A Proposed Assessment Metrics for Image Steganography

Mazhar Tayel, Hamed Shawky

Department of Electrical Engineering, Faculty of Engineering, Alexandria University, Egypt

ABSTRACT

Data security has become an important problem in the communication systems. Steganography is used to hide existence of a secret-message. In this article a modified Steganography algorithm will be proposed depending on decomposition principle of both secret-message and cover-image. A fuzzification is performed in the secret message to optimize the decomposed coefficients before embedding in the cover-image to get a Stego Image. The well known metrics (Cor., MSE, PSNR, and Entropy) were used to evaluate the modified algorithm. Also, a trade-off factor was introduced to determine an optimum value for the embedding strength factor to get an acceptable degradation. Moreover to evaluate and assess the modified algorithm and any Steganography algorithms, a new histogram metrics are proposed which represents the relative frequency occurrence of the various images.

KEYWORDS

Steganography, Cover- image, Secret-message, Decomposition, Fuzzy set, Histogram Deviation.

1. INTRODUCTION

In digital world, Steganography and Cryptography are synonymous used to protect information from unauthorised users (third party). Steganography can be used for different formats in digital media like, bmp, .gif, .jpeg, .mp3, .txt, and .wav. One of the most important and valuable tools to analyse image is the histogram. So what exactly is a histogram? A histogram is a graph that shows the colour range of image. A histogram shows how much of it is currently pure white, and how much of it falls somewhere between black and white images [1— 7].

2. Objective

This paper introduces a new Steganography metric able to evaluate effectiveness of any Steganography algorithm, applying this metric in the proposed algorithm which introduced in the previous paper.

3. 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.

DOI:10.5121/ijcis.2014.4101

(i)- Fuzzy Optimization.

Using nine triangular MF to compress the secret-image from (0 — 255) to (0 — 30) image color range. Then embeding into the cover image to obtain a uniformly diffused distribution of message pixels all over the cover image.

(ii) - Image decomposition

The fuzzified secret-message and the cover-image are decomposed and then embed the coefficients of the fuzzified message in the cover-image. When data is embedded in the frequency domain, the security of the secret data resides in more robust areas, spread across the entire image, to provide better resistance against statistical attacks, high capacity, high imperciptability and robustness.

The DCT is used to decompose image into spectral sub-bands, working from left to right, top to bottom. The embedding function resultant matrix, obtained by addition of the DCT coefficients of the cover-image and the fuzzified secret-message, 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 complementary ESF. Alpha is chosen to obtain a stego-image without perceptible degrading of the image quality and to provide better resistance against steganalysis process. Then apply inverse IDCT on this modified embedded coefficients to get the stego-image. Figure (1) shows the proposed embedding algorithm. This proposed system can take a decision for the Stego image, is it acceptable or not. Figure (2) shows the block diagram of the proposed message reconstruction algorithm to recovere the secret-message.

3.1 Steganography assessment

To assess the performance of the Steganography 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 methods. There used three messages (Cameraman, House, and Baboon) to be embedded in a cover-image (Barbara) to obtained three different stego-images which will be under evaluation. These evaluation metrics will be described in the following [8,9, 10].

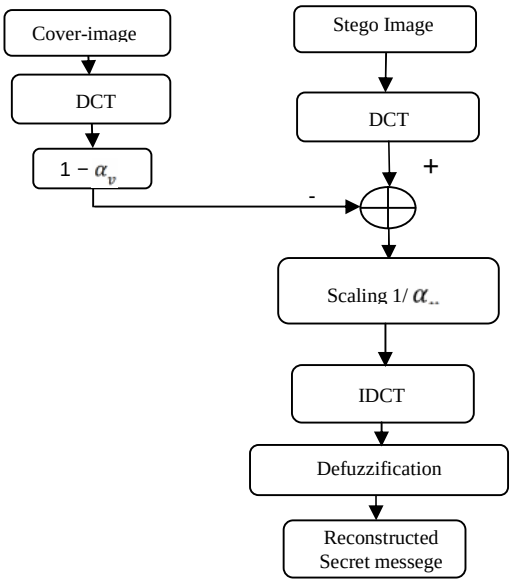


Fig.(2): The Block diagram of the reconstruction algorithm.

