Performance Evaluation of DWT Based Image Steganography

Vijay Kumar
Department of Computer Science & Engineering
J C D M College of Engineering,
Sirsa, Haryana, INDIA
vijaykumarchahar@gmail.com

Dinesh Kumar
Department of Computer Science & Engineering
Guru Jambheshwar University of Science & Technology
Hisar, Haryana, INDIA
dinesh_chutani@yahoo.com

***Abstract*—Steganography plays an important role in the field of information hiding. It is used in wide variety of applications such as internet security, authentication, copyright protection and information assurance etc. In Discrete Wavelet Transform (DWT) based steganography approaches the wavelet coefficients of the cover image are modified to embed the secret message. DWT based algorithm for image data hiding has been proposed in the recent past that embeds the secret message in CH band of cover image. This paper intends to observe the effect of embedding the secret message in different bands such as CH, CV and CD on the performance of stegano image in terms of Peak Signal to Noise Ratio (PSNR). Experimentation has been done using six different attacks. Experimental results reveal that the error block replacement with diagonal detail coefficients (CD) gives better PSNR than doing so with other coefficients.**

Keywords-steganography; discrete wavelet transform

I. INTRODUCTION

Due to advancement in multimedia processing technologies, it has been possible to exchange large amount of multimedia data over a wide variety of networks. The use of internet makes creation, edition, deletion and/or distribution of digital images, audio/ video very easy and at low cost. However, the data transmitted through internet may not be safe. Cryptography and steganography techniques are two preferred techniques among the number of data hiding techniques used for protection of data [1, 16, 18]. Though these two are related, but there is a difference between them. The former one scrambles messages in such a way that these are not easily understood by others. It does ensure the existence of message. Whereas the latter one conceals the fact that message exists by hiding the actual message in another media [18, 19].

The problem with cryptography is that encrypted message is obvious. The fact that anyone can observe encrypted messages during transmission makes cryptography less preferable as compared to steganography that provides the additional protection on a secret message [19]. The other two techniques that are closely related to steganography are watermarking and fingerprinting. These techniques are mainly used for protection of intellectual property. The algorithms have different requirements than those required for steganography [20].

There are two approaches related to steganography i.e., spatial-domain and frequency-domain approach [13]. In the former approach, the secret messages are embedded into least significant pixels of cover images. They are fast but sensitive to image processing attacks. The latter approach contains transforming the cover image into the frequency domain coefficients before embedding secret messages in it. The transformation can be either Discrete Cosine transform (DCT) and Discrete Wavelet Transform (DWT) etc. Though these methods are more difficult and slower than spatial domain, yet they have an advantage of being more secure and noise tolerant [20].

In this paper, we observe the effect of embedding the secret messages into different bands of cover image. The PSNR has been used as a measure of quality of stegano image. The remainder of this paper is organized as follows. Section 2 presents the related works. Section 3 presents DWT based steganography approach. Section 4 shows the experimentation and results followed by conclusions in section 5.

II. RELATED WORKS

A brief description of related works is presented in this section.

Least Significant Bit Substitution (LSB) [9] is the most frequently used stenographic technique. The basic concept of Least Significant Bit Substitution is to embed the secret data at the bits which having minimum weighting so that the embedding process will not significantly affect the original pixel value. In [10], a spatial domain approach, the authors proposed exploiting the correlation between adjoining pixels for determining the bit number to be embedded at certain specific pixel. Employing the variance between adjoining pixels, it is convenient to estimate whether a pixel is located in edge area or not. If the pixel is located in edge areas, we can embed more data than the smooth areas.

In [11], a frequency domain approach, the authors proposed that embedding is realized in bit planes of subband wavelet coefficients obtained by using the Integer Wavelet transform. In [12], authors proposed a new frequency domain method for image steganography. In this system, first transform the cover image into sub bands. The secret image is embedded into LL

978-1-4244-4791-6/10/$25.00 ©2010 IEEE

subband of cover image. Tsuang-Yuan et al. [2] proposed a new method for data hiding in Microsoft word documents by a change tracking technique. Sinha and Singh [3] proposed a technique to encrypt an image for secure transmission using digital signature of the image. Digital signatures enable the recipient of a message to verify the sender of a message and validate that the message is intact.

