EMBEDDING INFORMATION IN DCT COEFFICIENTS BASED ON AVERAGE COVARIANCE

Article *in* International Journal of Engineering Science and Technology · April 2011

CITATIONS
7

READS
413

4 authors:

Sathisha Narayanappa
Government S.K.S.J.T. Institute of Technology
11 PUBLICATIONS **33** CITATIONS
SEE PROFILE

Kasukurthi Suresh Babu
PACE Institute of Technology and Science
5 PUBLICATIONS **15** CITATIONS
SEE PROFILE

Raja K B
University Visvesvaraya College of Engineering
188 PUBLICATIONS **1,340** CITATIONS
SEE PROFILE

Lalit M Patnaik
Indian Institute of Science
836 PUBLICATIONS **8,645** CITATIONS
SEE PROFILE

EMBEDDING INFORMATION IN DCT COEFFICIENTS BASED ON AVERAGE COVARIANCE

N SATHISHA*

Department of Electronics and Communication Engineering.
R L Jalappa Institute of Technology, Doddaballapura, Bangalore Rural Dist. 561 203, India.

K SURESH BABU, K B RAJA, VENUGOPAL K R

Department of Computer Science and Engineering,
University Visvesvaraya College of Engineering, Bangalore University, Bangalore 560 001, India.

L M Patnaik

Defence Institute of Advanced Technologies, Pune, India.

Abstract:

The steganography is a covert communication to transfer confidential information over an internet. In this paper we propose Embedding Information in Discrete Cosine Transform Coefficients based on Average Covariance (EIDCT) algorithm. The Average Covariance of the Cover Image (ACCI) is computed and 0.15 is considered as the threshold value. The cover image is segmented into 8*8 cells and Discrete Cosine Transform (DCT) is applied to derive coefficients. The Most Significant Bits (MSBs) of payload are embedded into the cover image based on ACCI and DCT coefficients. It is observed that the capacity, Peak Signal to Noise Ratio (PSNR) and Security is better compared to the existing algorithm.

Keywords: Covariance, Cover Image, DCT, Payload, Steganography

1. Introduction

With the rapid development of information technology, security for the confidential information has become challenging issue today. Steganography techniques have been developed in order to achieve the security. Steganography is an art and science of hiding secret information into multimedia such as images, audios or text. The stegomedia is similar to the cover media hence it is difficult for the hackers to detect the existence of secret message on the cover media. The hidden secret information can be extracted by retrieving algorithm. Image steganography has become an essential and potential field in information hiding for protecting the confidential information.

The three important requirements need to be considered for steganographic model [1] are (i) Imperceptibility: means to preserve the details of the cover image when the secret information is being embedded. (ii) Payload capacity: means the maximum number of bits that can be hidden with an acceptable resultant stegoimage quality. (iii) Robustness: is the ability of stegoimage to retain its contents from attacks. The steganography techniques are broadly classified into two categories viz., (i) spatial domain and (ii) frequency domain. In spatial domain the secret information is directly embedded into the pixels of the cover image by LSB replacement. In frequency domain the cover image is transformed into coefficients such as Discrete Fourier Transform (DFT) [2], Discrete Cosine Transform [3], Discrete Wavelet Transform (DWT) [4], Integer Wavelet Transform (IWT) [5] etc., and the secret data to be embedded may be in spatial domain and/or frequency domain. The frequency domain embedding process is more secure than the spatial domain. Many types of images have been used as cover media like Bitmap File Format (BMP), Joint Photographic Experts Group (JPEG), and Graphics Interchange Format (GIF) images [6], JPEG is the common image format for internet and local usage, since it provides large compression ratio and maintains high image quality.

Steganography is employed in various applications like copy right control of materials, enhancing robustness of image search engines and smart identity cards, video-audio synchronization, protection of intellectual property, exchange of highly confidential data in a covert manner and bank transactions.

Motivation:

The internet allows exchange of information over large areas viz., Science, Technology, Arts, Law, Management etc., throughout the world. The information such as National Security issues, Personnel information and other important confidential data can't be sent through the internet as it attracts the attention of hacker's confidential issues. To solve this problem, the cryptography technique can be used to send the secret information but the hackers get suspicious of some information and may decrypt. The alternative method to avoid suspicion on scrambled data, the steganography is proposed, wherein the secret information is embedded into the cover object without disturbing much of its statistical characteristics. Steganalysis is used to retrieve the secret information. Hence we motivated to generate better steganographic algorithm, so that the steganalysis fails to identify the stego object.

