An Optimized Trade-off Decomposition Steganography Algorithm

Mazhar Tayel
Electrical Engineering Department
Faculty of Engineering
Alexandria University

Hamed Shawky
Electrical Engineering Department
Faculty of Engineering
Alexandria University

ABSTRACT

In this paper a modified Steganography algorithm is proposed. A fuzzification is performed in the message channel to compress the decomposed coefficients before embedding in the cover-image to get a new Stego-image. A relative embedding strength factor (ESF) is used for embedding the secret in the cover-image. The well known metrics (MSE, PSNR, Cor. and Entropy) were used to evaluate quality of the modified algorithm. Also, the trade-off factor was introduced to determine an optimum value for the ESF to get an acceptable degradation in the Stego-image. In addition, the reconstruction algorithm mentioned in previous paper was modified using the optimum value of the ESF. Comparisons show improved results w.r.t. other algorithms.

Keywords

Steganography, Cover-image, Secret-message, Decomposition, Fuzzy set

1. INTRODUCTION

There are two common types of image Steganography: Spatial domain and transform domain. The Spatial domain embeds secret-message in pixels of image intensity directly. The main advantage of this method is simple and fast but it has less capability towards signal processing and/or noise. The Transform domain is a frequency decomposition domain, that characterized by : high security, hard to detect, more flexible, and efficient technique for denoising. [1— 7].

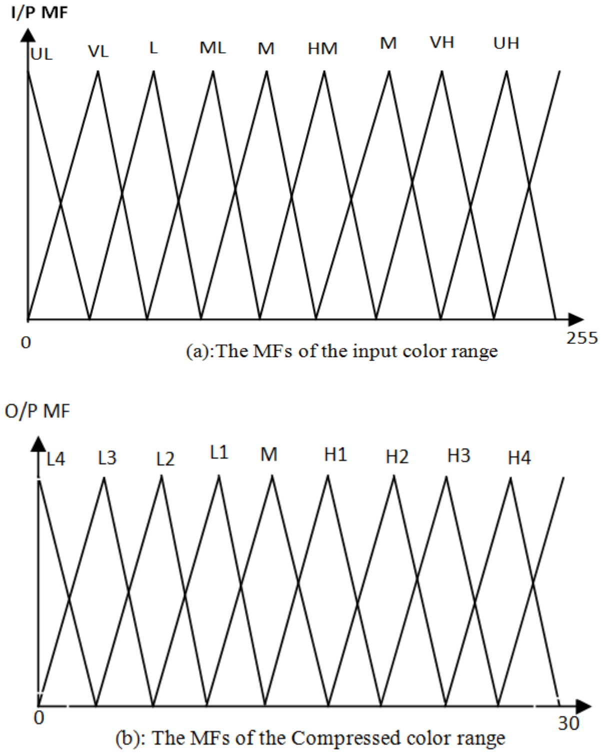
This paper introduces a modified algorithm able to perform Steganography, using decomposition technique for both secret-message and cover-image at the same time, and to introduce a method to determine the most probable value of the ESF for accepted vision of the Stego-image.

2. THE PROPOSED ALGORITHM

The aim of this algorithm is to hide secret-message coefficients in a cover image without perceptible degrading of cover-image quality and to provide better resistance against steganalysis process. The proposed algorithm is composed of two channels namely: cover-image channel and secret-message channel that are used to embed the decomposed coefficients together.

2.1 Fuzzy Optimization

A fuzzy set is completely characterized by its membership function (MF). Figure (1, a & b) shows the membership functions for fuzzification of the input and output secret message. Using nine triangular membership functions to compress the secret-image from (0 — 255) to (0 — 30) image color range. Then embedding into the cover image to obtain a uniformly diffused distribution of message pixels all over the cover image.



(a):The MFs of the input color range

(b): The MFs of the Compressed color range

Fig. 1. The MFs of the fuzzified input and compressed color range for the secret image

2.2 Image decomposition

The fuzzified secret-message and the cover-image are decomposed and then embed the coefficients together, The DCT is used to broke image into spectral sub-bands with 8×8 blocks of pixels, working from left to right, top to bottom. The embedding function is given by [10 —14]:

$$S(j,k)=\beta\ C(j,k)+\alpha\ M'(j,k) \quad (1)$$

where:

$$\beta+\alpha =1 \quad (2)$$

S(j, k) is the modified DCT coefficients of the stego-image, C(j, k) is the cover-image DCT coefficients and M'(j, k) is the modified secret-message coefficients. Beta and alpha are two the ESF. Alpha is chosen to obtain a stego-image without perceptible degrading of the image quality. Then apply inverse IDCT on this modified embedded coefficient to get the stego-image.