Kisik et al. [4] proposed a stegnographic algorithm which embeds a secret message into bitmap images and palette-based images. The algorithm divides a bitmap image into bit plane images from LSB-plane to MSB-plane for each pixel. Satish et al. [7] proposed a chaos based spread spectrum image steganography method. This method can be used for ensuring security and privacy. The majority of LSB steganography algorithm embed message in spatial domain such as pixel value differencing [5, 6].

III. Discrete Wavelet Transform Based Steganography Approach

Discrete Wavelet Transform based steganography approach was proposed by Ahmed A. Abdelwahab et al. [20]. In this approach, the cover image is decomposed into four sub-images such as approximation coefficients (CA), horizontal detail coefficients (CH), vertical detail coefficients (CV) and diagonal detail coefficients (CD). Similarly, the secret image is decomposed into four sub-images. These sub-images are divided into non-overlapping blocks. The blocks of approximation coefficients of cover image are subtracted from approximation coefficient of secret image. The differences of these coefficients are called error blocks. The replacement of an error block is being done with the best matched CH block.

In this paper, besides using CH block, we have done experimentation using CV and CD blocks also to see the effect on PSNR of the stegano image using the algorithm as proposed by Ahmed A. Abdelwahab et al. The experimental work includes six different attacks.

A. Embedding Procedure

The steps of embedding procedure are as follows [20]:

Step1. Decompose the cover image (*I* matrix) and the secret image *S* into four sub-images (*ICA*, *ICH*, *ICV*, *ICD*) and (*SCA*, *SCH*, *SCV*, *SCD*) respectively using DWT.

Step2. Each of *SCA*, *ICA*, *and ICH* are partitioned into blocks of 4×4 pixels and can be represented by:

$$SCA=\{BS_i, 1\le i\le ns\} \quad (1)$$

$$ICA=\{BC_j, 1\le j\le nc\} \quad (2)$$

$$\mathrm{ICH}=\{\mathrm{BH_k}, 1\le \mathrm{k}\le \mathrm{nc}\} \quad (3)$$

where BS_i, BC_j, and BH_k represent the i^{th} block in *SCA*, the j^{th} block in *ICA* and the k^{th} block in *ICH* respectively, ns is the total number of the 4×4 blocks in *SCA* and nc is the total number of the 4×4 blocks in each of *ICA* and *ICH*.

Step3. For each block BS_i in *SCA*, the best matched block BC_j of minimum error in *ICA* is searched by using the root mean squared error (RMSE).The first secret key K1 consists of the addresses *j* of the best matched blocks in *ICA*.

Step4. Calculate the error block EB_i between BS_i and BC_j as follows:

$$EB_i = BC_j - BS_i \quad (4)$$

Step5. For each error block EB_i, the best matched block BH_k in *ICH* is searched for using the RMSE criteria as before and that BH_k is replaced with the error block EB_i. The second secret key K2 consists of the addresses *k* of the best matched blocks in *ICH.*

Step6. Repeat the steps 3 to 5 until all the produced error blocks are embedded in *ICH*.

Step7. Apply the inverse DWT to the *ICA*, *ICV*, *ICD*, and the modified sub-image *ICH* to obtain the stegano-image.

B. Extraction Procedure

In this technique, by receiving the stegano-image *G* and the secret keys from the sender, the steps of secret image extraction procedure are as follows [20]:

Step1. Decompose the stegano-image *G* into four sub-images (*GCA*, *GCH*, *GCV*, *GCD*) using DWT transform.

Step2. Extract the block BC_j from the sub-image *GCA* by using the first secret key K1. Use the second secret key K2 to extract the error block. The secret block BS_i can be obtained by:

$$BS_i = BC_j - EB_i \quad (5)$$

Step3. Repeat step 2 until all secret blocks are extracted and form the sub-image *SCA*.

Step4. Assign each of sub-images *SCD*, *SCV*, *SCH* as zeros, and apply the inverse DWT to obtain the embedded secret image which is visually similar to the original image.

