Block Based Image Steganography in Spatial and Frequency Domain

D.N.F Awang Iskandar[1], Abdulmalik Bacheer Rahhal[1,2] and Wadood Abdul[2]
[1]*Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia.*
[2]*Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Kingdom of Saudi Arabia.*
dnfaiz@unimas.my

***Abstract*—Steganography is the art of hiding a secret message in different kind of multimedia (image, voice or video), such that the secret message is not detectable. In this paper, we propose two new algorithms, first one uses the spatial domain for steganography, where the host image is converted into blocks of bit-planes to insert the secret information. The algorithm divides the image into 8 bit planes and then the bit planes are further divided in to N x N blocks. The hidden message is inserted based on a chaotic sequence. We intend to find the most optimum bit plane to insert the hidden information, keeping high imperceptibility in terms of the human visual systems. The algorithm shows relatively good Mean Structural Similarity and Peak Signal to Noise Ratio values. The second algorithm is applied in the frequency domain where the host image is converted using the discrete wavelet transform. Then at second and third level of the transform, the secret information is inserted. The proposed algorithm divides wavelet level divide in to M x M blocks. The hidden message is inserted based on chaotic sequence in to the blocks. This algorithm shows better imperceptivity in terms of the human visual system and PSNR.**

***Index Terms*—Bit Plane; Force of Insertion; Spatial Domain Steganography; Wavelet Domain.**

I. INTRODUCTION

Steganography and encryption are used to transfer secret information. Steganography attempts to hide the transfer of information whereas encryption attempts to make it computationally difficult for an adversary to decrypt the encrypted information [1].

The main purpose of steganography or data hiding is to hide or protect important information for some application. As an example of why two parties wish to have secret communication, it can be used for a political reason as in case of a dissident organization wishing to communicate among themselves. It is also used in the medical field where patients do not want their identity to be linked to their medical records. The multimedia file is only accessible to the doctor and not to anyone else thus preserving the privacy of the patient through steganography.

The main objective of steganography is to ensure communication secrecy and security using different kinds of multimedia, we developed novel imperceptible algorithms for steganography in the spatial and frequency domains. These algorithms are evaluated and compared with other algorithms found in the literature.

The rest of the paper is organized as the follows. In the next section we present the related work. In section III, the proposed block steganography algorithm is described. In Section IV, results are illustrated followed by the capacity analysis and comparison. We conclude our findings in section V.

II. RELATED WORK

The steganographic algorithms are classified in to the spatial domain algorithms and frequency domain algorithms [2].

A. Spatial Domain Steganography

The Least Significant Bit (LSB) replacing is the most important data hiding method. It is a simple method with high embedding capacity but the hidden data is sensitive to image alteration and vulnerable to attacks [3-8]. In the frequency domain, the image is decomposed into transformed components by using transforms like the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) [3] and Discrete Wavelet Transform (DWT) [4],[5], [6]. These components are modified according to the embedding algorithm to insert the secret data. Hiding data in the frequency domain has certain advantages over hiding in the spatial domain; it provides higher robustness against changes and attacks, which means more resistance to loss from image manipulation and increased difficulty for a potential attacker. However, it is relatively costly in terms of complexity [3, 11], also the amount of secret data that can be hidden in frequency domain is less than the LSB scheme [7].

Bandyopadhyay et al. in [8] proposed a 3-3-2 LSB (three, three and two least significant bits from the red, green and blue color components respectively) insertion method in RGB color pixels. This pattern distribution is considered because the human eye is more sensitive to changes in the blue color component compared to the red and green color components. The secret image is inserted into the cover image using chaotic sequence and XOR operation.

In a similar method Amritpal Singh and Harpal Singh proposed 2-2-4 LSB (two, two and four significant bits from red, green and blue color components respectively) insertion method in RGB pixels respectively. Experimental results in [8] and [9] show better PSNR for Lenna image in [9] compared with [8], but on the other hand the algorithm proposed in [4] has less capacity.