Figure (2) shows the Block diagram of the proposed embedding algorithm. This proposed system can take a decision for the Stego image, is it acceptable or not.

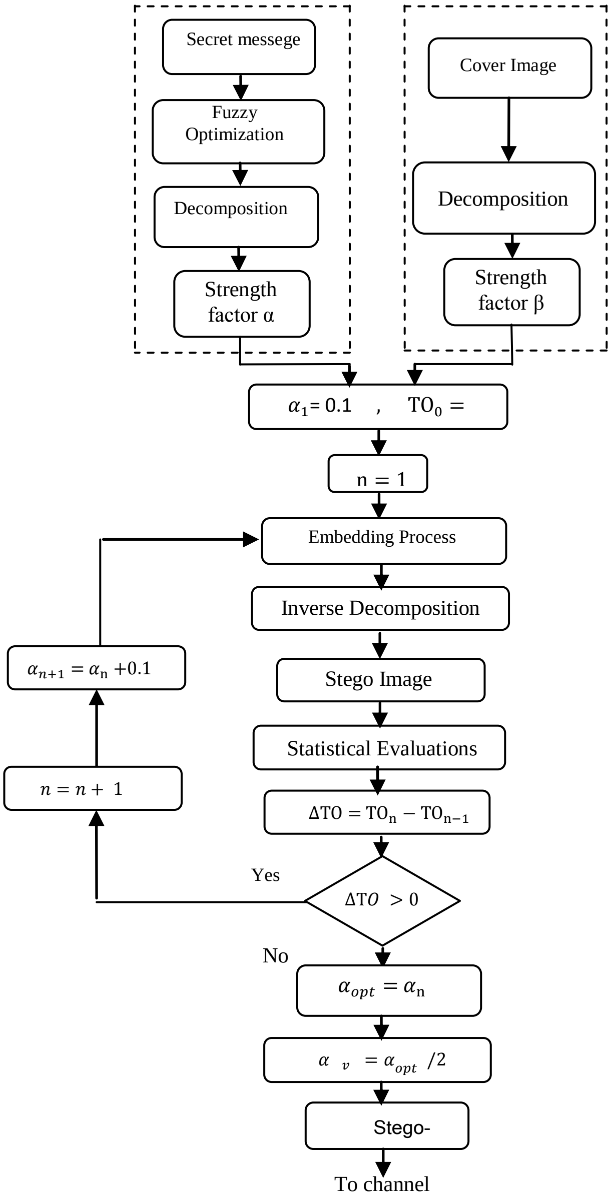


Fig. 2. The Block diagram of the modified algorithm

3. STEGANOGRAPHY ASSESSMENT

To assess the performance of the proposed algorithm, three evaluation statistical metrics are used. The first is the well known statistical metrics (MSE, PSNR, Cor, and Entropy), the others are two proposed metrics. There used three messages (Cameraman, House, and Baboon) to be embedded in a cover-image (Barbara) to obtained three different stego-images [8, 9, 10].

3.1 Common Metrics

3.1.1 Mean Square Error (MSE): The distortion in an image can be measured using the following equation

$$\mathbf{MSE} = \sum_{\mathbf{J=1}}^{\mathbf{M}} \sum_{\mathbf{K=1}}^{\mathbf{N}} \frac{(\mathbf{C(j,k) - S(j,k)})^2}{\mathbf{M * N}} \qquad (\mathbf{3})$$

Where: M, N is the size of the image.

3.1.2 Peak Signal to Noise Ratio (PSNR): The quality of stego-image, is computed by:

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

3.1.3 Cross Correlation coefficient: It is given by:

$$\mathrm{COR} = \frac{\sum_0^{N-1}(C(j,k)-m1)(S(j,k)-m2)}{\sqrt{(\sum_0^{N-1}(C(j,k)-m1)\ ^2(\sum_0^{N-1}(S(j,k)-m2)\ ^2}} \qquad (5)$$

It is used to comparing the similarity between the cover-image and the stego-image. Where m1 & m2 are the mean values of cover and Stego-image respectively.

