A Modified Approach of Image Steganography based on Block DCT and Huffman Encoding without Embedding Dictionary into Stego-Image

Anil N. Bhure
Vishwakarma Institute of Technology
Pune Maharashtra
India

Vaishali S. Jabade
Vishwakarma Institute of Technology
Pune Maharashtra
India

ABSTRACT
Image Steganography is superimposing a secret image into a cover image such a way that perceptability and properties of cover image remains unchanged. In this paper proposing a modified approach of Image Steganography which is based on Block DCT and Huffman Encoding without inserting a Huffman table into stego image. In the proposed method embedded an encoded secret image (Huffman Table) to the transformed cover image (Block DCT) by ± 1 embedding method. To working on N x N block DCT transforming cover image. The experimental result shows that the modified approach gives better Steganography properties of stego image in terms of PSNR, correlation coefficient than the existing algorithm.

Keywords
Steganography, Block DCT, Huffman Encoding.

1. INTRODUCTION

Steganography is not a new technique. The oldest example of steganography along back in Greek to revolt against the Persians was revealed [8].Nowadays different medias are used for information transmission. Steganography is keeping the existence of a message secret behind a carrier. It is used for securing information against unknown person. It gives security services i.e. Confidential, Identification and Authentication. Secret information can be text, image, video or anything can be represented as a bit stream [1] [2]. There are mainly two Steganography categories [3] [4]:

1. According to different technique used in the embedding process.
   - Substitution system technique.
   - Transfer domain technique.
   - Spread spectrum technique.
   - Distortion technique.
   - Cover generation technique.

2. According to carrier type.
   - Text
   - Image
   - Video
   - Protocol

Data insertion technique hiding data in the part of cover object. In substitution based technique replace data from cover data with secret message that substitution degrading cover object [9]. Generation technique creates a cover object for hiding secret information. It is depend upon secret message structure [9].

In [10] have spread spectrum image steganography hiding and recovering a secret message of significant length in digital image and maintaining original image size and dynamic range**.**

The aforementioned proposed theory has common drawback of low resolution, which inspired the authors. In this paper used transform domain of cover image and Huffman encoding of secret image. Simulation results show better solution in terms of security as well as perceptability of cover image.

Following sections are as follows. Section -2 gives brief idea about Block DCT and Huffman Encoding. Section-3 gives the modified approach for better resolution. Performance evaluation of modified approach is simulated in section-4. Finally conclusion is stated in section-5.

2. BLOCK DCT AND HUFFMAN ENCODING

2.1 Block DCT of Cover Image

Under the category of transform domain Steganography, doing Block DCT of cover image. Let f(x, y) denote an 8-bit gray scale cover image with x=1, 2…..M and y=1, 2….N. This M×N cover image is divided into n×n blocks and two-dimensional (2-D) DCT is performed on each of L=M×N/n × n blocks [3, 5]. As we are doing block DCT, cover image size i.e. number of rows & number of columns of image matrix should be divisible by n.

The mathematical definition of DCT is:

Forward DCT:

$$F(u,v) = \frac{1}{4}\, c(u)c(v) \sum_{x=0}^{n} \sum_{x=0}^{n} f(x,y) \cos\left(\frac{\pi(2x+1)u}{16}\right) \cos\left(\frac{\pi(2y+1)v}{16}\right) \quad (1)$$

For u=0……n and v=0…..n

Where c (k) = $\begin{cases} \frac{1}{\sqrt{2}} & for\ k = 0 \\ 1 & otherwise \end{cases}$ (2)

Inverse DCT:

$$f(x,y) = \frac{1}{4}\, c(u)c(v) \sum_{x=0}^{n} \sum_{x=0}^{n} F(u,v) \cos\left(\frac{\pi(2x+1)u}{16}\right) \cos\left(\frac{\pi(2y+1)v}{16}\right) \quad (3)$$

For u=0……n and v=0…..n

Now we are doing 8×8, 16×16, 32×32 bit block DCT. There is a trade-off in security level and computational complexity or because if we do a very small block DCT 8×8 or 4×4. It will increase the security but also computational complexity increases .if go for large block 16×16 or 32×32. It will be beneficial in term of computational complexity but it is less secure as compare to 4×4, 8×8 Block DCT. It is also found that by decreasing Block DCT size capacity also decreasing.

2.2 Huffman Encoding

In the traditional Steganography technique the encoding algorithm are such that they are directly embedding the secret image into cover image without compressing or encoding it. Because of this we required larger or greater size cover image to carry that secret image. So that to avoid this or to increase capacity we move to the encoding of secret image [6]. Now after encoding secret image by efficient loss less encoding scheme like Huffman encoding. We can get very much reduce secret image in case of encoded scheme. In terms of encoded bit stream that is converting a 2-D secret image into 1-D encoded bit stream.