In [10] authors proposed spatial domain steganography algorithm based on reversible logic. They use Feynman gate to achieve reversibility for the image with simple LSB technique. A nano-communication circuit for image steganography is shown using proposed encoder/decoder

circuit. The algorithm shows 28.33% enhancement in terms of area over complementary metal–oxide–semiconductor circuit.

In [11] Junlan et al. introduced new technique combining LSB and edge detection to improve invisibility. The cover image I of the algorithm is converted in to Imsb by clearing five LSB of each pixel to perform edge detection. Each pixel will be either edge area or non-edge area. The pixel which belong to edge area is used to embed secret data.

In [12] Shreyank and Sumit propose a secure steganography algorithm. They propose to break down the data to be sent in to N blocks, then encode each block of data in one image from poll of images using standard LSB algorithm. This set of images are sent in random order. A hash table is created which keeps record of the correct sequence of blocks and the corresponding images used for inserting the blocks.

In [13] Nag et al. proposed a new spatial domain method for image steganography using X-Box mapping. They generate four different X-Boxes (using XOR operation), and then the image is encrypted based on X-Box values. Finally, the encrypted values are inserted in 4 LSB bits of the cover image. The basic advantage of this approach is that the stego key is not required.

In [14] and [15] Shivani et al. proposed Zero Distortion Technique (ZDT) based on chaotic sequence. ZDT depends on extracting bits from the cover image in order to generate the text which is to be hidden. Then the locations of the pixels which are matching secret bits are stored.

In [16], the authors use LSB insertion method using chaos in the spatial domain. The main advantage of chaos theory is simplicity of implantation, more randomness than traditional pseudo random generators, non-periodicity and confidentiality. In a similar way to [8] they generate chaotic binary sequence XORed with the secret message, each XORed bit is again XORed with LSB of the selected pixel of the cover image. The algorithm presented in [16] outperforms the one presented in [8] in terms of imperceptibility with regard to PSNR (Peak Signal to Noise Ratio).

In [17] LSB embedding methods are secured by proposing a Histogram Preserving Stganographic (HPS) technique. By utilization of randomization scheme, this method is equipped to secure and preserve the histogram of the cover images. In this scheme, they partitioned the intensity scale into small chunks in order to minimize the visual distortion. In this method, they also restricted the intensity modulation inside the same section to minimize the loss of information. The method is resistant to numerous steganalysis schemes.

B. Frequency Domain Steganography

Elham et al. in [4] worked in the frequency domain. They used genetic algorithm to choose best discrete wavelet coefficient to insert the secret message. They used frequency domain to improve robustness of their algorithm. Also using genetic algorithm improves the hiding capacity with low distortion. This merger between two techniques gives PSNR equal to 39.94 dB with capacity equal to 4 bpp.

In [18] author apply steganography algorithm on ECG images to secure patient information. Edward and Ramu use curvelet transform on the images to convert 1D ECG images in to 2D images. A quantization approach is used to replace around zero coefficient with secure data. Author use PSNR and BER to evaluate the algorithm using MIT-BIH database.

In [5] Soodeh Ahani and Shahrokh Ghaemmaghami used sparse representation for more security to hide a message. They use wavelet transform for non-overlapping blocks of a color image. All four sub-images of the two-dimensional wavelet transform of two color bands are used for data embedding without affecting the image perceptibility. Capacity of the proposed method is about 1 bpp (bit(s) per pixel). The results show that the embedded data is invisible. The average PSNR of the algorithm is about 40 dB. The security of the method is evaluated using five steganalysis techniques which are unable to detect the hidden message. The authors used INRA and HOLIDAYS databases to show the effectiveness of their algorithm.

In [6] Sarreshtedari and Ghaemmaghami used frequency domain with 2D wavelet transform, they segmented the transformed image into blocks and used secret key to determine the order of blocks selected for embedding. They determine the capacity of each block using Bit Plan Complexity Segmentation (BPCS) algorithm. The embedding rule is: the pixel value is changed into the nearest integer with last LSB bit equal to the input bits. Then generate stego image by computing inverse 2D wavelet transform. In [3] authors use frequency domain, they used least significant bit number in each DCT coefficient for data hiding which depends on the characteristics of the image according to Human Visual System (HVS).

