

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Compression and Segmentation of JPEG Images Using DWT.

T Gomathi*.

Department of Electronics and Telecommunication Engineering, Sathyabama University, Chennai-119, Tamil Nadu, India.

ABSTRACT

Hiding capacity is very important for efficient covert communications. For JPEG compressed images, it is necessary to enlarge the hiding capacity because the available redundancy is very limited. Steganography enables to have a secret communication in modern information technology using Dual Transform Technique for Robust Steganography (DTTRS) [1]. The implementation of the Dual transform technique is carried out in the following sequences. The JPEG compressed grayscale cover image is segmented into 4×4 blocks each and Discrete Wavelet Transform (DWT) is applied on each block. The blocks of vertical band of 2×2 each obtained from the resulting DWT coefficients are considered and Integer Wavelet Transform (IWT) is applied to get blocks of 1×1 each. Next, to each 1×1 Block of the cover image, the secret data is embedded using LSB replacement technique. On applying IWT and IDWT, stego image is derived. Error Detection and Correction Code (EDCC) technique is implemented to ensure more reliable communication. For EDCC, Turbo Codes have been implemented in the field of forward error correction and high performance error correction so as to achieve maximal information over a limited bandwidth communication link. The encoded message is now hidden into the DWT and IWT transformed cover image by LSB substitution method. At the receiver side, the stego image is subjected to IWT and IDWT. Then the encoded secret data is retrieved after error detection and correction by the decoding process.

Keywords: Data hiding, JPEG, steganography, DCT, DWT, IWT, EDCC, Turbo Code, IWT and IDWT

**Corresponding author*

INTRODUCTION

Steganography or Stego as it is often referred to in the IT society, exactly means, enclosed script which is derived from the Greek language. Steganography is defined by Markus Khan as follows, "Steganography is the art and science of communicating in a way which hides the existence of the communication". In Cryptography the opponent is allowed to recognize, seize and amend messages without being able to violate certain security premises guaranteed by a cryptosystem, the objective of Steganography is to conceal messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a subsequent message present. In a digital globe, Steganography and Cryptography both intended to protect information from redundant parties.

Steganographic technologies are very important face of the future of security and privacy on open systems such as the Internet. Steganographic is primarily driven by the lack of strength in the cryptographic systems on their own and the desire to have complete secrecy in an open systems environment. Steganography can be used to hide important data inside another file so that only the parties intended to get the message even knows a secret message exists To add multiple layers of security and to help subside the "crypto versus regulation" problems, it is fine to carry out Cryptography and Steganography. Steganography techniques are classified as

The message will be embedded into text file in steganography based on text method.

- *Audio Steganography*
- *Image Steganography*
- *Text-based Steganography*

Steganography is the art of hiding secret information into the cover image. Steganography can be combined with cryptography to achieve a higher level of security. Recent techniques in steganography, focuses on higher embedding capacity and lower distortion. Dual Transform Technique is implemented in the proposed steganography technique in order to achieve an improved embedding capacity of the secret data along with better PSNR. Further the technique also implements an error detection and error correction technique so as to ensure a reliable and secured data communication and recovery. In this scheme of Dual transform technique, both DWT and Integer Wavelet Transform (IWT) are implemented. Integer Wavelet Transform maps an integer data set into another integer data set[2]. In DWT, the used wavelet filters have floating point coefficients so that when secret data is hidden in these coefficients, any truncations of the floating point values of the pixels that should be integers may cause the loss of the hidden information which may further lead to the failure of the data hiding system. In addition to dual transform technique in this project work, Error Detection and Correction Code (EDCC), namely Turbo Codes have been implemented in the field of forward error correction and high performance error correction so as to achieve maximal information over a limited bandwidth communication link. The encoded message is now hidden into the DWT and IWT transformed cover image by LSB substitution method. the performance analysis of the proposed Dual Transform Technique with turbo error detection and correction code was implemented and simulated by adding different noise percentages. The noise chosen was salt & pepper noise. The stego image received was subjected to filtering and then the embedded message was retrieved.

