A Scheme for Secret Image Communication using Image Steganography and DCT

Rohit Agrawal
Department of Computer Science and Engineering
Indian School of Mines, Dhanbad
Jharkhand-826004, India
E-mail: agarwal0115@gmail.com

Arup Kumar Pal
Department of Computer Science and Engineering
Indian School of Mines, Dhanbad
Jharkhand-826004, India
E-mail: arupkrpal@gmail.com

***Abstract*— In this paper, an image steganography is proposed for transmission of a secret image. The scheme initially employs block based discrete cosine transformation (DCT) on each cover and secret image to transform them from spatial domain to frequency domain. After DCT operation, some significant low frequency coefficients of the secret image are considered for embedding into the cover image, after performing suitable modification on the high frequency coefficients of the transformed cover image. During embedding process, the DC component of each block, which is obtained from the secret image, are embedded using suitable scaling factor. While the rest of the selected AC components of the secret image are embedded after performing proper normalization such that it produces significantly less distortion on the cover image. The scheme has been tested on several standard gray scale images and we have obtained the satisfactory results. The scheme was further compared with existing similar work to show the effectiveness of the proposed work.**

Keywords- Discrete Cosine Transform (DCT); Image Steganography; Normalization; Secrete Image Communication.

I. INTRODUCTION

Internet is one of the most popular and easiest medium for transmission of digital data among people. However the major concern issues during transmission is that anybody can access these data during transmission, so sender must employ some security mechanisms on these digital data to protect them from being accessed by illegitimate users. To protect the secret data, in general, two approaches are mainly used i.e. cryptography [1] and steganography [2]. In cryptography, the encryption process transforms the secret data i.e. known as plain text into a cipher text using an encryption key. The cipher text is appeared as unreadable form; only the decryption process of the cryptography can convert the cipher text into original or plain text using the decryption key. In cryptography, it focuses is that illegitimate users should not able to decrypt the cipher text into plain text without knowing the decryption key. However, in cryptography, cipher text resembles in unreadable form so it attracts the opponents to exploit the content of the cipher text by employing the brute-force attack. In cryptography, we cannot avoid such type of brute force attack. There is another approach i.e. known as steganography, can divert opponent's attention to employ some brute force attack on the secret data. Steganography derived from Greek word steganos means "covered or secret" and graphy means "writing or drawing". Its objective is to hide the secret data into some other unsuspected cover media so that the secret data will be visually imperceptible. Steganography hides the secret message within cover media, where the cover media may be audio, video, text or image. When it hides the secret data into a cover media like image then it termed as image steganography. In steganography, for embedding the secret data into the cover image, least significant bit (LSB) substitution [3] is one of the popular and widely used techniques. Some other substitution methods [3] have been proposed by modifying the conventional LSB substitution. But the all these embedding process have limited embedding capacity. For example, If we use 3LSBs embedding approach then we can only embed a gray-scale image of size 384×256 into a 512×512 size gray-scale cover image. More than 3LSBs substitutions are not suitable for insertion of the secret message into the cover image because it distorts the stego-image drastically [3]. In this paper, our objective is to transmit a secret gray-scale image through a same size of cover image. So our approach can transmit a secret image of size 512×512 through a gray-scale cover image of size 512×512.

The rest of the paper is organized as follows. Section II describes in briefly the preliminaries of block-based DCT. The proposed scheme, including the embedding and the extraction process, is presented in section III. The simulation results and performance analysis are furnished in section IV. Finally, the conclusion is drawn in section V.

II. PRELIMINARIES OF BLOCK-BASED DCT

The discrete cosine transform (DCT) [4] is one of the popular tools for transforming the spatial feature of an image into frequency domain. The DCT has wide application on image compression [5], image enhancement [6], digital watermarking [7], steganography [8, 10-11] and so on. Instead of applying DCT directly on the whole image, in general it is applied on block level of the image for its better performance. Most of the applications use DCT on block of size 8×8. In our proposed scheme, we have also employed DCT on block of size 8×8. The block-based

DCT transformation for an sub-image block of size 8×8 is defined as follow;

$$X(u,v)=\frac{1}{4}c(u)c(v)\sum_{m=0}^{7}\sum_{n=0}^{7}x[m,n]\cos\left[\frac{(2m+1)u\pi}{16}\right]\cos\left[\frac{(2n+1)v\pi}{16}\right] \quad (1)$$

Where x[m,n] with m=0, 1, 2, …, 7 and n=0, 1, 2, …, 7 and X[u,v] with u=0, 1, 2, …, 7 and v=0, 1, 2, …, 7 represent the pixel values of the sub-image block and the obtained frequency coefficients of DCT transformed sub-image block respectively. The coefficient value of *c* is obtained as follow:

$$C(k)=\begin{cases}\frac{1}{\sqrt{2}} & ,\text{for } k=0\\ 1 & ,\text{otherwise}\end{cases}$$