III. PROPOSED BLOCK BASED STEGANOGRAPHY ALGORITHMS

In this paper, we propose two cases of block based steganography, the first one in the spatial domain; we call this algorithm bit plane block steganography and the second one in the frequency domain; we call this algorithm wavelet block steganography. We will discuss each one separately.

A. Bit Plane Block Steganography

The proposed bit plane steganography algorithm divides the image into N×N blocks of 8-bit planes for a gray scale image. The hidden information is inserted into random blocks based on a chaotic sequence. The insertion procedure takes into account the local mean L (block of N×N) and global mean G (whole image) according to Equation (1):

$$L'_{B(a,b)} = \begin{cases} (1+\partial)G_B, & if\ M_{(i,j)} = 1 \\ (1-\partial)G_B, & if\ M_{(i,j)} = 0 \end{cases} \quad (1)$$

where $L'_{B(a,b)}$ is the new mean value of block (a, b) in bit plane B, G_B is mean value of bit plane B, ∂ is the force of insertion used for hiding the information, M is the message bit.

Now to change the local mean of the block ($L'_{B(a,b)}$), f number of randomly selected bits are flipped in the particular block, where f is calculated using Equation (2):

$$f = \lceil L' - L \rceil N^2 \quad (2)$$

In the extraction phase, the local and global mean values are compared for blocks specified by the chaotic secret key and the decision of '1' or '0' is reached based on Equation (3):

$$M_{(i,j)} = \begin{cases} 1, & if\ L'_{B(a,b)} \geq G_B \\ 0, & if\ L'_{B(a,b)} < G_B \end{cases} \quad (3)$$

The secret message insertion procedure for the bit plane block steganography algorithm is illustrated in Figure 1.