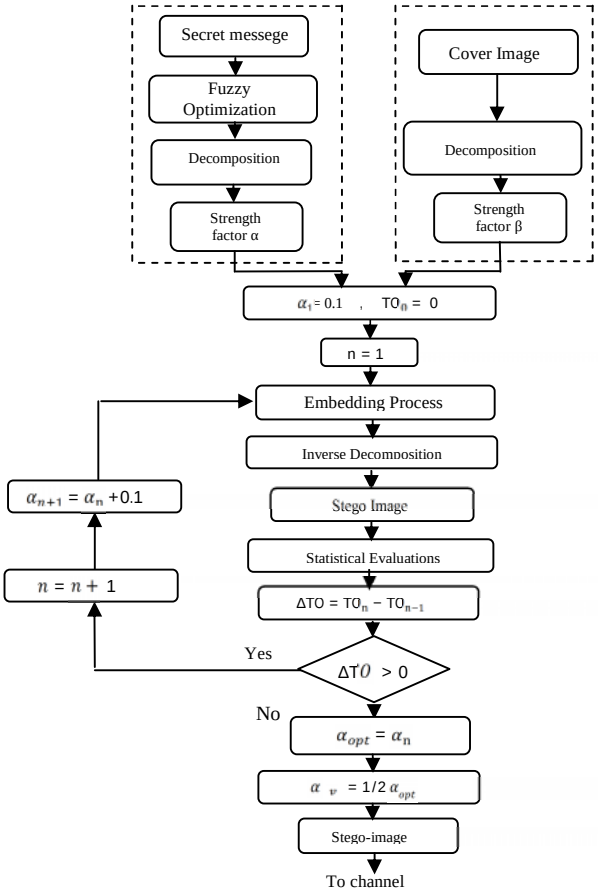


Fig. (1): The Block diagram of the introduced embedding algorithm.