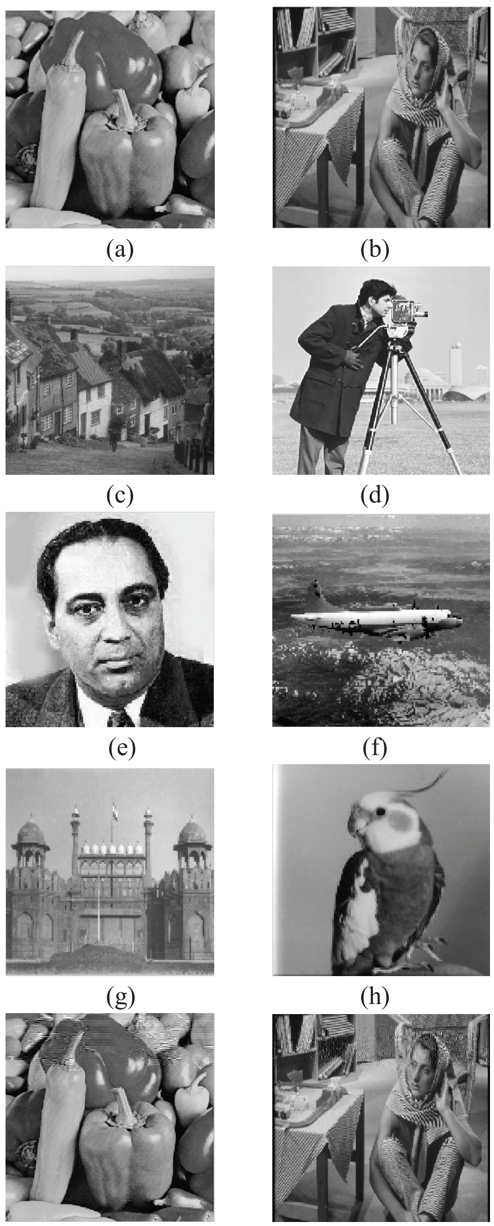
In this paper, experimentation has been done taking into consideration *ICH*, *ICV* and *ICD* separately.

IV. Experimentation and Results

A. Experiment 1 and results:

Our experimental work considers four cover images: Peppers, Barbara, Goldhill and Cameraman, each of size 256×256 and four secret images: Homi Bhaba, Redfort, Airplane and bird, each of size 128×128. The image Homi

Bhaba was embedded into cover image Peppers. Likewise, we embed the image Redfort into Goldhill cover image, Airplane into Barbara cover image and Bird into Cameraman cover image. We use Peak signal to Noise Ratio (PSNR) to measure the quality of stegano images and secret images. Figure 1 shows the cover images, secret images, Stegano images and extracted secret images. The experimental results are tabulated in tables 1, 2, 3, 4 and 5.



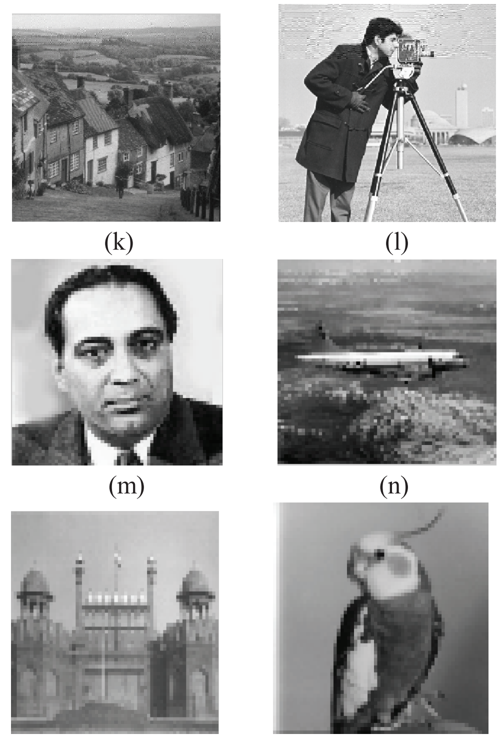


Fig. 1 Cover images; (a) Peppers (b) Barbara (c) Goldhill (d) Cameraman, Secret images; (e) Homi Bhaba (f) Airplane (g) Redfort (h) Bird , Stegano images; (i) Peppers as cover and Homi as secret (j) Barbara as cover and Airplane as secret (k) Goldhill as cover and Redfort as secret (l) Cameraman as cover and Bird as secret and Extracted Secret images;(m) Homi Bhaba (n) Airplane (o) Redfort (p) Bird .