Contribution:

In this paper we presented EIDCT that hides secret information in the frequency domain using DCT by calculating the average covariance of the cover image which results in increase of the security and capacity.

Organization:

This paper is organized into following sections. Section 2 is an overview of related work. The steganography model and Evaluation parameters are described in section 3. Section 4 discusses the algorithms used for embedding and extracting process. Performance analysis is discussed in section 5 and conclusion is discussed in section 6.

2. Related Work

Raja et al., [7] proposed a high capacity, secure steganographic algorithm in which the payload bits are encrypted and embedded in the wavelet coefficients of the cover image. The method utilizes the approximation band of the wavelet domain to improve robustness. Radovan Ridzon et al., [8] presented a technique of hiding secret information in still image. The digital water marking, DCT coefficients flipping and cryptography are discussed. Khalid Negrat et al., [9] proposed a multiple frequency domain steganography, Discrete Wavelet Transform (DWT) with DCT techniques are applied sequentially on the cover image Huffman encoding dictionary translation code for character of the secret information is used to improve the capacity. Security is improved using encrypted stego key and secret message by encoding. Adel Almohmmad et al., [10] proposed methods for optimizing the JPEG quantization table. JPEG optimized quantization table significantly improves the quality of stego images. Two least significant bits are of each middle frequency coefficients of 16x16 quantization DCT block are modified to embed two secret bits.

Masoud Afrakhteh and Subariah Ibrahim [11] developed an adaptive more surrounding pixels technique which utilizes all eight adjacent neighbor pixels for embedding secret information so that imperceptibility value grows. Mehdi Hussain and Mureed Hussain [12] presented a pixel intensity based high capacity data embedding method. The method improves the modified kekre's algorithm which is based on LSB method. The capacity is improved by embedding the payload into the low intensity pixels and hence maximum utilization of cover image. Fangjun Huang et al., [13] presented an experimental study on the security performance of Steganographic scheme. The study reports on steganography scheme security performance with different input images i. e., compressed images and JPEG compressed images. Steganography scheme performance compared with two other JPEG steganography scheme MB1 and F5. Divya Sharma et al., [14] proposed a robust and secure Steganographic algorithm using a combination of audio and visual steganography to provide two level security. The first stage involves the use of a waveform audio format file as medium to embed the secret text message, the second stage uses a JPEG image as medium for embedding the bit stream obtained in stage one. Saeed sarreshtedri et al., [15] proposed an efficient LSB method for embedding the secret information and transforming the stego image to frequency domain. The secret information is hidden in spatial domain and the stego image is transformed and quantized to enhance the security. Yifeng Lu et al., [16] developed a steganographic algorithm which improves security in LSB matching process. The distortion in the stego image of one dimensional histogram is minimized based on Cachins theory. Hung and ouyang [17] proposed a method to find appropriate regions in a cover image to embed the payload. The number of neighbor pixels is counted

only the neighbor pixels value with small difference is considered for LSB embedding method. Stanescu et al., [18] presented a segment compression steganographic algorithm. The input data is first compressed using the Karhunen Loeve transform to achieve higher concealing capacity and then hide the LSB of secret data in cover media. Vijay kumar and Dinesh kumar [19] has presented a performance evaluation of Discrete Wavelet Transforms (DWT). The cover image is divided into four sub images such as Approximation Coefficients (CA) Vertical detail Coefficients (CV) Horizontal detail Coefficients (CH) Diagonal detail Coefficients (CD), similarly the secret image is also divided into four sub images. The error blocks are calculated by subtracting the approximation coefficients of cover image from approximation coefficients of secret image. These blocks are replaced with the best matched CH blocks. They made use of CV and CD blocks also to embed the secret images. Nan-I Wu and Min-Shiang Hwang [20] developed steganographic techniques for gray scale images and introduced a high hiding capacity scheme and high stego-image degradation imperceptibility scheme. These schemes provide high imperceptibility and data hiding capabilities.