3.1.4 Entropy: It is a statistical measure of randomness that can be used to characterize the texture of the input image, it is given by:

$$\mathrm{Entropy} = -\sum_i \mathrm{PjLog\ Pj} \qquad (6)$$

Figure (3) shows the block diagram of the proposed message reconstruction algorithm to recover the secret-message. The reconstructed message function can be directly derived from equation (1) [9] as.

$$M' = \frac{(S - \beta C)}{\alpha_v} \qquad (7)$$

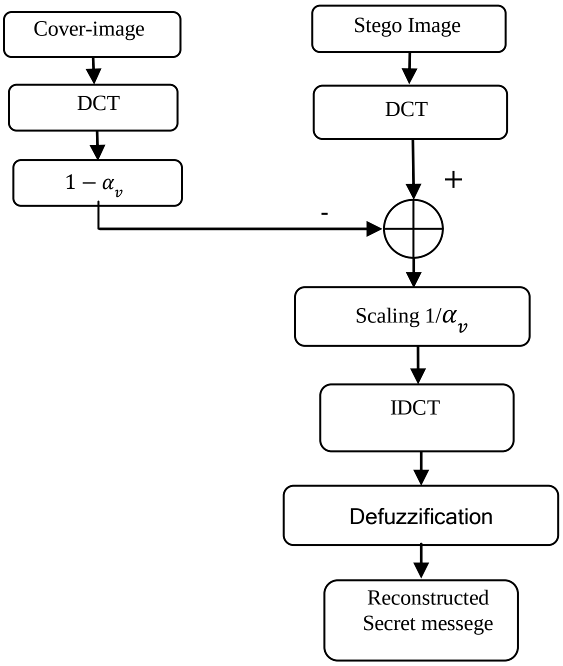


Fig. 3. The Block diagram of the reconstruction algorithm

Figure (4) shows the obtained Stego-images of the secret-messages (House as an example) using Barbara as a cover-image for different ESF (α) values. From this figure it is noticed that the Steg-image is drastically depending on the ESF (α) value. As the ESF (α) increases the visual Steg-image degrades.

