover image pixels' planes in a randomized and cyclic pattern [1] which results in: increase in robustness of the algorithm and random dispersion of secret data inside the cover image pixels. The disadvantage of this method is its vulnerability to different image processing and statistical attacks such as image cropping, scaling and noise attacks since it uses spatial domain approach.

A methodology on visual (2,2) sharing scheme [4] has been discussed. This method emphasizes on two main rules:

1) Recovering the secret image can be done by any qualified subset of shares.
2) Only the size of the secret image could be obtained by the forbidden subset of shares. This type of segment-based visual cryptography can be used to encrypt the messages containing symbols only especially numbers, like bank account number, balance, etc. The customer's signature is extracted from the application.

A method which ensures the security against the RS analysis [5] has been proposed. By the use of Genetic algorithm after embedding the secret message in LSB (least significant bit) of the cover image [8], the pixel values of the stego-image are modified to keep their statistic features. Thus, it will be difficult to detect the existence of the secret message by the RS analysis, and also, a better visual quality can be achieved by the system.

The DCT technique [6] is often being used in the secure steganography. The stego image is divided into blocks; the image is split into 8*8 pixels, laboring from top to bottom, left to right, the DCT has been applied to each block. The DCT efforts to decorrelate the image data will make the intruder difficult to identify the hidden image inside the cover image.

Text based steganography [7] and visual cryptography for net banking have been used. This is achieved by the introduction of a central Certified Authority (CA) to verify the

authentication of the customer. Once after verifying the customer, CA intimates the bank about payment transaction.

III. Proposed Work

The proposed method uses combined steganography and visual cryptography technique to secure the information being shared online. It uses LSB algorithm to hide the secret image inside the cover image but uses random hiding technique and it will not be sequential.

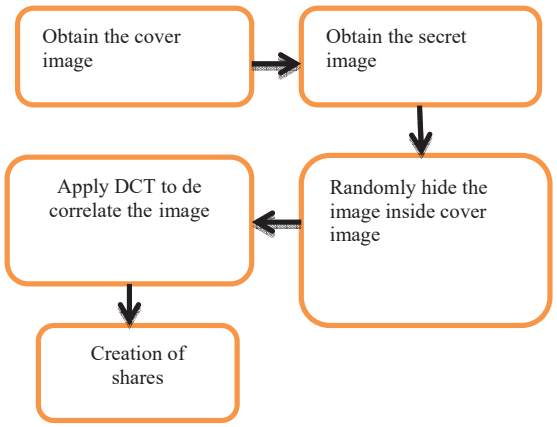

Fig. 1 Proposed System

A. 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 taken inside the function. The method determines the message type and uses the seed key to randomly select pixel locations to encode the message within. To do this, the method determines the dimensions of the cover image and multiplies the dimensions together to provide the number of available pixels. Then, by using the same random seed 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 way. This ensures the prevention of overwriting of message values in the cover image and can recover the secret message during the decoding stage. Then, the secret image is embedded inside the cover image. This method is more secure because the message is encoded across the entire image instead of the left portion of the image.

B. Application of DCT and Inverse DCT to the Stego Image to Perform De Correlation

Once the stego image is obtained DCT, quantization is applied on it to de correlate it. The use of transformation technique is to prevent the intruders from analyzing the type of steganography performed on the image even though they can identify that some types of steganography have been performed by RS analysis.

C. Separation of Image into Shares Using V [2, 2] Sharing Technique.

The decompressed image is divided into two shares with the help of V(2,2) sharing scheme. The decompressed image can be obtained by overlapping the two shares. The information will be obtained if and only if both shares are qualified.

D. Decoding Stage

During decoding, shares are authenticated using visual cryptography scheme. Upon overlapping the shares, if the obtained image is similar to the decompressed image, the steganography process can be decoded. The method takes in the cover image and random seed key to decode the header in order to determine the message type and message length. Then, it uses the random seed key to initialize and recover the random pixel locations using the permutation function. The method first yields the cover image's dimensions to determine the number of pixels available before obtaining the permutated pixel locations. Next, the function recovers randomly encoded message values [9] from the cover image by first isolating the header information to determine the message type and length. The function then proceeds to decode the rest of the message and decrypts the image.

IV. Experimental Results

From Table I, it could be seen that in the proposed method, both Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) are reduced in comparison with the existing DCT and LSB methods.

TABLE I
PSNR, MSE Comparison Based on Proposed Method and Existing Method

Stego Image	PSNR	MSE
Proposed Method	32.8553	33.6942
DCT Steganography	63.543	65.782
LSB Method	63.3775	64.823

V. Conclusion

In this paper, we proposed a more secure steganographic algorithm for RGB images using the concept of DCT based image steganography. The utilization of randomized hiding on of shares makes the extraction of original secret information from the stego image more difficult for a malicious user. The obtained PSNR value is far better than the existing system. Hence, the proposed technique provides interesting and appealing results in terms of robustness and security. This method can be used to provide secure online banking.

References

[1] Anandhi and S. Sathiyaraj, "*Embedded Visual Cryptography Schemes for Secret Images"* International Journal of Computer Science and Network Security (IJCSNS) Volume.12 – No.12, December 2012, Page 153-158.

[2] Souvik Roy and P. Venkateswaran 2014 "Online Payment System using Steganography and Visual Cryptography" IEEE Students Conference on Electrical, Electronics and Computer Science 978-1-4799-2526-1/14/$31.00 ©2014.

[3] D. B. Satre, Varad Durugkar, Akshay Ambekar, Amit Kumar Yadav, Sudarshan Patil "Securing Online Shopping System Using Visual Cryptography"International Journal of Emerging Technologies and Engineering (IJETE) Volume 2 Issue 1, January 2015, ISSN 2348 – 8050.

[4] B. Srikanth, G. Padmaja, Syed Khasim, P. V. S.Lakshmi, A. Haritha "*Secured Bank Authentication using Image Processing and Visual*

Cryptography" International Journal of Computer Applications (0975 – 8887) Volume 124 – No.6, August 2015.

[5] V. Lokeswara Reddy, T. Anusha "*Combine Use of Steganography and Visual Cryptography for Online Payment System*" International Journal of Computer Applications (0975 – 8887) Volume 124 – No.6, August 2015.

[6] Mahsuna Abdul Sathar, Nimya, Shana, Vipin Goutham, Geethu Bastian. "*Secured E-Payment System Using Image Steganography and Visual Cryptography*" International Journal of Computer Trends and Technology (IJCTT) – volume 28 Number 4 – October 2015 ISSN: 2231-2803 http://www.ijcttjournal.org Page 189.

[7] Navjot Kumar, Ashima Bansal, "*A Review on Digital Image Steganography"* International Journal of Computer Science and Information Technologies (IJCSIT), Volume 5 – No.6, 2014, 8135-8137.

[8] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, R. J. Qureshi, "*A Secure cyclic Steganographic Technique for color images using Randomization"* Technical Journal, University of Engineering and Technology Taxila, Volume 19 – No.III, 2014, 57-64.

[9] https://sites.google.com/site/cs534steganographyproject/home/matlab-code-and-examples.