Tables 1, 2 and 3 show the PSNR values of stegano images after embedding the secret images in CH, CV and CD bands of cover images. The results reveal that stegano image after embedding in CD band has higher PSNR value than the other two. The PSNR value of extracted secret image is same in all three sub-bands and is given in table 4.

B Experiment 2 and results:

The next experiment was performed to see the effect of chosen attacks such as Gaussian noise, Sharping, median filtering, Gaussian blur, Histogram Equalization and Gamma Correction. First attack applied on the image is Gaussian noise with zero mean and 0.001 variance. Second attack is Sharping. The third attack is median filtering. The fourth attack is blurring using low pass filter of 3×3 window size. The fifth attack is median filtering. Last attack, we applied is Gamma correction. Figures 2 and 3 show the stegano images and extracted secret images respectively after applying attacks. The PSNR values for three different stegano images and extracted secret images after different image processing attacks are shown in tables 5, 6 and 7.

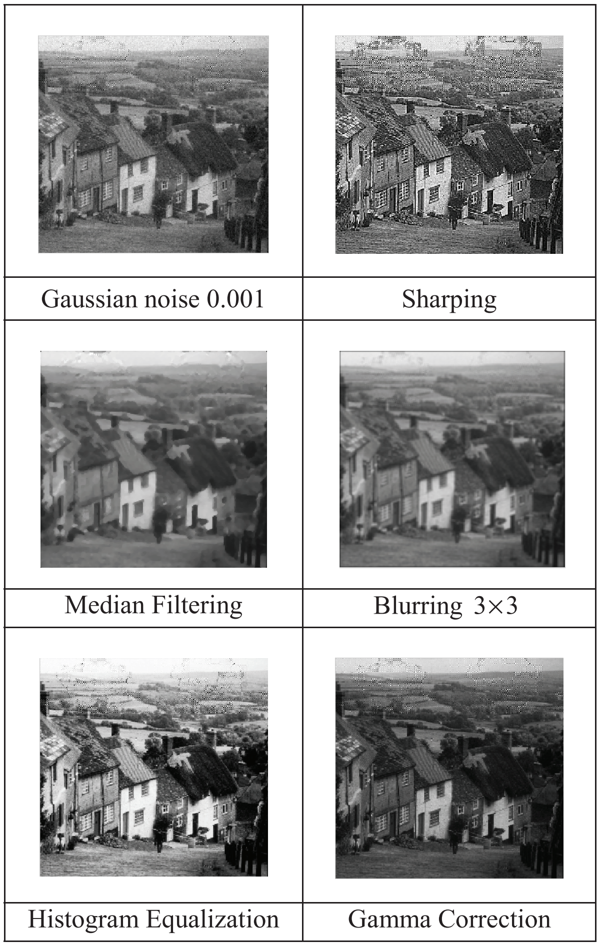
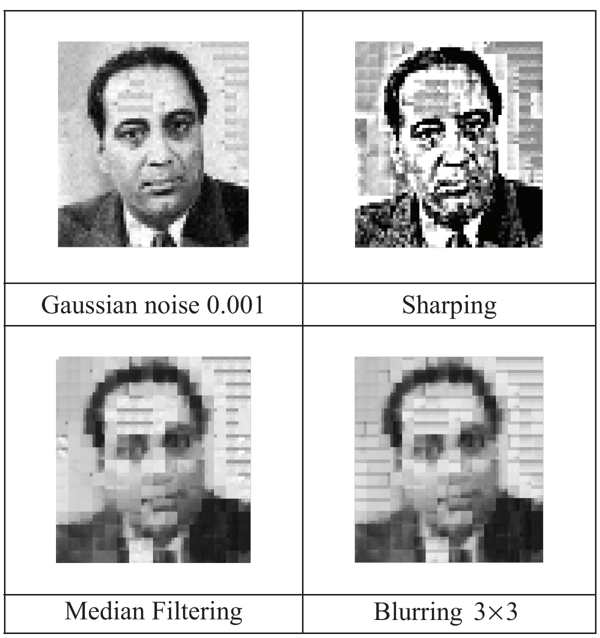