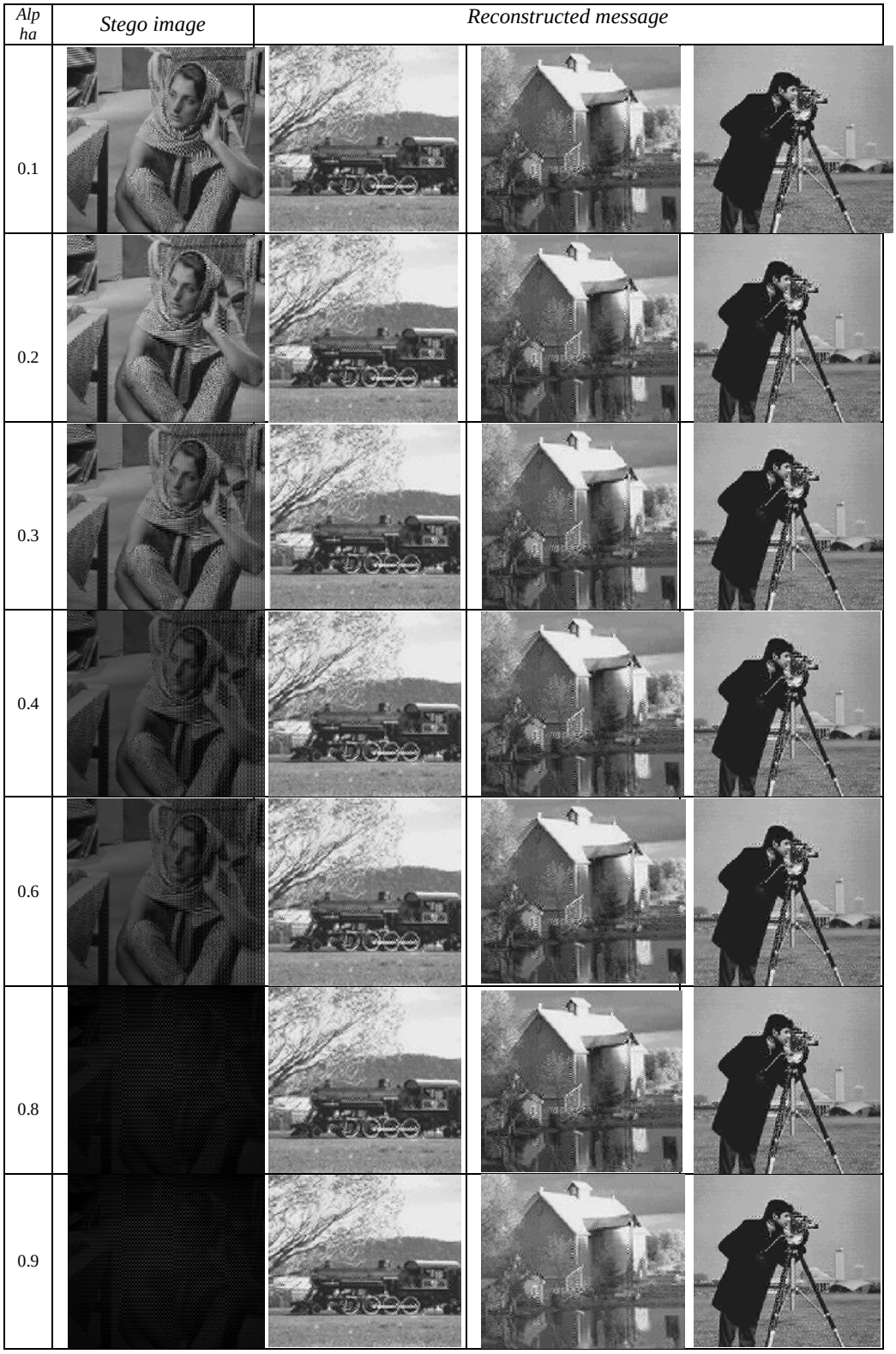


Fig. 3. Barbara as a Stego- image and different reconstructed secret messages for different values of alpha.

A. Common Metric Methods

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

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

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

2) Peak Signal to Noise Ratio (PSNR): The percentage of noise present in the stego-image, is to be computed using the equation:

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

3) Cross Correlation coefficient: which is given by:

$$COR = \frac{\sum_{0}^{N-1}(C(j,k)-m1)(S(j,k)-m2)}{\sqrt{(\sum_{0}^{N-1}(C(j,k)-m1)^2(\sum_{0}^{N-1}(S(j,k)-m2)^2}} \quad (5)$$

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

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:

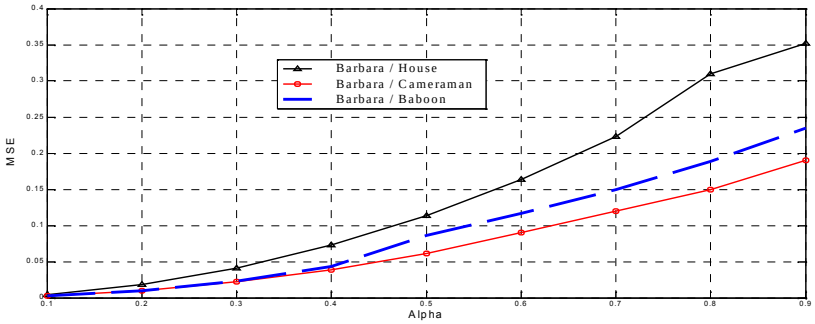
$$Entropy = -\sum_{i} Pj \, Log \, Pj \quad (6)$$

Figures (3) show the obtained Stego-images of the three secret-messages (Cameraman, Baboon, House) using Barbara as a cover-image with different ESF (α). From these figures it is worth to note that the Steg-image is drastically depending on the ESF (α) value. As the ESF (α) increases the visual Steg-image degrades.

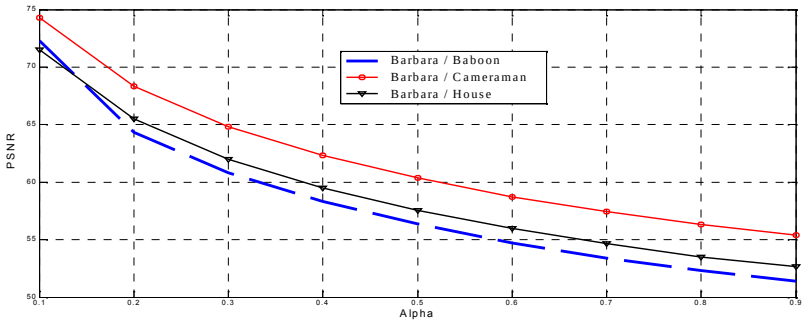
From figures it is worth to note that the Stego-image for $\alpha < \alpha_{opt}$ is accepted, while for $\alpha > \alpha_{opt}$the Stego-image is highly distorted.