So after transformation, it produces 64 coefficients for each block and these coefficients are processed according to the zig-zag scanning order as shown in Fig 1. The top-left coefficient refers as the DC value while the rest of the coefficients are known as AC values. The zig-zag scanning order implies the frequency distribution from low to high. Most of the visual information is concentrated towards the low frequency coefficients here we have termed them as a most significant components (MSC) while in this present work, the rest of the coefficients i.e. high frequency coefficients are termed as the lest significant component (LSC). The LSC have carry some less amount information. With out loss of information, the original sub-image block can be produced by using the following equation.

$$x(u,v)=\frac{1}{4}c(u)c(v)\sum_{m=0}^{7}\sum_{n=0}^{7}X[m,n]\cos\left[\frac{(2m+1)u\pi}{16}\right]\cos\left[\frac{(2n+1)v\pi}{16}\right] \quad (2)$$

For u=0, 1, 2……..7 and v=0,1,2……..7

$$C(k)=\begin{cases}\frac{1}{\sqrt{2}} & ,\text{for } k=0\\ 1 & ,\text{otherwise}\end{cases}$$

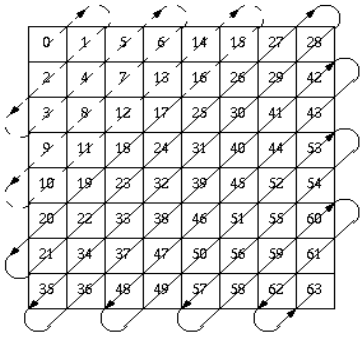

Figure 1. The Zig-zag scanning order.

The Eq. 2 is known as the Inverse 2-D DCT. The loss will be incurred when some LSC will be discarded. The dotted line of Fig 1 depicts the presence of MSC. We have reconstructed some approximate images as shown in Fig. 2 where we have selected various number of MSCs to show the disparity occurred in the reconstructed images. It can be observed that the approximate image based on 16 MSCs can also preserve high PSNR value. So in this present work, we have considered 16 MSCs of the secret image as a secret content.

Figure 2. The reconstructed images using various MSCs.

III. PROPOSED TECHNIQUE

In this work, we have embedded a DCT compressed image into another image where both the cover and the secret image size are same. The detail of the embedding procedure is described as below.

A. The Embedding Procedure:

Initially, the secret image, ***S*** and the cover image, ***C*** where both having the size $M\times N$, are decomposed into non-overlapping blocks of size 8×8 pixels and the total number of blocks are $N_B(=MN/64)$. After that, each block is transformed using Eq. 1 and it produces *64* DCT coefficients. Let $C_i=\{C_{i1},C_{i2},\cdots,C_{i64}\}$ and $S_i=\{S_{i1},S_{i2},\cdots,S_{i64}\}$ denote the DCT coefficients of ***i-th*** block from ***C*** and ***S*** respectively. In our proposed work, ***i-th*** block MSCs of the secret image are embedded into *i-**th*** block LSCs of the cover image. The traversing along the dotted line, as shown in Fig 1, represents the MSCs of any DCT transformed image block. In this work, we have selected ***n*** number of MSCs from each block of secret image and ***i-th*** block MSCs are denoted as $\{S_{i1},S_{i2},\cdots,S_{in}\}$. In the next stage, we have chosen ***n+ 2*** numbers of LSCs from the ***i-th*** block and that is denoted as $\{C_{i(n+1)},C_{i(n+2)},\cdots,C_{i(2n+2)}\}$. In general, the intensity variation between the DC and AC components is relatively high. So in our scheme, we have embedded the DC component by employing suitable scaling factor. Here S_{i1} denotes ***i-th*** block DC component of a secret image. Now, this DC component is embedded into ***i-th*** block cover image as follows

$$\tilde{C}_{i(n+1)}=C_{in}+\alpha S_{i1} \quad (3)$$

where $\tilde{C}_{i(n+1)}$ is the modified coefficients of the original coefficients $C_{i(n+1)}$ and α is the scaling factor.

In the next stage, a suitable normalization process has been carried out on the rest of the MSCs of ***i-th*** block secret image such that the range of the modified MSCs can be easily mapped into the range of the LSCs of ***i-th*** block cover image. Here the embedding process is done via

replacement of the LSCs of ***i-th*** block cover image by the normalized MSCs of ***i-th*** block secret image.