Figure2. Attacked Goldhill stegno images



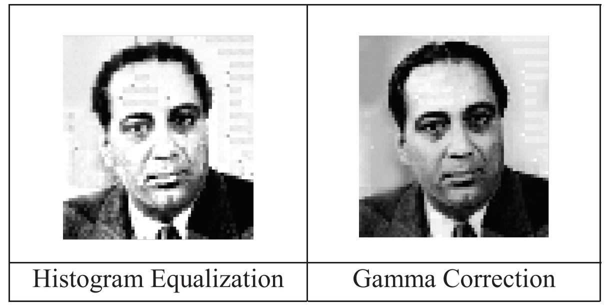


Figure3. Extracted Homi Bhaba images from Goldhill stegano images

The results shown in tables 5, 6 and 7 reveal that after applying attacks on stegano images, the secret images have high value of PSNR and hence the good visual quality.

V. CONCLUSIONS

In this paper, we observe the effect of embedding the secret messages into different bands of cover image. Experimental results show that error block replacement in diagonal detail coefficients (CD) gives better Peak Signal to Noise Ratio (PSNR) as compared to PSNR obtained when using the replacement with other coefficients (CV and CD).

REFERENCES

[1] N.F. Johnson and S. Katzenbeisser, "A survey of steganography techniques," in S. Katezenbeisser and F. Peticolas (Eds): Information Hiding , pp.43-78, Artech House, Norwood, MA, 2000

[2] L. Tsung-Yuan, T. Wen-Hsiang, "A New Steganography method for data hiding in Microsoft Word documents by a Change Tracking Technique," IEEE transaction on Information forensics and security , vol. 2, issue 1, pp.24-30, 2007

[3] A. Sinha and K. Singh, "A technique for image encryption using digital signature," optics communications, vol. 218, no.4, pp.229-234, 2003

[4] EE. Kisik Chang, J. Chango and L. Sangjin, "High Quality Perceptual Steganography Techniques," Springer, vol.2939, pp.518-531, 2004

[5] D.C. Wu and W.H. Tsai, "A Steganography method for images by pixel value differencing," Pattern Recognition Letters, pp.1613-1626, 2003

[6] X.Zhang and S.Z.Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security," Pattern Recognition Letters, pp.331-339, 2004

[7] K. Satish, T. Jayakar, C. Tobin, K. Madhavi and K. Murali, "Chaos based spread spectrum image steganography," IEEE transactions on consumer Electronics, vol.50, issue 2, pp.587-590, 2004

[8] Sas Agaian, "Steganography and Steganalysis: an overview of Research and Challenges," Network Security and Intrusion Detection, NATO Proceedings, 2005

[9] Chan, C.K., Chang, L.M., "Hiding data in image by simple LSB substitution," Pattern Recognition, vol 37, pp.469-471, 2003

[10] Chang, C.C, Tseng, H.W., "A Steganographic method for digital images using side match," Pattern Recognition, vol. 25, pp.1431-1437, 2004

[11] S. Tarres, M. Nakano and H. Perez, "An Image steganography Systems based on BPCS and IWT," 16 th International conference on Electronics, Communications and Computers, pp.51-56, 2006

[12] Po-Yueh Chen and Yue-chi Tseng, "A Study of DWT based steganography using Coefficient analysis," pp.242-248, 2007

[13] Chang, C.C, Chen, T.S and Chang, L.Z, "A Steganographic method based upon JPEG and Quantization table modification," Information Science, vol.141, pp.123-138, 2002

[14] A. Pommer and A. Vhl, "Wavelet Packet methods for multimedia compression and encryption," IEEE Pacific Rim Conference on Communications, Computer and signal processing, pp.1-4, Victoria, Canada, 2001

[15] X. Yi, "Fast Encryption for multimedia," IEEE transactions on Consumer Electronics, vol. 47, issue 1, pp. 101-107, 2001

[16] MAB. Younes, A. Jantan, "Image Encryption using Block-Based Transformation Algorithm," International Journal of Computer Science, vol. 35, issue 1, pp.15-23, 2008

[17] H. Zenon, V. Sviatoslov and R. Yuriy, "Cryptography and steganography of video information in modern communications," 1998