3. Proposed EIDCT Model

The proposed embedding, retrieval model and evaluation parameters are discussed in this section.

3.1 EIDCT Embedding Model: The block diagram of proposed embedding model is shown in the Figure 1. The number of cover image bits are replaced by the MSBs of payload based on ACCI of cover image, which results in better stego image with reasonable PSNR for any kind of cover image. The payload is secure from intruder as the number of cover image DCT coefficient bits are replaced on the basis of ACCI and DCT coefficient values.

(i) Cover Image: The cover image is color or gray scale of any size and any format. If the cover image is color then convert into gray scale image. The gray scale image f(x, y) is converted into M rows and N columns with discrete coordinates x and y pixel intensity values of image is represented in the following matrix form

$$f(x,y)=\begin{bmatrix} f(0,0) & f(0,1) & \dots\dots & f(0,N-1) \\ f(1,0) & f(1,1) & \dots\dots & f(1,N-1) \\ \dots & \dots & & \dots\dots\dots \\ f(M-1,0) & f(M-1,1) & \dots\dots & f(M-1,N-1) \end{bmatrix}$$

more precisely this is represented as

$$A=\begin{bmatrix} a_{0,0} & a_{0,1} & \dots\dots & a_{0,N-1} \\ a_{1,0} & a_{1,1} & \dots\dots & a_{1,N-1} \\ \dots & \dots & & \dots\dots \\ a_{M-1,0} & a_{M-1,1} & \dots\dots & a_{M-1,N-1} \end{bmatrix}$$

Clearly $a_{i,j} = f(x = i, y = j)$

(ii) Cover Image Pixel Adjustment: The gray scale cover image pixel intensity values vary from lower zero to upper 255 values. During the payload embedding process the lower and higher intensity values of cover image may exceed and which results in difficulty to retrieve the payload at the destination. Hence the cover image pixel intensity values are limited to lower 15 and upper 240, instead of zero and 255.

(iii) Covariance and Average Covariance [21]: The covariance cov (x, y) between two random variables x and y with expected values μ_x and μ_y is calculated using the Equation (1)

$$\text{cov}(x, y) = E[(x - \mu_x)(y - \mu_y)] \quad \dots\dots \quad (1)$$

The correlation coefficients $\rho_{x,y}$ between two random variables x and y with standard deviations σ_x and σ_y is calculated using the Equation (2)

$$\rho_{x,y} = \frac{\text{cov}(x,y)}{\sigma x\, \sigma y} = \frac{E[(x - \mu x)(y - \mu y)]}{\sigma x\, \sigma y} \quad \dots\dots \quad (2)$$

The average covariance is calculated by adding the correlation coefficients of the cover image and then dividing the sum by the size of the matrix. The threshold value of average covariance of cover image is fixed at 0.15 by trial and error method.