Let Min_C_i and Max_C_i denote the minimum and maximum coefficients obtained from LSCs i.e. $\{C_{i(n+1)}, C_{i(n+2)}, \cdots, C_{i(2n+2)}\}$ of ***i-th*** block cover image . The Max_C_i and Min_C_i values are stored in (n+2)-th and (2n+2)-th position in the LSCs of ***i-th*** block cover image. The normalization process has been carried out using Eq 4. After completion of embedding process, inverse DCT has applied on the modified cover image to form the stego-image. The schematic diagram of the embedding process is depicted in Fig 3.

$$\tilde{C}_{n+1+k} = \frac{S_k - Min\_C}{Max\_C - Min\_C} \quad (4)$$

where $k = 2,3,\cdots,n$

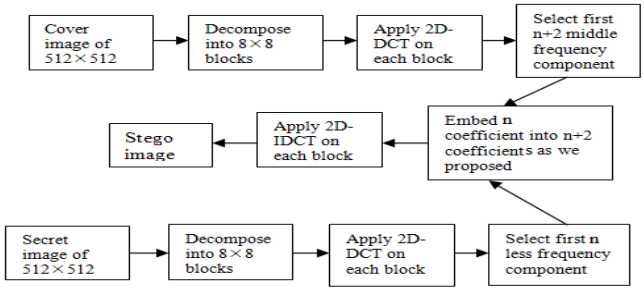

Figure 3. The proposed embedding process.

B. Extraction procedure:

In the extraction process, the secret image is extracted from the stego-image into three phases. In the first phase, the stego image is decomposed into non-overlapping blocks of size 8×8 after that in block label, DCT is employed on each block to extract the LSCs. In the second stage, from the LSCs of the stego-image, we produce the MSCs of the secret image. The DC component of the secret image is obtained using Eq. 5.

$$S_{i1} = \frac{\tilde{C}_{i(n+1)} - C_{in}}{\alpha} \quad (5)$$

The rest of the AC coefficients of the secret image are found as follow.

$$S_k = \tilde{C}_{n+1+k}\left(Max\_C - Min\_C\right) + Min\_C \quad (6)$$

where $k = 2,3,\cdots,n$

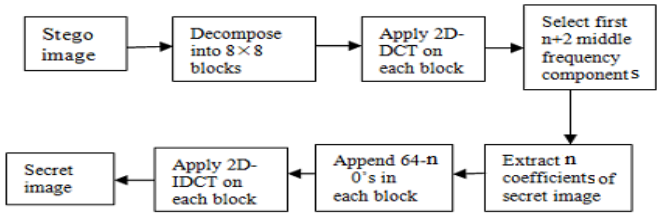

Figure 4. The proposed extraction procedure.

IV. EXPERIMENTAL RESULTS

In this section, the experimental result are presented to evaluate the performance of our propose scheme. We have tested our scheme on a set of standard test images. As representative, here we have presented the experimental results based on few images. In our experiment, we have considered 512×512 size of grayscale image for both the cover and the secret. In our experiment, we have chosen parameters values like n=16, α=0.001.The performance of the proposed scheme is evaluated based the computation of PSNR [9] values for the stego-image. We have also drawn the histogram (as shown in Fig 5) for both the cover image the stego-image to show the disparity occurred after embedding the secret image into the cover image. In our proposed scheme, the histogram of the cover image and the stego-image are almost similar. It implies that after embedding the secret image in the cover image, the visual quality of the stego-image is distorted minimum. The obtained PSNR values are given in Table 1.

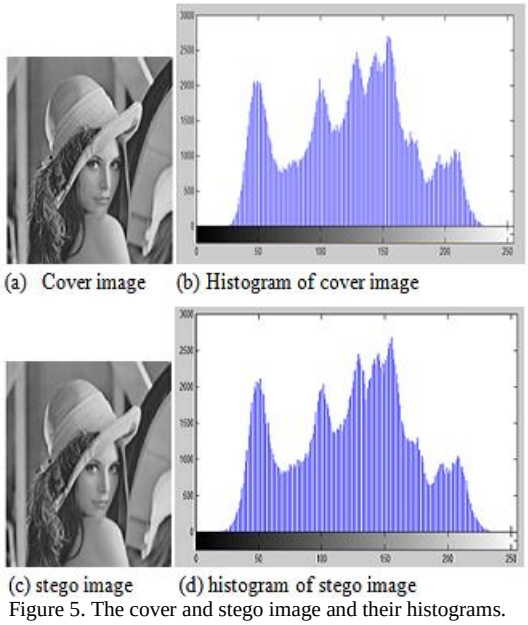

Figure 5. The cover and stego image and their histograms.