Discrete Cosine Transform

The existing scheme for improving embedding capacity in frequency domain is DCT. A DCT domain hiding scheme can be applied in JPEG very conveniently. This scheme for improving embedding capacity in frequency domain is DWT. A DWT domain hiding scheme can be applied in JPEG very conveniently [5]. There have been many kinds of DWT domain information hiding schemes developed for JPEG standard, such as J-steg, JPHide-seek and Out-Guess. In DWT, the used wavelet filters have floating point coefficients so that when secret data is hidden, any truncations of the floating point values of the pixels causes loss in the secret data, which leads to failure of the data hiding system. This limitation is overcome by Integer Wavelet Transform (IWT) which maps an integer data set into another integer data set thereby preventing loss of data [2]. Error detection and Correction Code (EDCC) convolution code to detect less number of errors to overcome that turbo code technique was implemented.

Discrete Wavelet Transform (DWT)

This is another frequency domain in which steganography can be implemented. DCT is deliberated on blocks of independent pixels, a coding error causes discontinuity among blocks ensuing in frustrating jamming artifact. This drawback of DCT is eliminated using DWT. DWT applies on entire image. DWT offers better energy compaction than DCT without any blocking artifact. DWT splits component into numerous frequency bands called sub bands known as

- LL – Horizontally and vertically low pass
- LH – Horizontally low pass and vertically high pass
- HL - Horizontally high pass and vertically low pass
- HH - Horizontally and vertically high pass

Since Human eyes are much more sensitive to the low frequency part (LL sub band) we can hide secret message in other three parts without making any alteration in LL sub band. As other three sub-bands is high frequency. Sub-band they contain insignificant data. Hiding secret data in these sub-bands doesn't degrade image quality that much. DWT used in this work is Haar-DWT, the simplest DWT.

Integer Wavelet Transform

Based Steganography Approach

Steganography in Frequency Domain

Robustness of steganography can be improved if properties of the cover image could be exploited. For example it is generally preferable to hide message in noisy regions rather than smoother regions as degradation in smoother regions is more noticeable to human HVS (Human Visual System). Taking these aspects into consideration working in frequency domain becomes more attractive [3]. Here, sender transforms the cover image into frequency domain coefficients before embedding secret messages in it. Different sub-bands of frequency domain coefficients give significant information about where vital and non vital pixels of image resides. These methods are more complex and slower than spatial domain methods; however they are more secure and tolerant to noises. Frequency domain transformation can be applied either in DCT, DWT or IWT.

Integer Wavelet Transform (IWT)

This is another frequency domain in which steganography can be implemented. Integer Wavelet Transform is an efficient lossless compression technique [7]. Integer Wavelet Transform is much faster than the floating point arithmetic in almost all general purpose computers because the floating point wavelet transform demands for longer data length than the integer wavelet Transform. Integer Wavelet Transform maps an integer data set into another integer data set. The image can be reconstructed without any loss because all the coefficients are integers and can be stored without rounding off errors.

Error Detection and Correction Code technique (EDCC)

Error Detection and Correction Code (EDCC), namely Turbo Codes have been implemented in the field of forward error correction and high performance error correction so as to achieve maximal information over a limited bandwidth communication link[8]. The secret data to be extracted at the destination without any deviation from the original even though it is transmitted through noisy channel and attacked by the hacker. EDCC turbo code is used to detect and correct more errors compared to the existing convolution technique.

Embedding phase

Let C and S be the cover-image and the secret-image respectively. The stego-image G can be obtained by the following steps:

Step 1: Decompose by one level of 2D-DWT each of the cover image C and the secret image S using a linear phase two-channel integer filter bank proposed in for obtaining the four sub-images (CLL1, CLH1, CHL1, and CHH1) and the four sub-images (SLL1, SLH1, SHL1, and SHH1) respectively[9].