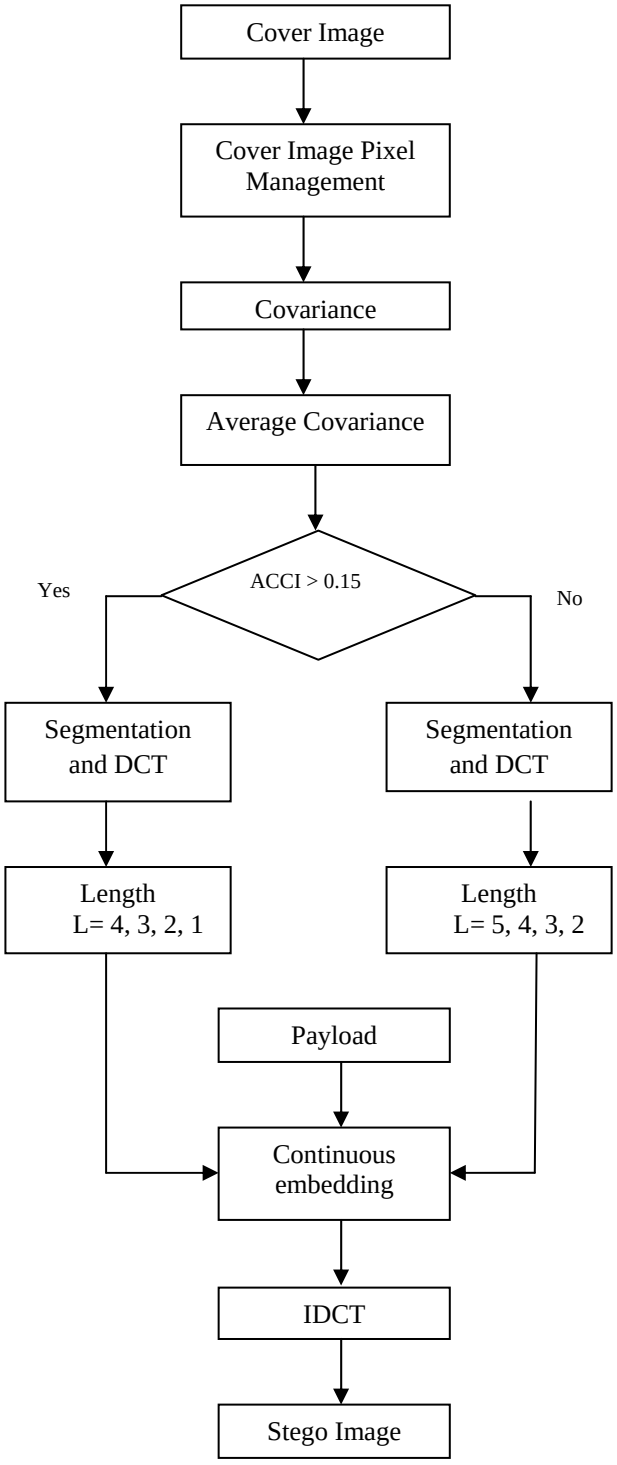

Fig. 1: EIDCT Embedding Flowchart

(iv) Segmentation and DCT: The cover image matrix is segmented into 8x8 matrices. The DCT is applied on each 8x8 block to get DCT coefficients which are used to hide the payload depending on the adaptive length *L*. The frequency domain improves the security and robustness during communication of payload. The description of the two-dimensional DCT [22] for an input image *F* and an output image *T* is calculated using Equation (3)

$$T_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \mathrm{F_{mn}} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N} \ldots\ldots\ldots (3)$$

Where, $0 \le p \le M-1$
$0 \le q \le N-1$
and

$$\alpha_p = \begin{cases} 1/\sqrt{M}, p = 0 \\ \sqrt{2/M}, 1 \le p \le M-1 \end{cases} \quad \alpha_q = \begin{cases} 1/\sqrt{N}, q = 0 \\ \sqrt{2/N}, 1 \le q \le N-1 \end{cases}$$

Where *M, N* are the dimensions of the input image while *m, n* are variables ranging from *0* to *M-1* and *0* to *N-1* respectively.

(v) Variable bit length L: After converting the 8x8 matrices into the frequency domain, pixel values of the cover image are transformed to DCT coefficients (Co). The length *L*, which determines the number of LSBs of each coefficients of cover image to be replaced by the payload bits, is calculated according to the conditions given below.

If Average Covariance of Cover Image (ACCI) > 0.15

If $Co \ge 2^5$; L=4

If $2^5 \le Co \ge 2^4$; L=3

If $2^4 \le Co \ge 2^3$; L=2

Else L=1

Else

If $Co \ge 2^5$; L=5

If $2^5 \le Co \ge 2^4$; L=4

If $2^4 \le Co \ge 2^3$; L=3

Else L=2

(vi) Embedding: Four MSBs of each payload pixel are embedded into the segmented 8x8 cover image DCT coefficients in a continuous manner. After embedding the payload into each cover image block the 8x8 stego coefficient matrix is obtained.

(vii) Inverse Discrete Cosine Transform (IDCT) and Stego image: The 8x8 stego coefficient matrix is converted into the spatial domain by applying IDCT. The all 8x8 spatial domain matrix are arranged in a proper way to obtain stego image which is equivalent to the cover image.

3.2 EIDCT Retrieval Technique: The payload is extracted from the stego image in the retrieval technique is shown in the Figure 2.

(i) Stego image: The stego image is received at the destination over the open channel. Any intruder interfering in the transmission process will only be able to read the stego image and cannot extract the secret image.