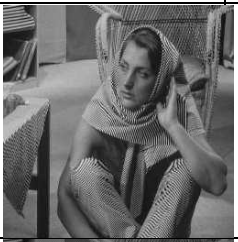
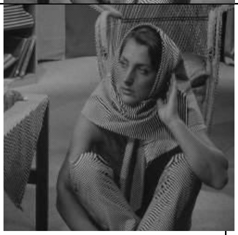
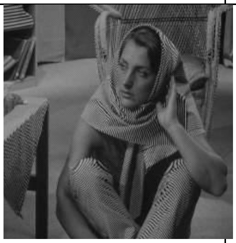
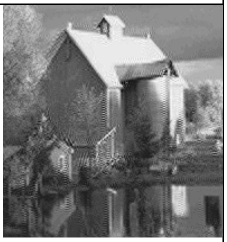
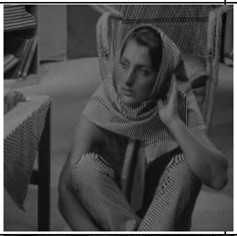
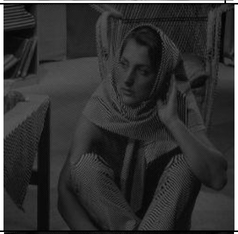
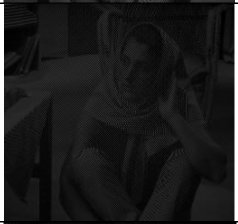
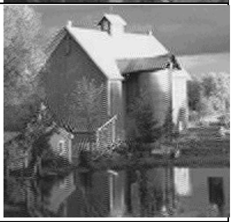
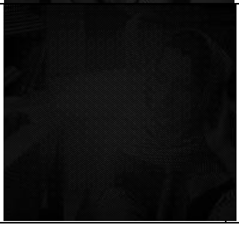
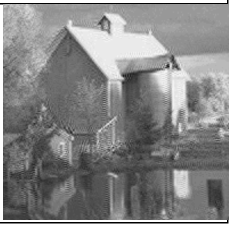
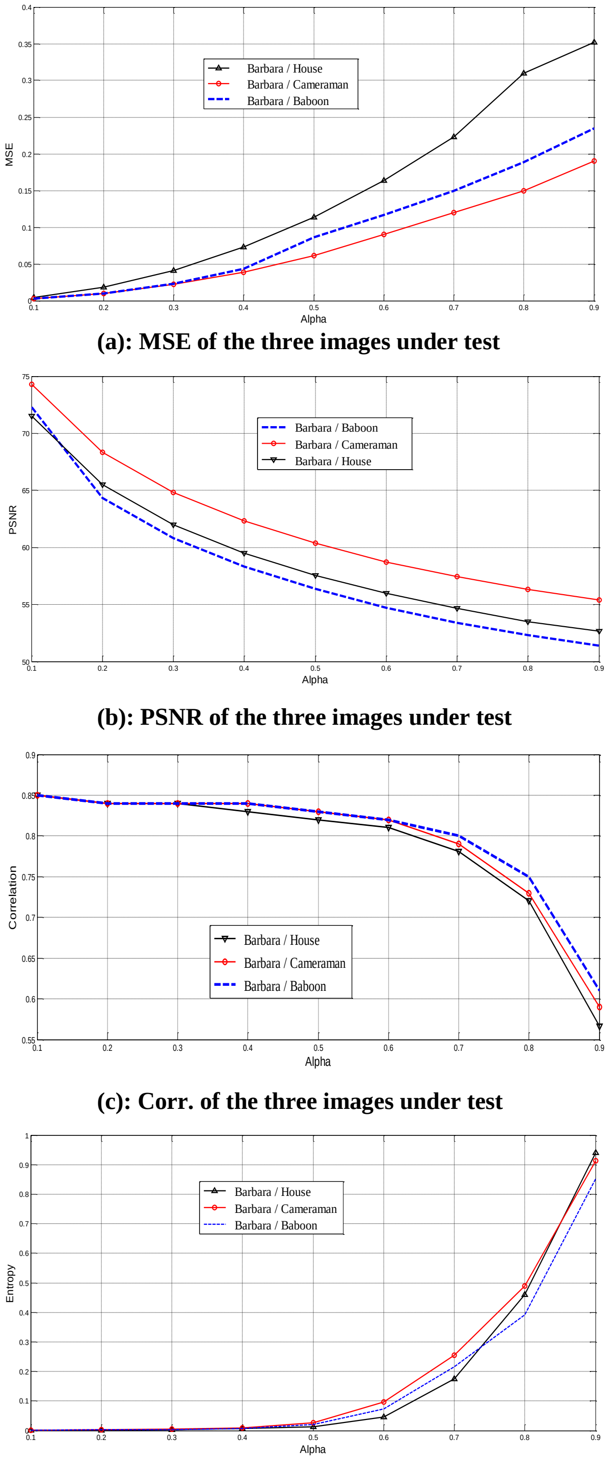
Alpha	Stego image	Reconstructed message
0.1		
0.2		
0.3		
0.4 $\alpha_v = \alpha_{opt}/2$		
0.6 $\alpha < \alpha_{opt}$		
0.8 $\alpha \geq \alpha_{opt}$		
0.9		

Fig. 4. Barbara as a Stego-image and house as a reconstructed secret-message for different values of alpha.

Figure (5 - a, b, c & d) shows the statistical results of the proposed algorithm for the Stego-image of the House, Baboon, and the Cameraman using the common metrics (MSE, PSNR, Cor and Entropy)