Figure (4 - a, b, c & d) shows the statistical results of the proposed steganography algorithm for the Stego-image of the House, Baboon, and the Cameraman using the common metrics (MSE, PSNR, Cor and Entropy).

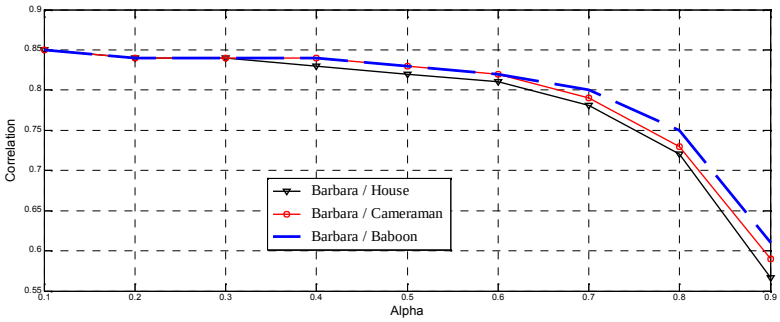
From this figure it is seen that as the ESF (α) increases the MSE and entropy are increas, the PSNR decreases and the Corr. is very slowly decreasing up to ESF $\alpha \approx 0.7$, then rapidly decreasing. Considering the mentioned above results, it is necessary to find some measurable metric parameter to determine to which limit the ESF is to be applied.



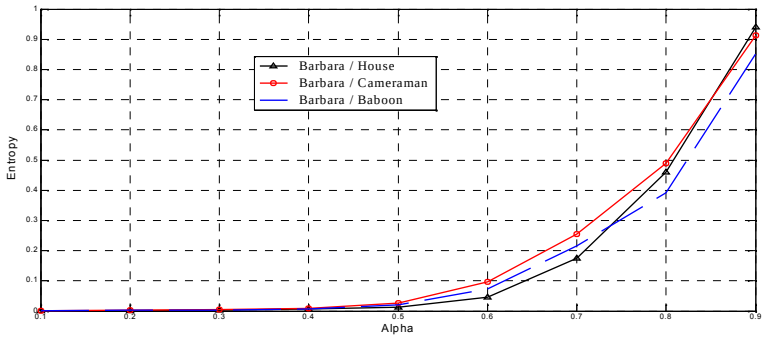
(a): MSE of the three images under test.



(b): PSNR of the three images under test.



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



(d): Entropy of the three images under test.

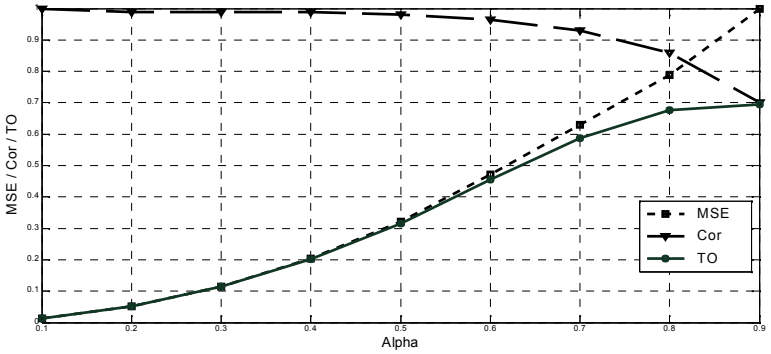
Fig. 4. The common assessment metrics against ESF.

B. A Proposed Trade-Off Evaluation Metric

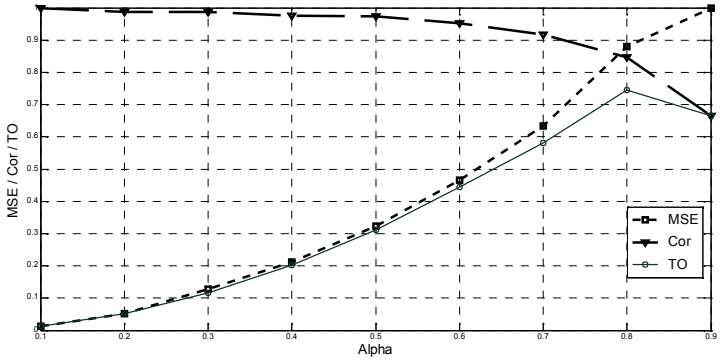
A proposed Trade-Off (TO) combining between the MSE and correlation to satisfy the most suitable value for ESF (α) is introduced, as follows