(ii) Covariance: The covariance and average covariance of the stego image matrix is calculated. Based on the value of the average covariance the number bit length *L* is calculated at the receiver.

(iii) Segmentation and DCT: the stego image is converted into 8x8 blocks to ensure faster computation of DCT coefficients.

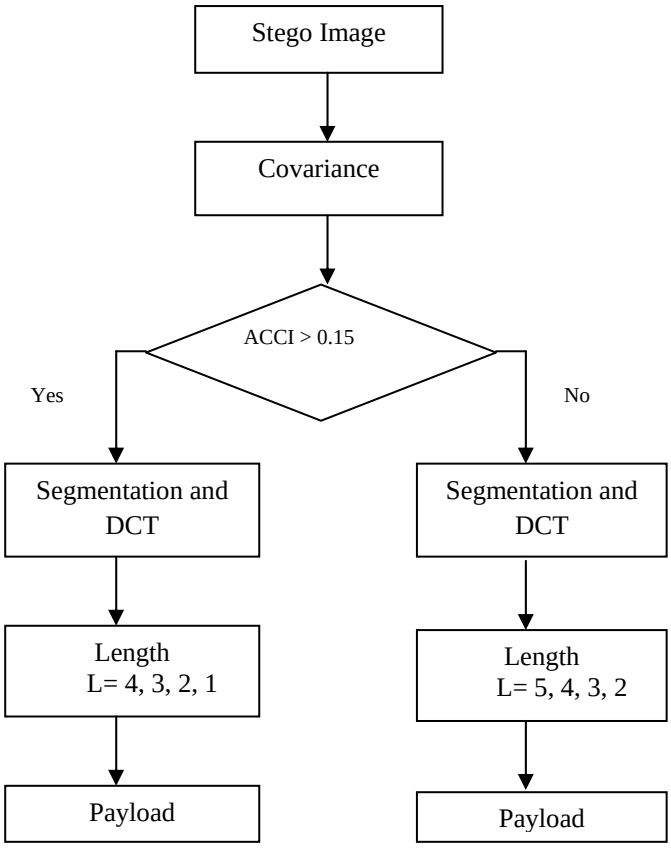

Fig. 2: EIDCT Retrieval Flowchart

(iv) Length L: At the receiver *L* is calculated for the stego image using the procedure as adopted in the embedding process to extract payload.

(v) Payload: The extracted payload bits are rearranged in a proper way to get the payload.

3.3 Evaluation Parameters:

(i) *Mean Square Error (MSE):* It is defined as the square of error between cover image and stegoimage. The distortion in the image can be measured using MSE. It is calculated using Equation

$$MSE = \left[\frac{1}{N * N}\right]^2 \sum_{i=1}^{N}\sum_{j=1}^{N}\left(X_{ij} - \bar{X}_{ij}\right)^2$$

Where:

X_{ij}: The value of the pixel in the cover image.
$\bar{X}_{ij}$: The value of the pixel in the stego image.
N: Size of Image.

(ii) Peak Signal to Noise Ratio (PSNR*):* It is the measure of quality of the image by comparing the cover image with the stegoimage, i.e. it measures the percentage of the stegano data to the image percentage. PSNR is calculated Equation 8.

$$PSNR = 10log_{10}\frac{255^2}{MSE}db$$

(iii) Capacity: It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The steganographic embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. Capacity is represented by bits per pixel (bpp).

4. Algorithm

Problem definition: Given a cover image and payload, the objectives are

(i) The payload is to be embedded into the cover image to derive stegoimage using average covariance, DCT and variable payload bit stream.
(ii) The stego image with reasonable PSNR.

Assumptions:

(i) The cover and payload objects are images with different dimensions and formats.
(ii) The stego object is transmitted over an ideal channel.

The payload is embedded into the cover image DCT coefficients based on average covariance of cover image and the values of DCT coefficients is given in the Table 1.

Table 1: Algorithm of EIDCT

Input: Cover Image and Payload.

Output: Stego Image.