(a): MSE of the three images under test

(b): PSNR of the three images under test

(c): Corr. of the three images under test

(d): Entropy of the three images under test

Fig. 5. The common assessment metrics against ESF

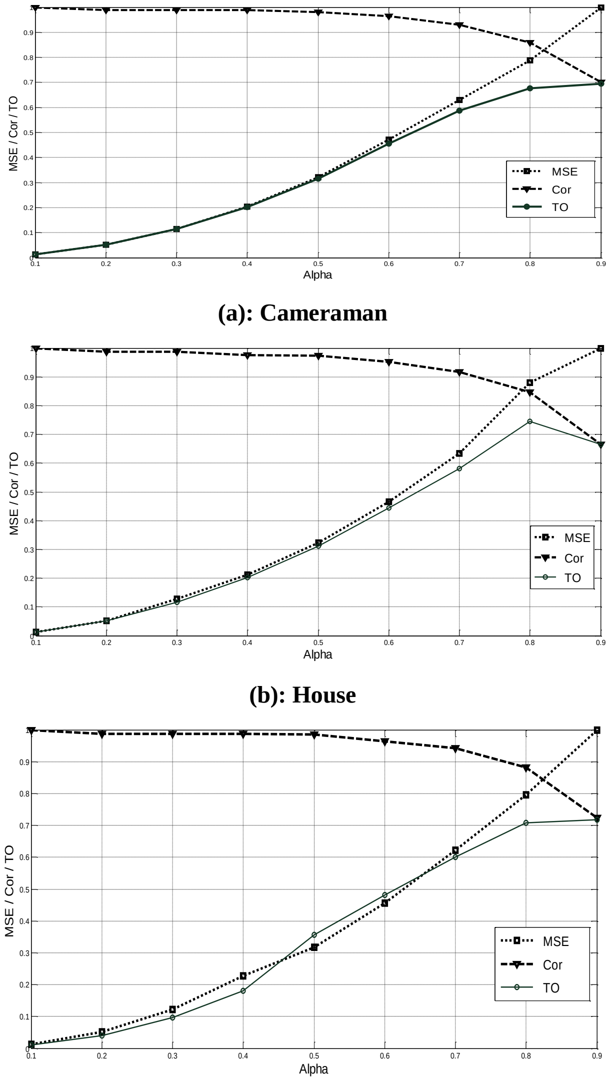
image (Barbara) to obtained three different stego-images [8, 9, 10]. From this figure it is seen that as the ESF (α) increases the MSE and entropy are increase, the PSNR decreases and the Corr. is very slowly decreasing up to ESF α≅0.7, then rapidly decreasing. Considering the mentioned above results, it is necessary to find some measurable metric parameter to determine to which limit the ESF is to be applied.

3.2 A Proposed Trade-Off Evaluation Metric

A proposed metric is introduced to combining between the MSE and correlation to obtain the most suitable Trade-Off (TO) value for the ESF (α), as follows

$$\mathrm{TO} = \left(\frac{\mathrm{MSE}}{\max}\right) . \left(\frac{\mathrm{Corr}}{\max}\right) \qquad (8)$$

Figure (6) shows the Trade-Off between the correlation (Cor.) and the MSE for the three secret messages under evaluation. The maximum value of the trade-off (TO_{max}) and its corresponding optimum value for the ESF (α_{opt}) are determined for ESF range (α = 0.1 — 0.9). From figure (4) it is worth to note that the Stego-image for $\alpha < \alpha_{opt}$ is accepted, while for $\alpha > \alpha_{opt}$ the Stego-image is highly distorted.



(a): Cameraman

(b): House

(c): Baboon

Fig. 6. The Trade-Off Corr. and MSE for the tested images

3.3 Visual Acceptance of Stego-image

From the visual inspection of figure (4) it is seen that acceptable value of the ESF (α) for the Stego-image must satisfy the condition:

$$\boldsymbol{\alpha_v = \frac{1}{2}\alpha_{opt}} \qquad (\mathbf{9})$$

where $\alpha_v$is the visual acceptable Stego-image.

Figure (7) shows the Stego-images for the House, Baboon, and Cameraman with their reconstructed secret-messages for the visual acceptance values ($\alpha_v = \alpha_{opt} / 2$).

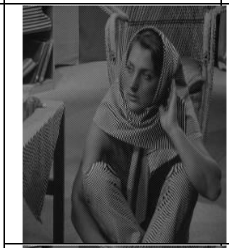
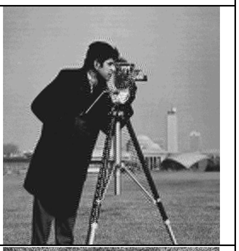
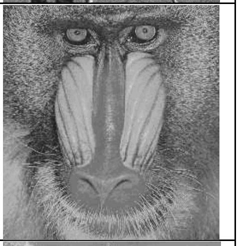
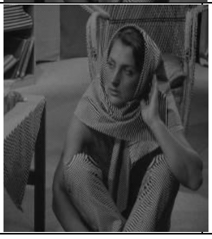
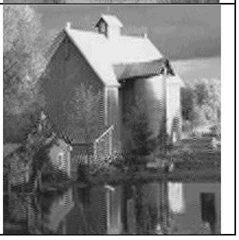
Alpha	Stego image	Reconstructed message
0.4 $\alpha_v = \alpha_{opt}/2$		
		
		

Fig. 7. The Stego and reconstructed images for the visual acceptance value

Thus the proposed algorithm enables to reconstruct the original message with degradation depending on the visual acceptance of the ESF (α). In order to improve the degradation of the reconstructed image a scaling factor $(1/\alpha_v\ )$ is proposed as in [9]. Table (1) shows a comparison among different algorithms [11].