$$TO = \left(\frac{MSE}{max}\right).\left(\frac{Corr}{max}\right) \quad (7)$$

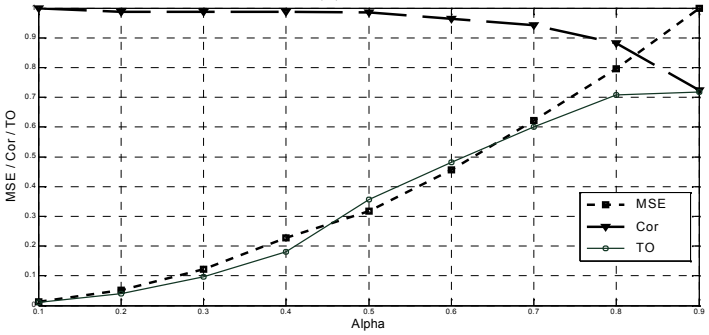
Figure (5) shows the Trade-Off between the correlation (Cor.) and the MSE for the three secret messages under evaluation. The proposed TO was iterated for ESF range (α = 0.1 — 0.9) to evaluate the Stego image. The iteration runs to determine the optimum value of alpha ($\alpha = \alpha_{opt}$), see figure (1).



(a): Cameraman.



(b): House.



(c): Baboon.

Fig. 5. The Trade-Off Corr. and MSE for the tested images.

C. Visual Acceptance of Stego-image

From the visual inspection of figure (3) it is seen that acceptable value of the ESF (α) for the Stego-image must satisfy the condition:

$$\alpha_v = \frac{1}{2}\alpha_{opt} \tag{8}$$

where α_v is the visual acceptable Stego-image.

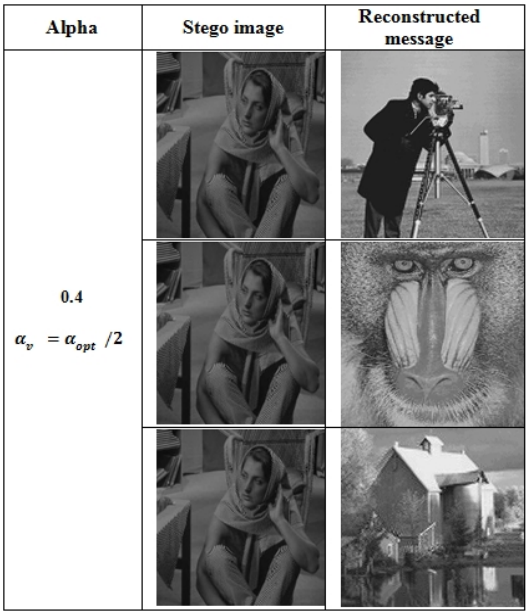


Fig. 6. The Stego and reconstructed images for the visual acceptance value.

Figure (6) shows the Stego-images for the House, Baboon, and Cameraman with their reconstructed secret-messages for the visual acceptance values ($\alpha_v = \alpha_{opt}/2$). 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].

D. A Proposed Histogram Deviation metric

Deviation histograms for the coefficients of the cover, fuzzified secret-message and Stego-image are introduced as follows:

i- Stego-Message Histogram Deviation (SMD)
It is given as

$$\Delta SMD = |SIC - MC| \tag{9}$$

where:

SIC is the Stego-Image Coefficients, and MC is the Message Coefficients and its percentage deviation is