Step 1) A cover image of any size and format is considered and if it is color image convert it into grayscale image.
Step 2) Applying pixel management to the cover image to avoid overflow and underflow of the pixel values 0 and 255.
Step 3) Covariance of cover image is determined and average is computed to get average covariance.
Step 4) The average covariance of cover image value is fixed as 0.15, if ACCI > 0.15 go to step 5 else step 6
Step 5)
(i) The cover image is segmented into 8*8 matrix and DCT is applied on each matrix.
(ii) Embedding bit length *L* for each coefficient is calculated as following:
L=4, if $Co \geq 2^5$;
L=3, if $2^4 \leq Co \leq 2^5$;
L=2, if $2^3 \leq Co \leq 2^4$;
else L=1;
(iii) Depending on the value of *L* the number of bits of cover image DCT coefficients are replaced by the MSB bits of payload.
(iv) The stego image obtained in the DCT domain is converted back to the spatial domain using IDCT.
Step 6)
(i) The cover image is segmented into 8*8 matrix and DCT is applied on each matrix.
(ii) Embedding bit length L for each coefficient is calculated as following:
a. L=5, if $Co \geq 2^5$;
b. L=4, if $2^4 \leq Co \leq 2^5$;
c. L=3, if $2^3 \leq Co \leq 2^4$;
d. else L=2;
(iii) Depending on the value of *L* the number of bits of cover image DCT coefficients are replaced by the MSB bits of payload.
(iv) The stego image obtained in the DCT domain is converted back into the spatial domain using IDCT.

5. Performance Analysis

For the performance analysis payload image of Boat and the cover images Lena, Old Image, Baboon, Barbara, Ranch House, Bridge and Casa are considered and shown in the Figure 3. The average covariance of cover image is calculated and the payload bits are embedded into the cover image depending on the ACCI.

The payload is embedded into the DCT coefficients of cover image based on ACCI and length L. The performance parameter such as PSNR between cover image and stegoimage is computed and given in the Table 2. It is observed that the PSNR depends on the ACCI of the cover image and also the PSNR decreases as the Hiding Capacity (HC) increases. The PSNR value is maintained around 42 dB for the capacity of 34%.

The graph shown in Figure 4 gives the PSNR for different capacity values of two sets of images. In first set Lena is used as cover image and in the second set Barbara as the cover image. In both the sets Boat is taken as the payload. The graph also depicts the quality of the stego image which is determined by PSNR not only depends on the algorithm but also on the images used. Using Barbara as cover image gives higher PSNR.

(a) Lena

(b) Old Image

e) Ranch House.

(f) Bridge

(g) Casa

(h) Boat

Fig. 3: (a) to (g) are Cover images and (h) Payload

Table 2: ACCI and PSNR for different cover images with payload boat

Cover Image	**ACCI**	**H C 12.5%**	**H C 20.0%**	**H C 25.0%**	**HC 34.0%**
		PSNR	**PSNR**	**PSNR**	**PSNR**
Lena	0.064	46.31	41.51	40.51	39.41
Old image	0.122	45.41	41.95	40.85	39.09
Baboon	0.154	47.25	42.64	41.88	40.71
Barbara	0.203	47.08	43.48	42.54	41.17
Ranch House	0.280	46.06	41.50	40.46	39.20
Bridge	0.358	46.13	41.78	40.96	39.69
Casa	0.504	47.56	43.33	42.57	41.35

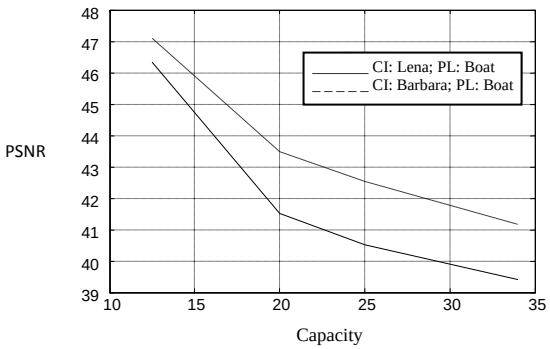

Fig. 4: PSNR for different capacity

The Maximum Hiding Capacity (MHC) and the PSNR between the cover image and stego image is tabulated for existing algorithm *An Adaptive Steganographic Technique Based on Integer Wavelet Transform (ASIWT)* [23] and the proposed algorithm EIDCT is given in the Table 3. It is observed that the PSNR is improved in the proposed algorithm compared to the existing algorithm.