3. MODIFIED APPROACH

In [6] at embedding DCT coefficient of cover image is firstly converted into binary form and then just replacing a LSB of coefficient with hcode and then convert back to decimal. After that at the same time (Embedding) they are also embedding a Huffman table into cover image. After doing this they take Block IDCT stego image. While doing this process of converting decimal DCT coefficient to binary and then after LSB replacement convert binary to decimal will increase the computational complexity and second thing they are embedding dictionary which was reduce the capacity of cover image of carrying more secret information.

In our approach to understand doing binarization (converting decimal to binary and binary to decimal) we can using ±1 embedding method i.e. DCT coefficient is even and hcode bit is odd then increasing DCT coefficient value by 1 (i.e. +1). If DCT coefficient is odd and hcode is 0 hence we are reducing value of DCT coefficient by 1 (i.e. -1). This will reduce computation and second thing instead of inserting of embedding dictionary into cover image. We are inserting a symbol and its probabilities to the image are at the time of extracting search image. We are get symbol and probabilities back and by using that create Huffman dictionary at receiver and by using Huffman dictionary and extracting hcode can recover the secret image.

3.1 Generation of Stego Image

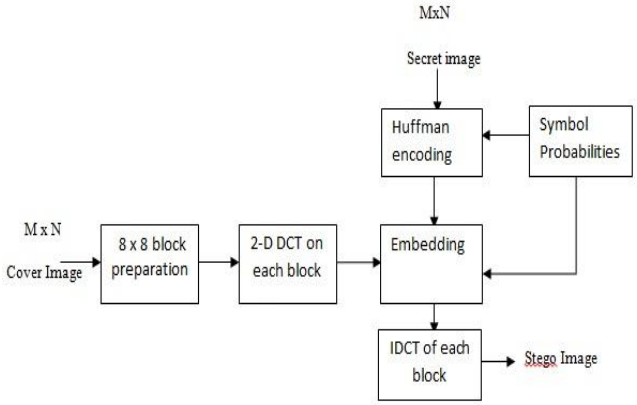

Fig 1: Generation of Stego Image

The block diagram of generation of stego image shows the cover image M X N applies to 8 X 8 preparation block. In this stage carrier image (Cover Image) divided into non overlapping blocks of size 8 X 8. In next stage apply DCT on each block of cover image. After applying DCT to get DCT coefficient of cover image. In other hand take a secret image and applying Huffman encoding using Huffman table that produce hcode bit steam of secret image. At embedding stage embedded hcode of secret image and probabilities into cover image. Then taking IDCT of embedding image to get stego image.

3.2 Extraction of Secret Image

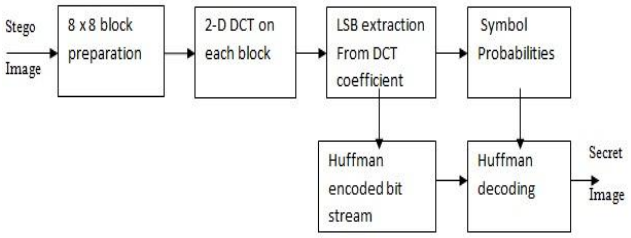

Fig 2: Extraction of Secret Image

At receiver stego image divided into non overlapping block of size 8×8 then applied DCT on each 8×8 block. After DCT of stego image using LSB extraction to get Huffman encoded bit stream and probabilities. To the help of probabilities produce Huffman table. These hcode bit stream and Huffman table applied to the Huffman decoding block to get secret image. In next chapter we discuss experimental setup and obtained result.

4. IMPLEMENTATION AND PERFORMANCE EVALUATION

This section observed some experiments of proposed method. The proposed method has been simulated using the MATLAB 7.8.0 program on windows 7 platform. Fig shows the cover images and secret image.

Here we are using 512×512 size of cover image and 154×154 size of secret image. As per previous discussion the size of secret image very less than cover image so that to get maximum security.

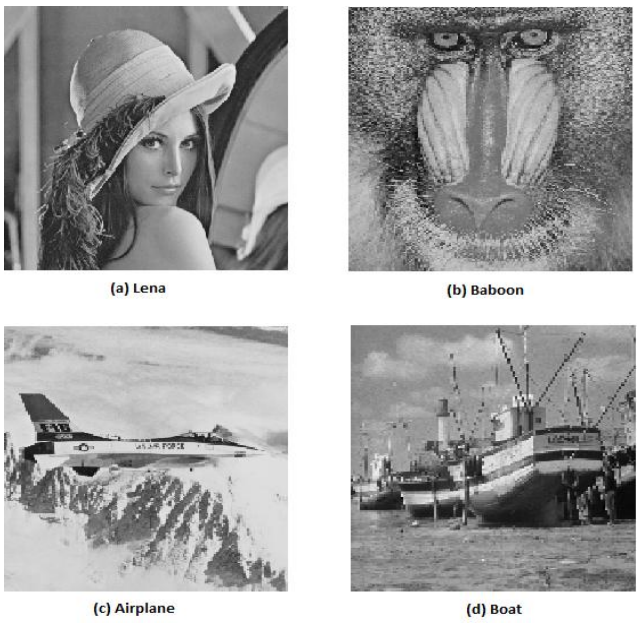

Fig 3: Cover Image

Fig 4: Secret Image

4.1 PSNR (Peak Signal to Noise Ratio)

The peak signal to noise ratio (PSNR) is used for to evaluate the image quality of cover image and stego image.