Step 2: Each of SLL1, CLL1, and CHL1 are partitioned into blocks of 4x4 pixels and can be represented by:

$$SLL1 = \{BS_i; 1 \leq i < ns\} \tag{1}$$

$$CLL1 = \{BCK_1; 1 \leq k_1 < nc\} \tag{2}$$

$$CHL1 = \{BHK_2; 1 \leq k_2 < nc\} \tag{3}$$

Where BS_i , BCK_1 , and BHK_2 represent the i th block in SLL1, the k_1 th block in CLL1, and the k_2 th block in CHL1 respectively, ns is the total number of the 4x4 blocks in SLL1 and nc is the total number of the 4x4 blocks in each of CLL1 and CHL1.

Step 3: For each block BS_i in SLL1, the best matched block BCK_1 of minimum error in CLL1 is searched for by using the root mean squared error (RMSE) criteria.

The first secret key K_1 consists of the addresses k_1 of the best matched blocks in CLL1.

Step 4: Calculate the error block EB_i between BCK_1 and BS_i as follows:

$$EB_i = BCK_1 - BS_i \tag{4}$$

Step 5: For each error block EB_i , the best matched block BHK_2 in CHL1 is searched for using the RMSE criteria as before and that BHK_2 is replaced with the error block EB_i . The second secret key K_2 consists of the addresses k_2 of the best matched blocks in CHL1.

Step 6: Repeat the steps 3-5 until all the produced error blocks are embedded in CHL1.

Step 7: Apply the 2D-IDWT to the CLL1, CLH1, CHH1 and the modified sub-image CHL1 to obtain the stego image.

SIMULATION RESULTS

The source image is Lena, a grayscale image of 256*256,. Each pixel has eight bits. The secret message to be embedded in JPEG cover image using Dual Transform technique (DWT and IWT). The secret message is 10 KB of secret message in total and cover image (Lena) size is 25KB. In the following procedure, the source image is compressed at a ratio of 16, and information hiding is conducted simultaneously.



Figure 1 Lena cover



Figure 2 flower(JPEG)



Figure 3 simple(JPEG)

1-D wavelet decomposition

From Figure 4 Lena JPEG image is modified into 1-D wavelet decomposition to get more than the single descriptions. All these carried out only in the DWT domain. This figure represents L-Low, H-High frequency or wavelet part of the image. The image divided into four sub-bands LL,LH,HL and HH. Figure 5 shows the secret data(10KB) is embedded into the JPEG cover image derived as stego image. Table 1and Table clearly indicates that the statistical values of the images do not differ drastically from the cover images. It is inferred from the table that there is only a minute variation in all these parameters between cover and

stego images.

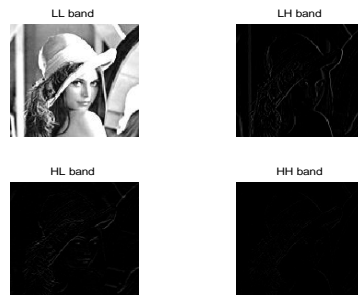


Figure 4: 1-D wavelet decomposition



Figure 5: Stego

Table 1: Mean & PSNR values for different jpeg images.

I IMAGES	M MEAN	VA VARIANCE	P PPSNR(dB)	SECRET MSG
S LENA IMAGE	24 221.1 375	0.7452	24 20.9835	10KB
FF FLOWER IMAGE	84 68.82 12	0.0705	28. 22.1527	10KB
SI SIMPLE IMAGE	22 18.46 42	0.0049	34 26.3478	10KB

From Table 1 and Table 2 it is referred that the proposed modulo based image steganography technique provides more than 33% of good insertion capacity for any of the cover images. From Table1 and Table2 clearly indicates that the statistical values of the images do not differ drastically from the cover images. Its is inferred from the table that there is only a minute variation in all the parameters between adding noise to the stego image without filter and with filter.