Table 1. comparison among different algorithms

Method / **Parameter**	**LSB**	**DCT**	**The proposed algorithm**
PSNR	40.344	50.99	62.5

From table (1) it is seen that, the proposed steganography algorithm gives PSNR=62.5 at the accepted visual ESF ($\alpha_v = \alpha_{opt} /2$), while the LSB algorithm gives PSNR=40.344 and the DCT algorithm gives PSNR=50.99. Thus, the proposed algorithm is more secure than the other algorithms, With 22.16 dB gain w.r.t. the LSB method, and 11.51 dB gain w.r.t. the direct DCT method.

4. CONCLUSION

In this paper a modified Steganography algorithm using DCT and fuzzification of secret message provides compression & improved uniformity over the Stego-cover image. The proposed TO metric enables to select the most suitable optimized ESF for acceptable vision of the Stego-image. The application of the modified algorithm drastically improves the PSNR of the Stego-image. For the proposed trade-off when $\alpha < \alpha_{opt}$ the stego image is highly accepted where as for $\alpha > \alpha_{opt}$ the stego image is highly degraded. The embedding of the fuzzified secret-message using the optimized ESF for visual acceptance provides stego-image with negligible degradation w.r.t the original cover-image and a reconstructed secret-message without any degradation. From the comparative study it was seen that this method is better in terms of statistical metric parameters (PSNR, COR, MSE, Entropy and TO). The method not only provides a better and easy way for embedding large amount of data into a cover image with imperceptions, but also offers high robustness.

5. REFERENCES

[1] Nuno Roma, Leonel Sousa "A tutorial overview on the properties of the discrete cosine transform for encoded image and video processing" Rua Alves Redol, Lisboa – Portugal, February 2011.

[2] Ekta Walia, Payal Jain, Navdeep "An Analysis of LSB & DCT based Steganography " Global Journal of Computer Science and Technology, April 2010.

[3] Abbas Cheddad , Joan Condell, Kevin Curran, Paul Mc Kevitt" Digital image steganography: Survey and analysis of current methods " www.elsevier.com/locate/sigpro Signal Processing 2010.

[4] Hardik Patel, Preeti Dave " Steganography Technique Based on DCT Coefficients" International Journal of Engineering Research and Applications, Jan-Feb 2012.

[5] Hossein Malekmohamadi and Shahrokh Ghaemmaghami" stegoanalsis of lsb based image Steganography using spatial and frequency domain features" IEEE 2009.

[6] 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, June 2010.

[7] Matus Jokay — Tomas Moravcık " Image-Based JPEG Steganography", Tatra Mt. Math. Publ. 2010.

[8] Orea flores, M.A.acivedo "wavelet and discreet transforms for insetting information into BMB image ", July 2006.

[9] Mazhar Tayel, Alaa Hafez, Hamed Shawky "A New Hybrid Fuzzy-Decomposed Full Capacity Stego-System " under publication in IEEE Aerospace Conference 2014.

[10] George Corser," Entropy as an Estimate of Image Steganography" Oakland University Rochester, USA 2013, gpcorser@oakland.edu.

[11] Nedal M. S. Kafri and Hani Y. Suleiman "Bit-4 of Frequency Domain-DCT Steganography Technique" IEEE, 2009.

[12] Deepak Singla1, Rupali Syal "Data Security Using LSB & DCT Steganography in Images ", International Journal of Computational Engineering Research/ IJCER , Mar-Apr 2012.

[13] Blossom Kaur, Amandeep Kaur, Jasdeep Singh" steganographic approach for hiding image in DCT domain" IJAET, July 2011.

[14] Mazhar Tayel, Hamed Shawky, Alaa El-Din Sayed Hafez "New Chaos Steganography algorithm for Hiding Multimedia Data" advanced communication technology (ICACT), 2012.

[15] Mazhar Tayel, Alaa Hafez, Hamed Shawky," A Hybrid Chaos- Fuzzy –Threshold Steganography Algorithm for Hiding Secure Data" ICACT Transactions on Advanced Communications Technology (TACT), Jan. 2013.