Volume 2, Issue 2, February 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Session Based Multiple Image Hiding Technique using Discrete Cosine Transformation

Tanmay Bhattacharya,Nilanjan Dey
Asst. Professor Dept. of IT
JIS College of Engineering
Kalyani, West Bengal, India

S. R. Bhadra Chaudhuri
Professor, Dept of E&TCE
Bengal Engineering and Science University
Shibpur Howrah, West Bengal, India

Abstract— ***This work proposes a DCT based Steganographic technique for the color image. The true color cover image is decomposed into three separate color planes namely R, G and B. During embedding of secret images into different color planes, images are dispersed among the selected DCT coefficients using a pseudo random sequence and a Session key. Secret images are extracted using the session key and the size of the images from the planer decomposed stego image. In this approach the stego image generated is of acceptable level of imperceptibility and distortion compared to the cover image and the overall security is high.***

Keywords - DCT, Session Based Key, Pseudo Random Sequence, RGB Color planes

I. INTRODUCTION

Steganography [1, 2, 3] is the process of hiding of a secret message within an ordinary message and extracting it at its destination. Anyone else viewing the message will fail to know it contains secret/encrypted data. The word comes from the Greek word "*steganos*" meaning "covered" and "*graphei*" meaning "writing".

LSB [4] insertion is a very simple and common approach to embedding information in an image in spatial domain. The limitation of this approach is vulnerable to every slight image manipulation. Converting image from one format to another format and back could destroy information secret in LSBs. Stego-images can be easily detected by statistical analysis like histogram analysis. This technique involves replacing N least significant bit of each pixel of a container image with the data of a secret message. Stego-image gets destroyed as N increases. Data hiding can also be done in the frequency domain. Cover Image is transformed using conventional transformation like DFT, DCT [5, 6], DWT [7, 8] etc. Secret information is embedded in the less significant frequency components of cover image. The advantage of using frequency domain Steganography is that it is very secure, hard to detect, flexible and has different techniques for manipulation of DCT coefficients values.

II. DISCRETE COSINE TRANSFORMATION

A discrete cosine transform (DCT) is a technique for converting a signal into elementary frequency components. It expresses a sequence of finitely numerous data points in terms of a sum of cosine functions oscillating at different frequencies which is widely used in image compression. The application is pioneered by Chen and Pratt in 1984.

The DCT is closely related to the Discrete Fourier Transform (DFT) with some dissimilarity.

- The DCT is more efficient in concentrating energy into lower order coefficients than what the DFT does for image data.
- The DCT is purely real whereas the DFT is complex (magnitude and phase).
- Coefficients produced by a DCT operation on a block of pixels are similar to the frequency domain coefficients produced by a DFT operation. As an N-point DCT is closely related to a 2N-point DFT, it has the same frequency resolution. The N frequencies of a 2N point DFT correspond to N points on the upper half of the unit circle in the complex frequency plane.
- Unlike DCT, the magnitude of the DFT coefficients is spatially invariant (phase of the input does not matter) assuming a periodic input.

For processing one-dimensional signals such as speech waveforms one-dimensional DCT is used. For analysis of two-dimensional (2D) signals such as images, a 2D version of the DCT is required. As the 2-Dimensional DCT can be computed by applying 1D transforms separately to the rows and columns, it can be said that the 2D DCT is separable in the two dimensions.

For an M × N digital image f (x, y), its two-dimensional discrete cosine transform and its inverse transformation is defined by the following equations.

$$C(u,v) = \alpha(u)\,\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\Pi(2x+1)u}{2N}\right]\cos\left[\frac{\Pi(2y+1)v}{2N}\right]$$

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} \alpha(u)\,\alpha(v)\,c(u,v)\cos\left[\frac{\Pi(2x+1)u}{2N}\right]\cos\left[\frac{\Pi(2y+1)v}{2N}\right]$$

There, C (u, v) is the result of discrete transform, and also known as DCT coefficient.

Where, u, v = 0, 1, 2, ... N-1
x, y = 0, 1, 2, ... N-1

α (u) is defined as follows:

$$\alpha(u) = \sqrt{\frac{1}{N}} \qquad u=0;$$

$$\alpha(u) = \sqrt{\frac{2}{N}} \qquad u=1,2.....N-1$$

III. PROPOSED ALGORITHM

A. *Secret Image Hiding*

1. Cover color image is decomposed into three color planes (R, G and B).
2. Each color plane is transformed into corresponding frequency domain using DCT.
3. Information of three secret binary images are dispersed separately into selected high frequency components of each color plane (in frequency domain) using a session based pseudo random 2D sequence.
4. After embedding bits of the secret images into three color planes inverse transformation are applied to get back the planes in the spatial form.
5. Finally, three color planes are combined to generate the color stego image.