Histogram Analysis

Figure 6 and 7 shows the Lena(JPEG) image Histogram analysis of the cover and stego images. From the analysis only very minute variation in the histogram of the stego image is obtained. The embedding capacity achieved without degradation in the Histogram Analysis of stego image was 10KB.

Segmentation

Figure 8 shows the Lena (JPEG) image is segmented in 4*4 blocks. Each segmented blocks are modified into 1-D wavelet decomposition to get more than the single descriptions as shown in figure 9 and figure 10.

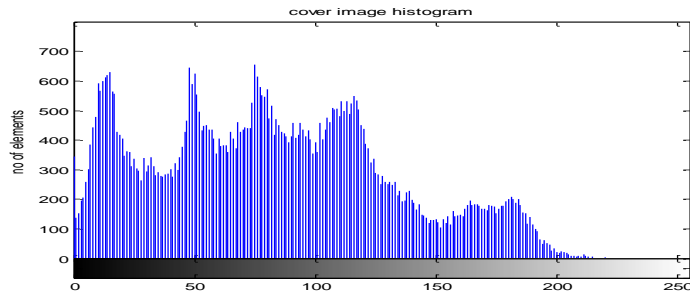


Figure 6: Lena original image histogram

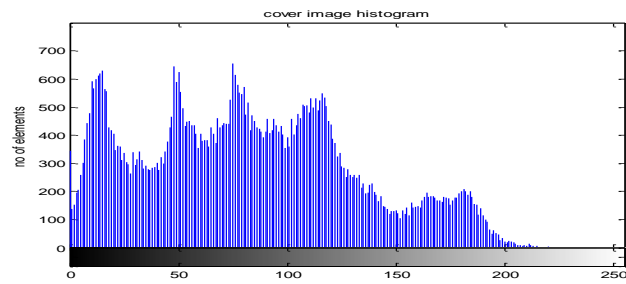


Figure 7: Lena stego image histogram



Figure 8: Segmented Lena image

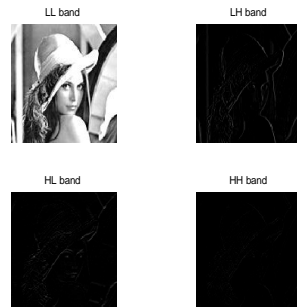


Figure 9: Sub-bands of cover image using DWT

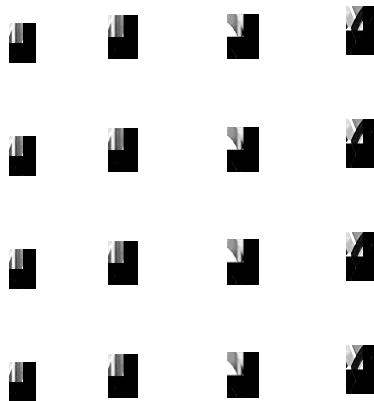


Figure 10: 1-D wavelet description of each segmented block

Stego image

From 11 and 12 shws that the secret data(max 15KB) is embedded into JPEG cover image using LSB replacement technique. The stego image perceptual quality is good in comparison with the cover image. The maximum embedding data was 15KB . If the data size was increased the stego image appeared distorted. After embedding data in each segmented blocks, combined the vertical segmented blocks into 1*1 each finally to obtain the stego image. Figures 13 and 14 are the Histogram analysis of the original and stego images.