Table 3: PSNR of existing and proposed techniques for a MHC of 47%

Image	Existing Method (ASIWT)	Proposed Method (EIDCT)
	PSNR	PSNR
CI: Lena PL: Barbara	31.80	39.35
CI: Baboon PL: Cameraman	30.89	37.96

6. Conclusion And Future Work

The steganography is used to transfer secret message over open channel. In this paper EIDCT is proposed. The cover image covariance is computed to consider number of MSBs of payload to be embedded based on DCT coefficients. The cover image is divided into 8*8 cells and converted into DCT coefficients to determine the length of the payload bits to be embedded into the cover image. It is observed that the capacity, security and the PSNR values are improved compared to the existing algorithm. In future the same technique can be extended by applying different transforms to both cover image as well as payload and thus the robustness of algorithm can be verified.

References

[1] Hanizan Shanker Hussain, Syed Ahmad Aljunid, Saadiah Yahya and Fakariah hani Mohd Ali, “A Novel Hybrid Fuzzy SVM Image Steganographic Model,” International Symposium in Information Technology, pp. 1 – 6, 2010.

[2] Debnath Bhattacharyya, Jhuma Dutta, Poulami Das, Rathit Bandopadhyaay, S K Bandyopadhyay and Tai hoon Kim, “Discrete fourier Transformation based Image Authentication Technique,” Eighth International Conference on Cognitive Informatics, pp. 196 – 200, 2009.

[3] Qiudong Sun, Yongping Qiu, Wenxin Ma, Wenying Yan and Hong Dai, “Image Steganography Based on Sub band Coefficient Adjustment in BDCT Domain,” International Conference on Multimedia Technology, pp. 1 – 4, 2010.

[4] Paul Bao and Xiaohu Ma, “Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition,” IEEE Transactions on Circuits and Systems for Video Technology, Vol. 15. pp. 96 – 102, January 2005.

[5] K. B. Raja, S. Sindhu, T. D. Mahalakshmi, S. Akshatha, B. K. Nithin, M. Sarvajith, K. R. Venugopal and L. M. Patnaik, “Robust Image Adaptive Steganography using Integer Wavelets,” Third International conference on Communication Systems Software and Middleware and Workshops, pp. 614 -621, January 2008.

[6] Adel Almohammad and Gheorghita Ghinea, “Image Steganography and Chrominance Components,” IEEE International Conference on Computer and information Technology, pp. 996 – 1001, 2010

[7] K. B. Raja, Vikas, Venugopal K. R and L. M. Patnaik, “High Capacity Lossless Secure Image Steganography using Wavelets,” International Conference on Advances Computing and Communications, pp. 230 – 235, 2006.