$$\Delta SMD\% = \frac{\Delta SMD}{CC} \times 100 \quad (10)$$

where

CC is the cover coefficient

ii- Stego-Cover Histogram Deviation (SCD)
It is given as

$$\Delta SCD = |SIC - CC| \quad (11)$$

and its percentage deviation is

$$\Delta SCD\% = \frac{\Delta SCD}{CC} \times 100 \quad (12)$$

iii- Stego-Image Variance Deviation (Δvar),
It is given as

$$var(x) = \Sigma(Xi,j - \mu)^2 / N \quad (13)$$

where: μ Is the mean value, (Xi,j) is the image pixels, N is

number of pixel. The variance deviation (Δvar) is given as

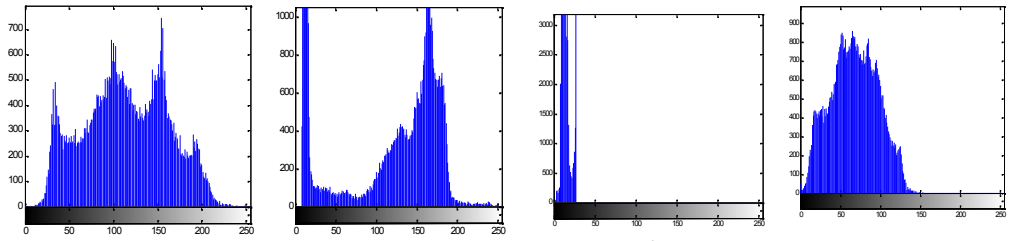
$$\Delta var = |var(SIC) - var(CC)| \quad (14)$$

and its percentage deviation is

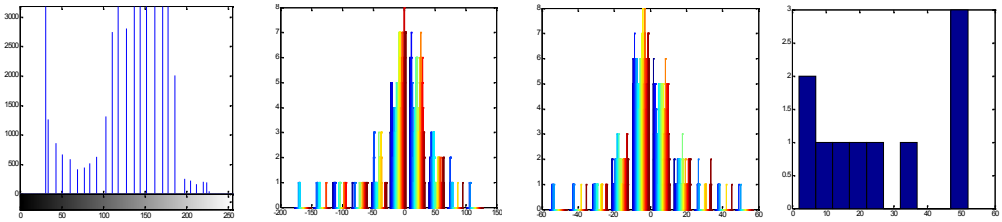
$$\Delta var\% = \frac{\Delta var}{var(CC)} \times 100 \quad (15)$$

3.2 EXPEREMINTAL RESULTS

Figures (7) and (8), show the proposed histogram deviation metric at $\alpha = \alpha_{opt}$, for (a) the histogram of Barbara as a cover image, (b) the histogram of Cameraman as a secret message, (c) the histogram of Cameraman after fuzzification as a secret message, (d) the histogram of Stego-image, (e) is the reconstructed secret message, (f) and (g) are the histograms for ΔSMD, ΔSCD compared with the histograms of (c) and (d) respectively, and (h) is the variance deviation.

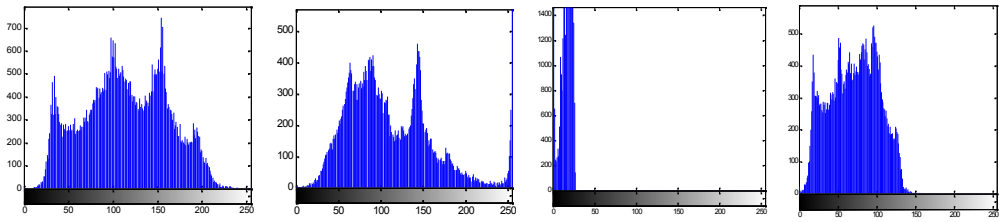


(a):Barbara as a cover (b): Cameraman as a secret (c) Fuzzified secret message (d) Stego-message

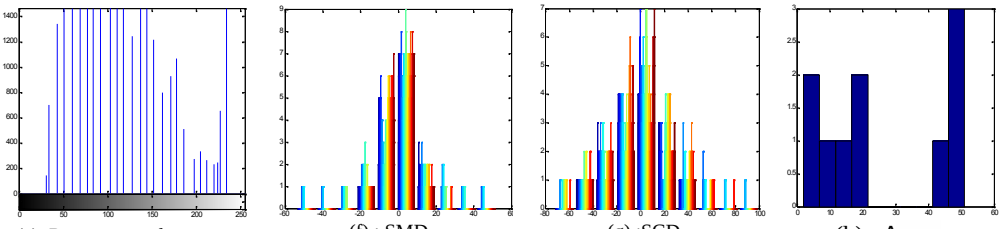


(e) :Reconstructed message (f) : SMD (g) :SCD (h): Δvar

Fig.7. Histogram metric for the Barbara and Cameraman.