Figure 11: Sub-bands of cover image using DWT



Figure 12: Stego image

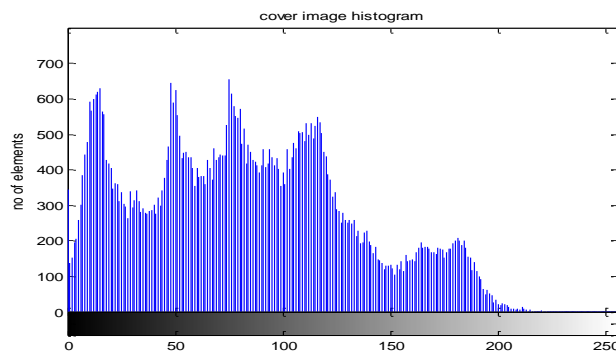


Figure 13: lena original image histogram

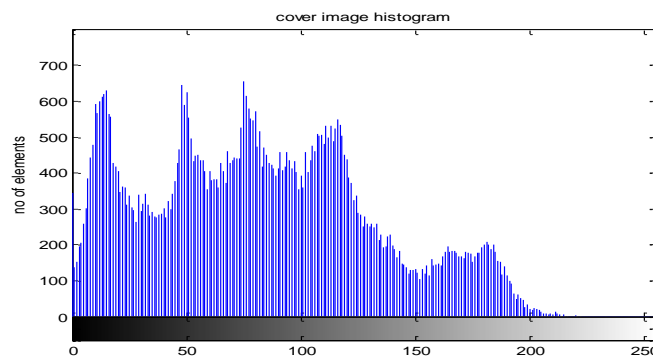


Figure 14: lena stego image histogram

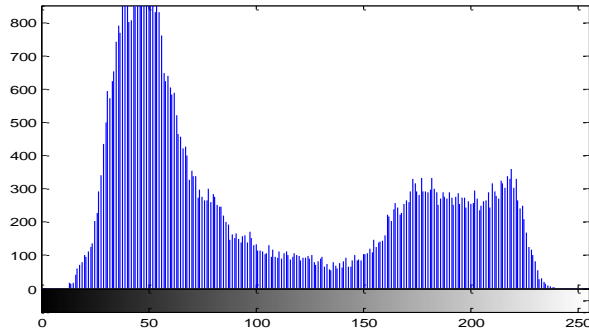


Figure 15: flower original image histogram

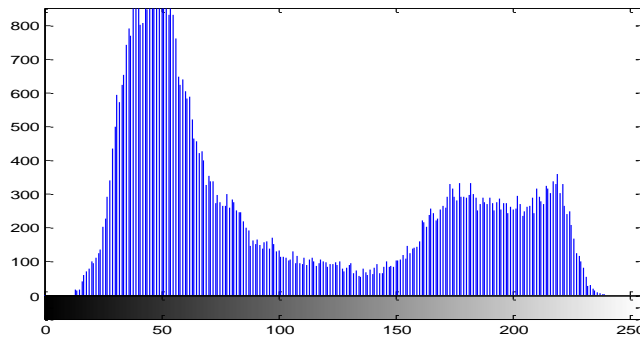


Figure 16: flower(stego) histogram

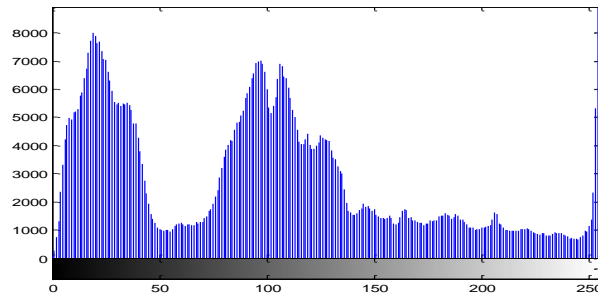


Figure 17: Simple original image histogram

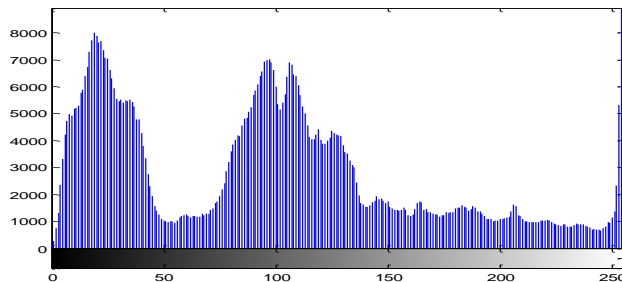
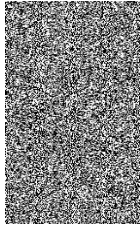