[18] M.M. Amin, M. Salleh, S. Ibrahim and M.Z.I. Shamsuddin, "Information hiding using Steganography," National Conference on Telecommunication Technology, pp.21-25, 2003

[19] Mohammad Ali Bani younes, and AmanJantan, "A New Steganography approach for image encryption exchange by using the Least Significant Bit Insertion," International Journal of Computer Science and Network security, vol. 8, No. 6, pp. 247-253, 2008

[20] Ahmed A. Abdelwahab and Lobha A. Hassan, "A Discrete Wavelet Transform based Technique for image data hiding," 2nd National Radio Science Conference, pp. 1-9, Egypt, 2008

[21] V.M Potdar, S. Han, and E. Chang, "A survey of Digital Image Watermarking Techniques," 3rd IEEE International Conference on Industrial informatics, 2005

TABLE I. THE PSNR OF COVER IMAGE AFTER EMBEDDING IN CH BAND

Cover images (256×256)	Secret images (128×128)			
	Homi	Airplane	Redfort	Bird
Peppers	24.9107	27.2455	29.9537	29.6487
Goldhill	25.3385	28.0788	30.1460	29.5505
Cameraman	26.5329	27.0287	29.0293	28.0547
Barbara	24.2305	27.1889	29.2020	29.1018

TABLE II. THE PSNR OF COVER IMAGE AFTER EMBEDDING IN CV BAND

Cover images (256×256)	Secret images (128×128)			
	Homi	Airplane	Redfort	Bird
Peppers	24.8689	27.3004	29.9793	29.5865
Goldhill	25.5264	28.3188	30.8176	29.9979
Cameraman	26.2302	26.8453	28.8480	28.0313
Barbara	23.3890	26.1639	27.4963	27.4015

TABLE III. THE PSNR OF COVER IMAGE AFTER EMBEDDING IN CD BAND

Cover images (256×256)	Secret images (128×128)			
	Homi	Airplane	Redfort	Bird
Peppers	25.1024	27.7162	30.7849	30.3551
Goldhill	25.5766	28.4215	30.9055	30.1924
Cameraman	26.6422	27.3910	29.7531	28.6094
Barbara	24.5379	27.9162	30.3389	30.1200

TABLE IV. EXTRACTED SECRET IMAGE

Cover images (256×256)	Extracted secret images (128×128)			
	Homi	Airplane	Redfort	Bird
Peppers	23.5329	22.3544	26.1742	28.8265
Goldhill	23.5329	22.3544	26.1742	28.8265
Cameraman	23.5329	22.3544	26.1742	28.8265
Barbara	23.5329	22.3544	26.1742	28.8265

TABLE V. THE PSNR OF STEGNO-IMAGE GOLDHILL AND EXTRACTED HOMI UNDER DIFFERENT ATTACKS

Images after attack	Image Processing Attack					
	Median Filtering	Sharping	Histogram Equalization	Gaussian Blur	Gamma Correction	Gaussian Noise
Stegno-image Goldhill	26.6800	16.0623	16.9690	25.6657	22.5282	25.1056
Extracted Homi	17.5449	15.2715	18.9282	16.8314	25.0332	22.0608

TABLE VI. THE PSNR OF STEGNO-IMAGE BARBARA AND EXTRACTED REDFORT UNDER DIFFERENT ATTACKS

Images after attack	Image Processing Attack					
	Median Filtering	Sharping	Histogram Equalization	Gaussian Blur	Gamma Correction	Gaussian Noise
Stegno-image Barbara	28.3512	17.0031	20.1865	26.3821	19.1236	27.8336
Extracted Redfort	21.7709	17.9317	19.6252	21.0677	20.3607	25.2781

TABLE VII. THE PSNR OF STEGNO-IMAGE PEPPERS AND EXTRACTED BIRD UNDER DIFFERENT ATTACKS

Images after attack	Image Processing Attack					
	Median Filtering	Sharping	Histogram Equalization	Gaussian Blur	Gamma Correction	Gaussian Noise
Stegno-image Peppers	28.4738	16.1707	19.1366	26.3291	16.6721	26.6781
Extracted Bird	23.9203	15.7403	20.2270	22.4901	17.1634	27.3192