TABLE 1. PSNR VALUES OF STEGO AND EXTRACTED SECRET IMAGE

Secret image of size 512×512	**PSNR value of stego image (Cover image of size 512×512)**			**PSNR value of extracted secret image**
	Airplane	**Boat**	**Lena**	**Lena as cover image**
Peppers	**34.948**	**33.998**	**35.566**	**34.820**
Baboon	**34.466**	**33.660**	**35.267**	**29.825**
Barbara	**35.444**	**34.163**	**35.888**	**26.892**
Lena	**35.316**	**34.446**	**36.507**	**34.606**

Table 1 show that our proposed scheme can preserve high PSNR values i.e. more than 30dB even after embedding the secret image of same size of the cover image. The similar type of work with different approach have done by A. Nag et-al[10], and Chin et-al[11]. Our propose approach have higher embedding capacity and PSNR value greater than 30dB. Which are represented in Table 1. Both the original and extracted secret images and their histogram are shown in fig 6 to show the discrepancy occurred after extracting the secret image from stego image. In our propose approach the extracted secret image is not much more distinct to original secret image and their histogram are also similar.

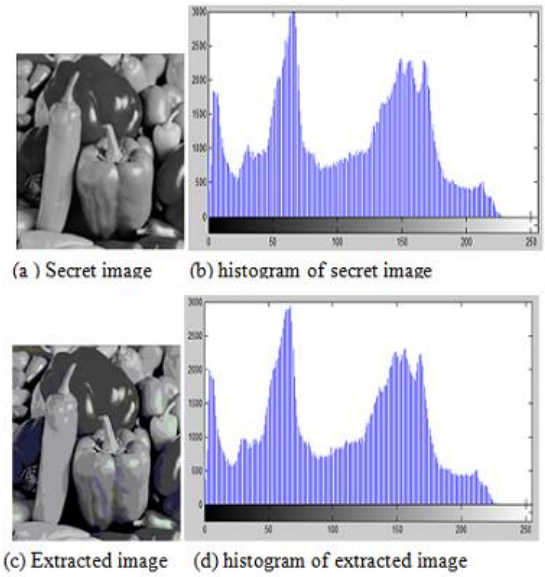

Figure 6. The original and extracted secret images and their histograms.

V. CONCLUSION

In this paper, the propose data hiding scheme is not only simple and effective in retaining good quality stego-image, but also provide high embedding capacity for secure image communication. The simulation results of our proposed scheme on gray label image of size 512×512 have been carried out using MATLAB and satisfactory result have been obtained. We are able to preserve the high PSNR values that are greater than 30dB for both the stego and the cover image and it is also difficult to distinguish between original and stego image and their histograms are also similar.

REFERENCES

[1] Cryptography and Network security Principles and Practice, fifth edition by William stalling.

[2] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, Digital image steganography: Survey and analysis of current methods, Signal processing 90 (2010) 727-752, pp. 728-750, 6 September 2009.

[3] Chi-Kwong Chan, L.M. Cheng, Hiding data in images by simple LSB substitution, Pattern Recognition 37 (2004) 467-474, pp 470-474, August 2003

[4] Digital Image processing third edition by Rafael C. Gonzalez, Richard E. Woods.

[5] Andrew B. Watson NASA Ames Research Center, Image Compression Using the Discrete Cosine Transform, Mathematica Journal, 4(1), pp. 81-88, 1994.

[6] Jinshan Tang, Senior Member, IEEE, Eli Peli, and Scott Acton, Senior Member, *IEEE* Image Enhancement Using a Contrast Measure in the Compressed Domain, IEEE SIGNAL PROCESSING LETTERS, VOL. 10, NO. 10, pp 289-292, October 2003.

[7] Shinfeng D. Lin and Chin-Feng Chen, A Robust DCT-Based Watermarking for Copyright Protection, IEEE Transactions on Consumer Electronics, Vol. 46, **No.** 3, pp 415-420, August 2000.

[8] Dr. Ekta Walia , Payal Jain, Navdeep, An Analysis of LSB & DCT based Steganography, Global Journal of Computer Science and Technology, Vol. 10 Issue 1, Ver 1.0, pp 4-8, April 2010.

[9] Deepak S. Turaga, Yingwei Chen, Jorge Caviedes, No reference PSNR estimation for compressed pictures, Signal Processing: Image Communication 19, pp173-184, 2004.

[10] A. Nag, S. biswas, D. Sarkar, P.P. Sarkar, A novel technique for image steganography based on Block-DCT and Huffman Encoding, International journal of Computer Science and information technology, volume 2, pp 104-122, number 3, June 2010.

[11] Chin-Chen Chang, Chi-Lung Chiang, and Ju-Yuan Hsiao, A DCT-domain System for Hiding Fractal Compressed Images, 19th International Conference on Advanced Information Networking and Applications (AINA'05), pp 1-4, 2005.