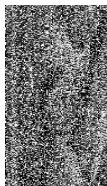




Figure 18: Simple(stego)image histogram

 <p>Figure 1</p>	 <p>Figure 2</p>
 <p>Figure 3</p>	 <p>Figure 4</p>
 <p>Figure 5</p>	 <p>Figure 6</p>
 <p>Figure 7</p>	 <p>Figure 8</p>
 <p>Figure 9</p>	 <p>Figure 10</p>

Information with noise consideration

The stego image was tested with noise added to test the stability, agility and efficiency of it. Then denoising operation was also performed to restore the original information. Adding noise with certain percentages as shown in Figures 20, 21 will blur the image and alter the secret information. This was overcome

by using filters and Error Detectio and Correction Code technique. Figure 22 shows how data has been recovered from noise. The salt and pepper noise has been removed with the help of filter and EDCC.It ,is shown in Figures 25, 26, 27 and 28 and Histogram Analysis of the cover and stego images are picturised.

Removal of noise with percentage of noise

a Stego	b 70% of noise Added
c 90% noise added	d Recovered image
e Stego image	F Salt & Pepper
g. 50%noise reduced	70 h. 70 % noise reduced
i. 80%noise reduced	j.95% Noise reduced

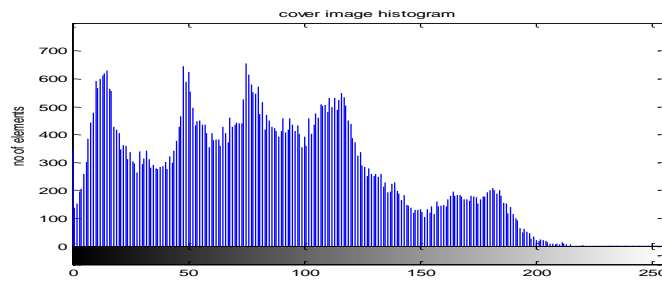


Figure 28 Lena original image histogram

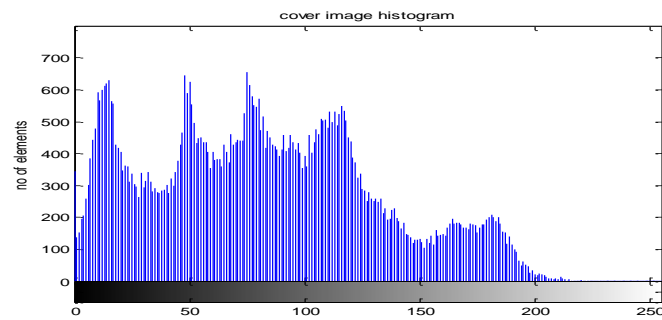


Figure 29 Lena stego image histogram

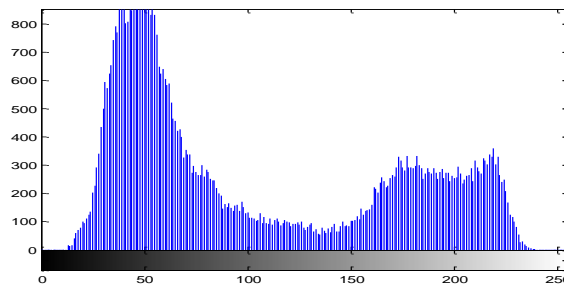


Figure 30 Flower original image histogram

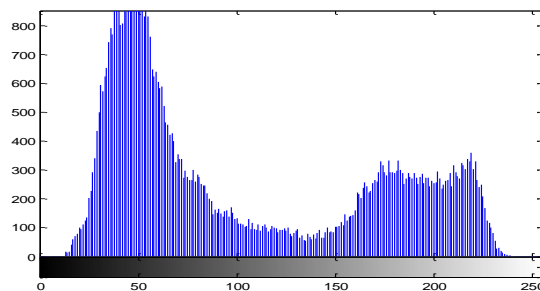


Figure 31 Flower(stego) histogram

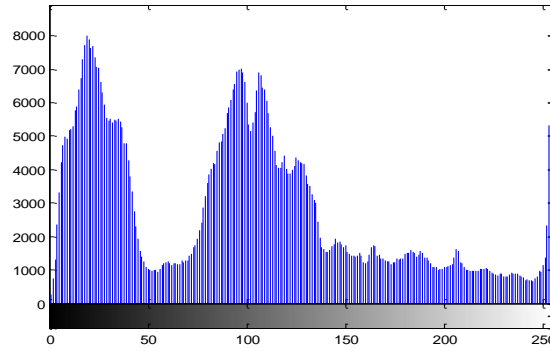


Figure 32 Simple original image histogram

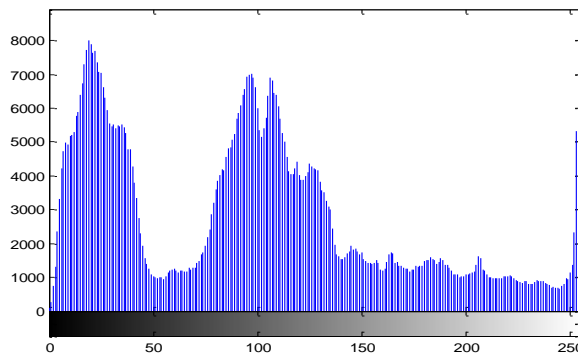


Figure 33 Simple(stego)image histogram

From the Figures 32 and Figure 33 shows that Histogram analysis for the simple (JPEG) original and stego images both are same but minute differences.

Error Detection and Correction Code technique