(a):Barbara as a cover (b): Cameraman as a secret. (c) Fuzzified secret message (d) Stego-message



(e) :Reconstructed message (f) : SMD (g) :SCD (h): Δvar

Fig.8. Histogram metric for the Barbara and House.

From this figures it is concluded that the stego-image is very close to the cover-image. This shows that the proposed algorithm is more secure. Also, it is worth to note that deviations are message dependent.

4. CONCLUSION

Steganography is used to transfer secret message over open channel. The human visual system will be unable to perceive any difference in a Stego image. So the proposed metrics analyze the Stego image to evaluate performance of the Steganography algorithm. In this paper a new assessment metrics are proposed to evaluate security of any Steganography algorithm.

REFERENCES

[1] D. Lee Fugal "conceptual wavelet in digital signal processing" 2009 Space & Signals Technologies LLC, www.ConceptualWavelets.com.

[2] Ivan W. Selesnick Polytechnic University Brooklyn, NY "Wavelet Transforms A Quick Study" September 27, 2007.

[3] Eric Cole Ronald D. Krutz, Consulting Editor "Hiding in Plain Sight: Steganography and the Art of Covert Communication" Published by Wiley Publishing, Inc., Indiana Published simultaneously in Canada 2003.

[4] H S Manjunatha Reddy, N Sathisha, Annu Kumad, K B Raja," Secure Steganography using Hybrid Domain Technique" ICCCNT'12, July 2012, Coimbatore, India.

[5] Mehdi Kharrazi, Husrev T. Sencar, "Image Steganography: Concepts and Practice" Lecture Notes Series: April, 2004.
[6] L LAWSON and J. ZHU "Image compression using wavelet and a jpeg: tutorial" electronics and communication engineering journal, June 2002.
[7] Elham Ghasemi, Jamshid Shanbeh zadeh, Nima Fassihi "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm" proceeding of International Multi Conference of Engineers and computer scientists 2011, Hong Kong.
[8] H S Manjunatha Reddy, K B Raja " Steganography based on Adaptive Embedding of Encrypted Payload in Wavelet domain " International Journal of Scientific & Engineering Research, Volume 3, Issue 8, August-2012.
[9] Souvik Bhattacharyya and Gautam Sanyal " Data Hiding in Images in Discrete Wavelet Domain Using PMM" World Academy of Science, Engineering and Technology 2010.
[10] Vladimír BÁNOCI, Gabriel BUGÁR, Dušan LEVICKÝ " A Novel Method of Image Steganography in DWT Domain" IEEE, 2011.
[11] Saurabh V. Joshi, Ajinkya A. Bokil, Nikhil A. Jain,and Deepali Koshti " Image Steganography Combination of Spatial and Frequency Domain" International Journal of Computer Applications Volume 53– No.5, September 2012.
[12] DEE - Politecnico di Bari," Steganography Effects in Various Formats of Images. A Preliminary Study" International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications -4 Foros Ukraine, July 2001.
[13] Vijay Kumar, Dinesh Kumar "Performance Evaluation of DWT Based Image Steganography" IEEE, 6/10/2010.
[14] Haiying Gao, Xiaolong Zheng," Image Information Hiding Algorithm Based on DWT with Alterable Parameters" IEEE, 7/10/2010.

Author

Mazhar Basyouni Tayel *is professor in Faulty of Engineering, Alexandria University, Alexandria, Egypt. He holds B.Sc. in Electronics and Communications from Faculty of Engineering, Alexandria University, He also holds M.Sc. and Ph.D. in Electrical Engineering from Faculty of Engineering, Alexandria University. He tought many technical courses in Electrical and Electronic (Analog and Digit al) system design and Implementation, works as System Engineer for more than 20 years, teach up to 30 undergraduate, postgraduate subjects, supervising more than 75 thesis, publish more than 150 papers in different international conferencse, Forums and Journals.*

Hamed Shawky Zied *is a Post Graduate Student (Ph.D.), Alexandria University, Alexandria, Egypt and became a Member of IEEE in 2012. He was born in Minoufia, Egypt in 1973. He holds B.Sc. in Electronics and Communications from Faculty of Engineering, Alexandria University, M.Sc. in Electrical Engineering from Faculty of Engineering, Alexandria University. He received many technical courses in electronic engineering design and Implementation.*