[8] Radovan Ridzon, Dushan Levisky and Tomas Kanocz, "Information Hiding within Still Images Based on the DCT Coefficients Flipping and Encryption," Fifty Second International Symposium, pp. 147 – 150, September 2010.
[9] Khalid Negrat, Raoof Smko and Abdelsalam Almarimi, "Variable Length Encoding in Multiple Frequency Domain Steganography," Second International Conference on Software Technology and Engineering, pp. 305 – 309, 2010.
[10] Adel Almohammad, Gheorghita Ghinea and Robert M Hierons, "JPEG Steganography a Performance Evaluation of Quantization tables," International Conference on Advance information Networking and Applications, pp. 471 – 478, 2009.
[11] Masoud Afrakhteh and Subariah Ibrahim "Adaptive Steganography scheme using More Surrounding pixels," International Conference on Computer Design and Applications, pp. 225-229, 2010.
[12] Mehdi Hussain and Mureed Hussain, "Pixel Intensity Based High Capacity Data Embedding Method," International Conference on Information and Emerging Technologies, pp. 1 – 5, 2010.
[13] Fangjun Huang, Jiwu Huang and Yun Qing Shi, "An Experimental Study on the Security Performance of YASS," IEEE Transactions on Information Forensics and Security, Vol. 3, pp.374 – 380, September 2010.
[14] Divya Sharma, Abha Tripathi and Agam Gupta, "A Two Level Message Adaptive Steganographic Approach," International Conference on Advances in Computer Engineering, pp.139 – 143, 2010.
[15] Saeed Sarreshtedari, Mohsen Ghotbi and Shahrokh Ghaemmaghami, "On the Effect of Spatial to Compressed Domains Transformation in LSB based Image Steganography," International Conference on Computer Systems and Applications, pp. 260 – 264, 2009.
[16] Yifeng Lu, Xiaolong Li and Bin Yang, "A 1 –based Steganography by Minimizing the Distortion of First Order Statistics," Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 754 – 758, 2009.
[17] Qinhua Huang and Weimin Ouyang, "Protect Fragile Regions in Steganography LSB Embeddeing," International Symposium on Knowledge Acquisition and Modeling. pp 175 – 178, 2010
[18] Daniela Stanescu, Ioan Gabriel Bucur and Mircea Stratulat, "Segment Compression Steganograhic Algorithm" International Joint Conference on Computational Cybernetics and Technical Informatics Communications, pp. 349 – 354, May 2010.
[19] Kumar V and Kumar D, "Performance Evaluation of DWT based Image Steganography," Second IEEE International Conference on Advance Computing, pp. 223 – 228, 2010.
[20] Nan-I Wu and Min-Shiang Hwang, "Data Hiding: Current Status and Key Issues," International Journal of Network Security, Vol. 4. No.1, pp.1-9, January 2007.
[21] Souvik Bhattacharyya and Gautam Sanyal, "A Data Hiding Model with High Security Features Combining finite State Machines and PMM Method," International Journal of Electrical and Computer Engineering, pp. 78 – 85. 2010.
[22] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods," Journal of Signal Processing, Vol. 90, Issue 3, pp. 727 – 752, March 2009.
[23] R. O. El Safy, H. H. Zayed and A. El Dessouki, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform," IEEE Proceedings on International Conference on Networks and Media, pp. 111 – 117, March 2009.

N Sathisha received the BE degree in Electronics and Communication Engg. from Bangalore University and the MTech degree in Digital Communication and Networking from Visvesvaraya Technological University, Belgaum. He is pursuing Ph.D. in Computer Science and Engineering of Bangalore University under the guidance of Dr. K Suresh Babu, Assistant Professor, Department of Electronics and Communication Engineering, University Visvesvaraya College of Engineering. He is currently an Assistant Professor, Dept. of Electronics and Communication Engineering, R L Jalappa Institute of Technology, Doddaballapur. His research interests include Image processing, information security and computer networks. He has 02 research publications in refereed International Conference Proceedings. He is a life member of Indian Society for Technical Education, New Delhi. He is a life member of Institute of Electronics and Telecommunication Engineers, New Delhi.

K Suresh Babu is an Assistant Professor, Dept. of Electronics and Communication Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his BE and ME in Electronics and Communication Engineering from University Visvesvaraya College of Engineering, Bangalore. He was awarded Ph.D. in Computer Science and Engineering from Bangalore University. He has over 10 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Biometrics, Signal Processing,

K B Raja is an Assistant Professor, Dept. of Electronics and Communication Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his BE and ME in Electronics and Communication Engineering from University Visvesvaraya College of Engineering, Bangalore. He was awarded Ph.D. in Computer Science and Engineering from Bangalore University. He has over 60 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Biometrics, VLSI Signal Processing, computer networks

K R Venugopal is currently the Principal, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science, Bangalore. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored 27 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ etc. He has been serving as the Professor and Chairman, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. During his three decades of service at UVCE he has over 250 research papers to his credit. His research interests include computer networks, parallel and distributed systems, digital signal processing and data mining.

L M Patnaik is the Vice Chancellor, Defence Institute of Advanced Technology (Deemed University), Pune, India. During the past 35 years of his service at the Indian Institute of Science, Bangalore, He has over 550 research publications in refereed International Journals and Conference Proceedings. He is a Fellow of all the four leading Science and Engineering Academies in India; Fellow of the IEEE and the Academy of Science for the Developing World. He has received twenty national and international awards; notable among them is the IEEE Technical Achievement Award for his significant contributions to high performance computing and soft computing. His areas of research interest have been parallel and distributed computing, mobile computing, CAD for VLSI circuits, soft computing, and computational neuroscience.