The simulated results for the proposed error detection and correction code technique turbo code where compared with the existing convolution code. The various parameters namely strength of the code, code rate, error rate for both Gaussian noise and salt& pepper noise and computational complexity were compared for both proposed turbo code and existing convolution code as shown in Table3. It is inferred from the results that the proposed EDCC outperforms the existing EDCC. The statistical analysis between cover and stego images were performed. The maximum embedding capacity was 15KB on a size of 25KB Lena cover image without degradation in histogram analysis and using EDCC it detect and correct more errors

From Table 4 shows results inferred by using EDCC turbo code technique as shown encoded message bits, adding noise corrupted messages bits and using median filter technique remove the salt pepper noise to recover the encoded bits.

Table3: Comparison of standard parameters for original cover image, stego image without noise and with noise.

IMAGE TYPE	STATASTICAL PARAMETERS	ORIGINAL IMAGE	WITHOUT FILTER	WITH FILTER
	MEAN	221.1375	248.2675	116.7175
	VARIANCE	0.7452	0.9384	0.2079

LENA	PSNR(dB)	24.1816	29.3824	32.9513
FLOWER	MEAN	68.8212	84.4712	98.8017
	VARIANCE	0.0705	0.1076	0.0107
	PSNR(dB)	22.1527	32.1423	36.6381
SIMPLE	MEAN	20.9835	22.7902	26.5369
	VARIANCE	0.0049	0.0073	0.0049
	PSNR(dB)	26..3478	30.6942	44.0600

CONCLUSION

A High capacity steganographic scheme using Dual Transform technique Discrete Wavelet Transform (DWT) and Integer Wavelet Transform (IWT) are implemented. The cover image is divided into 4*4 each and DWT is applied on each block. The resulting blocks of vertical band of 2*2 each are considered and IWT is applied to get 1*1 blocks. IWT coefficients of secret data are embedded into cover image to derive stego image. The Error Detection and Correction Code technique is used to ensure reliable communication. The resultant stego image obtained after embedding secret message does not show any change when compared to original image. Histogram and stastical analysis performed on the stego image proved that the proposed technique can effectively resist steganalysis.