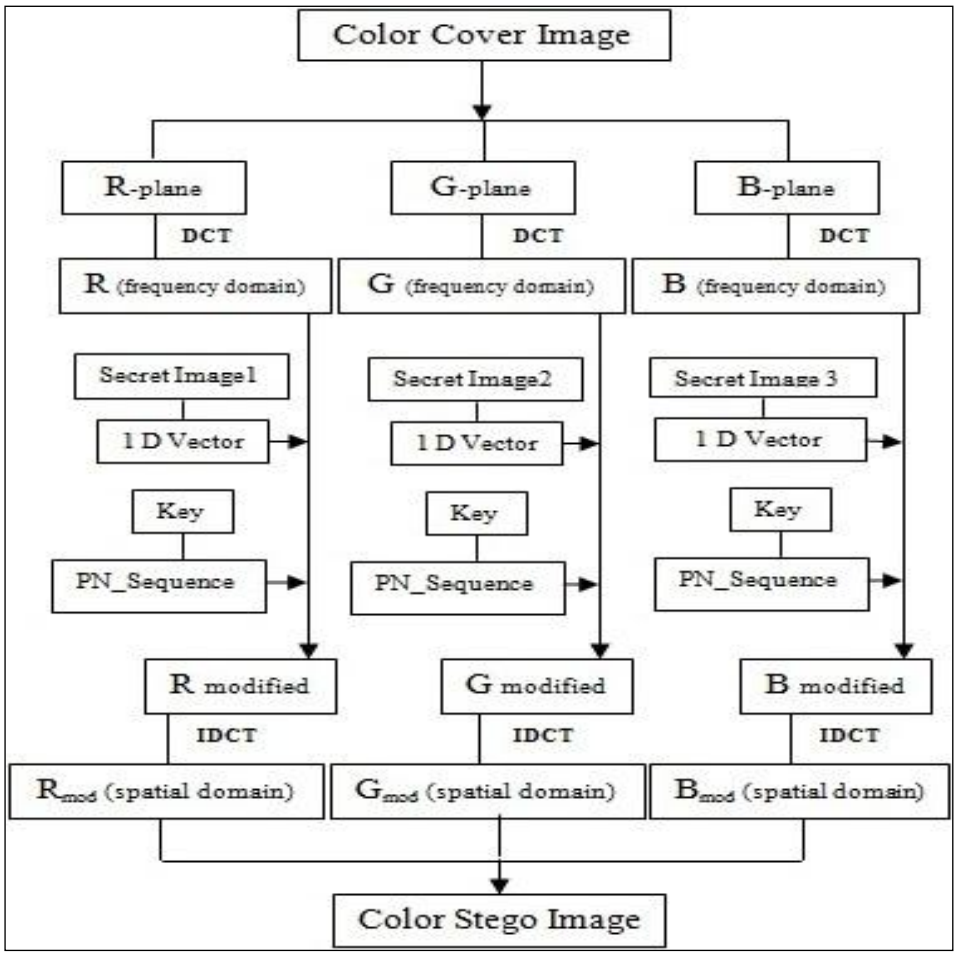

Figure 1. Image Hiding Process

B. Secret Image Extraction

1. Stego color image is decomposed into three color planes (R, G and B).
2. Planes are transformed into corresponding frequency domain using DCT.
3. Three secret images are extracted from the color planes using the session based key and the size of the secret images which are known to the intended receiver only.

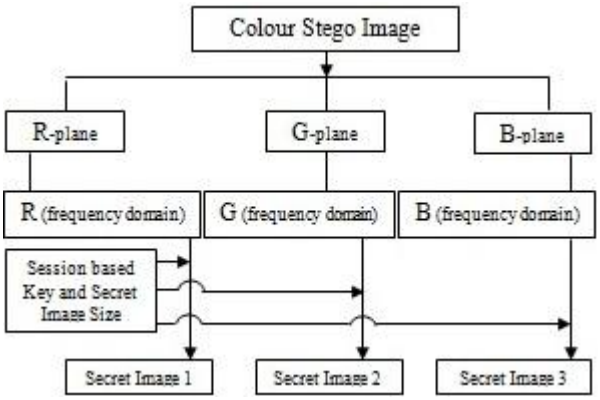

Figure 2. Image Extraction Process

IV. EXPLANATION OF THE ALGORITHM

A. Secret Image hiding procedure

The Cover Image (Color) is decomposed into three color planes namely Red, Green and Blue. Each color planes are transformed from special domain to frequency domain using DCT.