$$PSNR = 10\ log_{10}\ \frac{255^2}{MSE}\ dB \qquad (4)$$

Where

$$MSE = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}(f(x,y) - g(x,y))^2\ /N^2 \qquad (5)$$

Where f(x, y) and g(x, y) mean the pixel value at the position (x, y) in the cover image and the stego image respectively [6]. PSNR is larger to get more image quality. It is expressed in dBs.

Table 1. PSNR of Cover Image and Stego Image.

Cover Image	DCT Block size 8 X 8	DCT Block size 16 X 16
Lena	51.6818	42.0498
Baboon	49.9238	42.5163
Airplane	51.9926	41.4864
Boat	51.5928	50.9856

4.1 Correlation Coefficients

The correlation coefficient matrix represents the normalized measure of the strength of linear relationship between variables [7]. The correlation coefficient $r_{X\,Y}$ between two random variables X and Y with expected values μ_X and μ_Y and standard deviations σ_X and σ_Y is their covariance normalized by their standard deviations, as follows

$$r_{X\,Y} = \frac{cov(X,Y)}{\sigma_X\,\sigma_Y} = \frac{E((X-\mu X)(Y-\mu Y)}{\sigma_X\,\sigma_Y} \qquad (6)$$

Where E is the expected value operator and cov means covariance.

Since μX = E(X), σX2 = E(X2) − E2(X). (7)

Our proposed method gives better correlation coefficient as previous methods. It is nearly 1 so which is gives better image quality.

Table 2. Correlation Coefficient of Cover Image and Stego Image.

Cover image	DCT Block size 8 X 8	DCT Block size 16 X 16
Lena	0.9999	0.9991
Baboon	0.9998	0.9988
Airplane	0.9999	0.9999
Boat	0.9999	0.9998

5. CONCLUSIONS

In this paper, proposed a modified approach of image steganography process in frequency domain with higher three layer security and quality of image is better than previous method. According to simulation result stego image is identical to cover image. This method gives better PSNR and correlation coefficient result. Embedding of secret image into cover image without Huffman table reduce secret data only probabilities inserted. Transform cover image spatial domain to frequency domain at other side converting secret image into Huffman encoded bit. These operations keep the secret images away from unauthorised user and hence this method robust against attacks.

6. ACKNOWLEDGEMENT

I would like to thank Prof. Vaishali S. Jabade. Without her enthusiasm and support, this paper would not have been completed. I would also like to send a special thanks to my family and friends for their encouragement and support.

7. REFERENCES

[1] Krenn J. R. 2004, "Steganography and Steganalysis ", http://www.krenn.nl/univ/cry/steg/article.pdf.

[2] Wang Huaiqing & Wang Shuozhong 2004, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, Vol. No 47, Issue. No 10, pp 72-82.

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

[4] Weiss M. 2012, "Principles of steganography", http://www.math.ucsd.edu/~crypto/Projects/MaxWeiss/steganography.pdf.

[5] Ying Wang and Pierre Moulin 2003, "Steganalysis of Block-DCT Image Steganography", IEEE workshop on Statistical Signal Process.

[6] A.Nag, S. Biswas, D. Sarkar, P.P. Sarkar 2010, " A novel technique for Image Steganography based on Block-DCT and Huffman Encoding", International Journal of Computer Science and Information Technology Vol. No 2, Issue. No 3, pp 103-112.

[7] K.D. Chinchkhede, Govind Sharan Yadav, S.R Hirekhan, D.R Solanke 2011, " On the Implementation of FIR Filter with Various Windows for Enhancement of ECG signal," International Journal of Engineering Science and Technology, Vol. No 3, Issue. No 3, pp. 2031-2040.

[8] N. Provos and P. Honeyman 2003, "Hide and Seek: An Introduction to Steganography", IEEE: Security & Privacy, Vol. No 1, pp 32-44.

[9] Fridrich, J. 2010, "Steganography in Digital media: Priciples, Algorithms and Applications," Cambride University Press.

[10] Lisa M. Marvel, Charles G. Boncelet, Jr., and Charles T. Retter 1999, "Spread Spectrum Image Steganography," IEEE Transactions on Image Processing, Vol. No 8, Issue. No 8, pp. 2031-2040.