REFERENCES

- [1] Liang Zhang, Haili Wang and Renbiao Wu, "A High-Capacity Steganography Scheme for JPEG2000 Baseline System", IEEE Transactions on image processing, vol.18, no. 8, pp.1797-1803, August 2009.
- [2] Jing-Ming Guo and Thah-Nam Le, "Secret Communication Using JPEG Double Compression", IEEE Signal processing letters, vol.17, no. 10, pp. 879-882, October 2010.
- [3] Chan, C.K., Chang, L.M., "Hiding data in image by simple LSBsubstitution," Pattern Recognition, vol 37, pp.469-471, March, 2003.
- [4] K. Satish, T. Jayakar, C. Tobin, K. Madhavi and K. Murali, "Chaosbased spread spectrum image steganography," IEEE transactions onconsumer Electronics, vol.50, no. 2, pp.587-590, April, 2004.
- [5] Chang, C. C., Chen, T.S and Chung, L. Z., "A steganographic method based upon JPEG and quantization table modification," Information Sciences, vol.4, pp. 123-138 (2002).
- [6] Chen,P. Y.and Liao,E.C., :A new Algorithem for Haar Wavelet Transform," 2002 IEEE International Symposium on IntelligentSignal Processing and Communication System, pp.453-457 (2002).
- [7] Z. Ni and Y. Shi, "Robust lossless image data hiding designed for semi-fragile image authentication, "IEEE Transactions on Circuits Systems Video Technology, vol. 18, no.4, pp.497-509, April 2008.
- [8] A. A. Abdelwahab and L. A. Hassan, "A discrete wavelet transform based technique image data hiding", In Proceedings of 25th National Radio Science Conference, Egypt, 2008.
- [9] Jaskolka, Jason Khedri and Ridha, "Exploring Covert Channels", Hawaii International Conference on System sciences, vol. 16, pp.1-7, April 2011.
- [10] Bhattacharyya S Kshitij and A P Sanyal G, "A Novel Approach to Develop a Secure Image Based Steganographic Model using Integer Wavelet Transform", International Conference on Recent Trends in Information, Telecommunication and computing, pp. 173-178, October 2010.
- [11] Sarreshtedari S and Ghaemmaghami S, "High capacity Image Steganography in Wavelet Domain", International Conference on Consumer Communications and Networking, vol. 21, pp.1-6, June 2010.
- [12] Chen Yongqiang, Hu Hanping and Chen Yongqiang, "Gray Image Watermark Algorithm in Integer Wavelet Transform Domain", International Conference on Electrical and Control Engineering, vol. 18, pp. 74-93, March 2010.
- [13] Kumar V and Kumar D, "Performance Evaluation of DWT based Image Steganography", IEEE International Conference on Advance Computing , vol. 8, pp.223-228, February 2010.



- [14] Liaw, Jiun-jian Wang, Wen-Sheng Chiu and Min-Yen, "A Data Hiding Method Using Secret Data Division and Pixel value Differencing", International Conference on Genetic and Evolutionary Computing, vol. 6, pp. 650-654, June 2010.
- [15] R O El Safy, H H Zayed and A El Dessouki, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform", International Conference on Networking and Media Convergence, pp. 111-117, March 2009.
- [16] Herbert Taub, Donald L Shilling and Goutam Saha, "Principles communication Systems", McGraw-Hill Education Private Limited, May 2009.
- [17] Xuan G., Shi Y.Q., Yang C., Zhang Y., Zou D. and Chai P, Kumar "Lossless Data Hiding using integer wavelet transform, and threshold embedding technique", IEEE International workshop on Multimedia Signal Processing, vol. 64, pp.9-11, December 2002.