Three secret binary images are converted into three 1-D vectors.

Selected high frequency components of each plane are modified according to the bits of the individual image vector and the session based 2D pseudo random sequence.

Inverse transformation (IDCT) is applied to the planes separately to convert them into corresponding spatial domain. Three planes are then combined to generate the final color stego image.

B. Secret Image Extraction procedure

The color stego image is decomposed into RGB planes and transformed into corresponding frequency domain using DCT. Extraction algorithm along with the session based key and the secret image size is used to recover three secret images from the color planes of the stego image.

V. RESULTS

Results of the proposed algorithm are shown below (Fig. 3 to Fig. 8).

Figure3. Cover Image

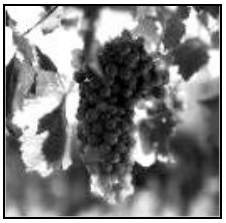

Figure 4. Cover Image(R Plane)

Figure 5. Cover Image (G Plane)

Figure 6. Cover Image (B Plane)

Figure 7. Stego Image

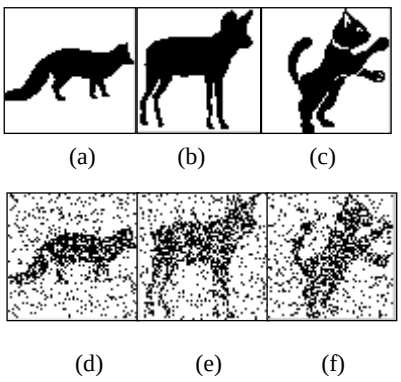

Figure 8. (a) Secret Image1 (b) Secret Image2 (c) Secret Image1 (d) Extracted Secret Image 1 (e) Extracted Secret Image 2 (f) Extracted Secret Image 3

Peak Signal to Noise Ratio (PSNR)

It measures the quality of a stego image. This is basically a performance metric and is used to determine perceptual transparency of the stego image with respect to host image:

$$PSNR = \frac{MN \max_{x,y} P_{x,y}^2}{\sum_{x,y} \left(P_{x,y} - \overline{P}_{x,y}\right)^2}$$

Where, M and N are number of rows and columns in the input image,

$P_{x,y}$ is the original image and

$\overline{P}_{x,y}$ is the Stego Image.

PSNR between Cover Image and Stego Image is 34.0244 shown in Table1.

TABLE 1

Cover Image vs. Stego Image	PSNR
	34.0244

VI. CONCLUSION

In this approach embedding is done randomly in the frequency domain. So, it will be difficult to detect the existence of the secret image using conventional steganalysis methods. Proposed approach gives satisfactory PSNR value to establish the robustness of the work. Since only selected high frequency components are modified for the hiding method, therefore there must be a constraint on the secret image size. Final results can be improved further by applying proper image filter.

REFERENCES

[1] N. F. Johnson and S. Katzenbeisser," *.A survey of steganographic techniques*", in S. Katzenbeisser and F. Peticolas (Eds.): *Information Hiding*, pp.43-78. Artech House, Norwood, MA, 2000.

[2] Lou, D. C. and Liu, J. L. 2002. *"Steganography Method for Secure Communications"*. *Elsevier Science on Computers& Security*, 21, 5: 449-460.

[3] J. Fridrich and M. Goljan, .Practical steganalysis of digital images-state of the art., *Proc. SPIE Photonics West, Vol. 4675*, pp. 1-13, San Jose, California, Jan. 2002.

[4] Chan, C. K. and Cheng, L. M. 2003. Hiding data in image by simple LSB substitution. *Pattern Recognition*, 37:469-474.

[5] Iwata, M., Miyake, K., and Shiozaki, A. 2004. *"Digital Steganography Utilizing Features of JPEG Images",* IEICE Transfusion Fundamentals, E87-A, 4:929-936.

[6] Blossom Kaur, Amandeep Kaur, Jasdeep Singh, "*Steganographic Approach for Hiding Image in DCT Domain",* International Journal of Advances in Engineering & Technology, July 2011.

[7]Po-Yueh Chen* and Hung-Ju Lin, "*A DWT Based Approach for Image Steganography",* International Journal of Applied Science and Engineering 2006. 4, 3: 275-290

[8] Ali Al-Ataby and Fawzi Al-Naima, "*A Modified High Capacity Image Steganography Technique Based on Wavelet Transform",* The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010