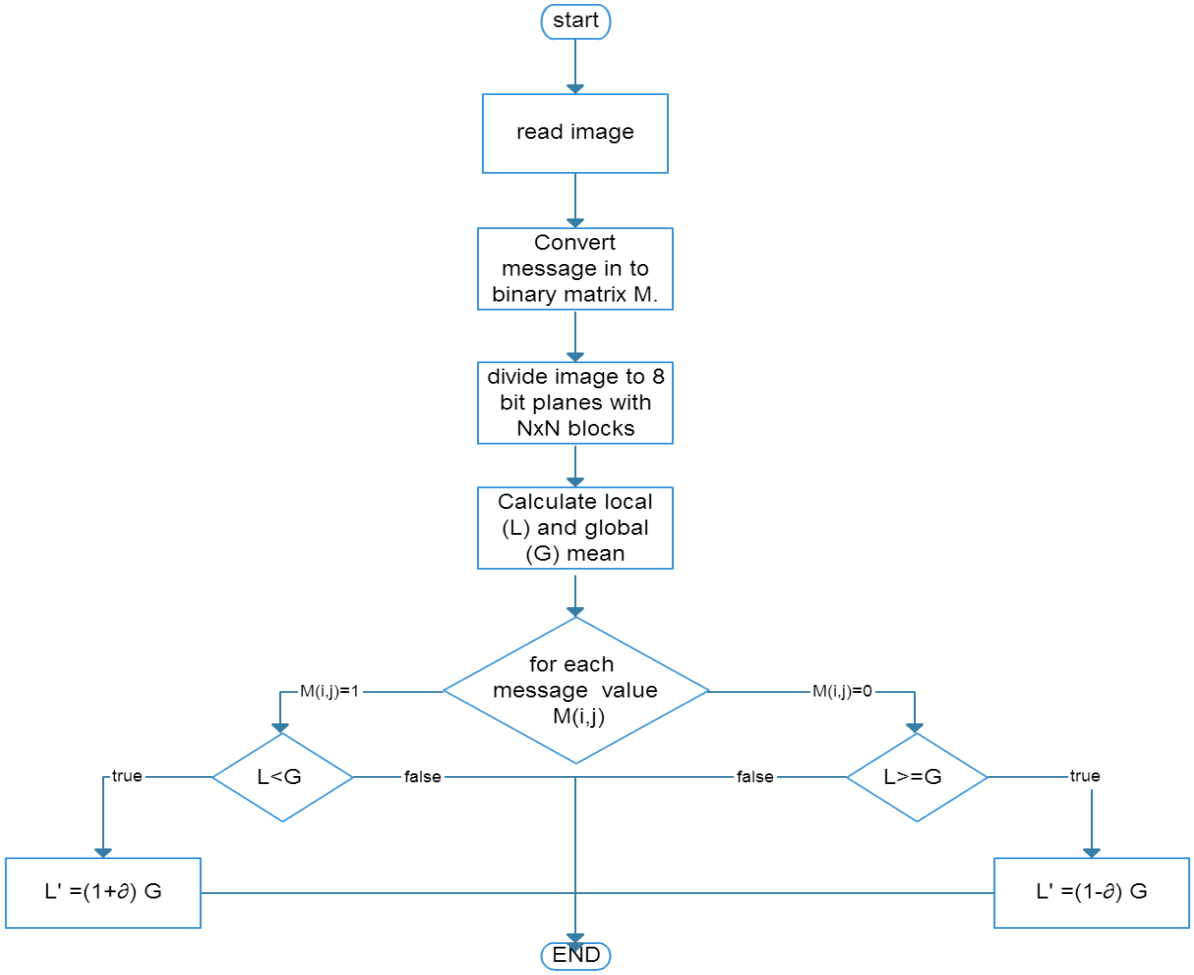

Figure 1: Secret message insertion procedure for the bit plane block steganography algorithm.

B. Wavelet Block Steganography

The standard technique of storing in the least significant bits (LSB) of a pixel still applies. The only difference is that the information is stored in the wavelet coefficients of an image, instead of changing bits of the actual pixels. The idea is that storing in the least important coefficients of each 4 x 4 Haar transformed block will not perceptually degrade the image.

In this proposed algorithm, for insertion process we applied three level of wavelet transform on the image, then we divided the second and third level of diagonal coefficients into 4×4 blocks. Based on the chaotic sequence binary key and inserted bit we increase or decrease the value of the block coefficients to force the local average to be either less than the average of local mean in case inserted bit is zero or greater than the local mean in case inserted bit is one as given by Equation (4) in case insertion is carried out in the second level and Equation (5) in case insertion is carried out in the third level:

$$\mathrm{BC}_{(a,b)} = \begin{cases} \mathrm{BC}_{(a,b)} + \left(L_{B(a,b)}\right) + abs(\partial 1 \times G_B), & if\ M_{(i,j)} = 1 \\ \mathrm{BC}_{(a,b)} - \left[\mathrm{abs}\left(L_{B(a,b)}\right) + abs(\partial 1 \times G_B)\right], & if\ M_{(i,j)} = 0 \end{cases} \quad (4)$$

$$\mathrm{BC}_{(a,b)} = \begin{cases} \mathrm{BC}_{(a,b)} + \mathrm{abs}\left(L_{B(a,b)}\right) + abs(\partial 2 \times G_B), & if\ M_{(i,j)} = 1 \\ \mathrm{BC}_{(a,b)} - \left[\mathrm{abs}\left(L_{B(a,b)}\right) + abs(\partial 2 \times G_B)\right], & if\ M_{(i,j)} = 0 \end{cases} \quad (5)$$

where $\mathrm{BC}_{(a,b)}$ represents the coefficients of lock(a,b), G_B is the mean value at the decomposition level, and ∂ is the force of insertion for the hidden information, where $\partial 2 = \frac{\partial 1}{10}$ was found to be the best ratio for the imperceptibility requirement through the PSNR measure.

The capacity C for an X×Y image is given by Equation (6):

$$C \approx \frac{d \times X \times Y}{2^l \times 2 \times N^2} \text{ bit} \quad (6)$$

where N is block size, l is wavelet level and d is number of directional sub-bands. In our case N and d are equal to 3.

In the extraction phase, the local and global mean values are compared for blocks specified by the chaotic secret key and the decision of '1' or '0' is reached based on Equation (7):

$$M_{(i,j)} = \begin{cases} 1, & if\ L'_{B(a,b)} \geq G_B \\ 0, & if\ L'_{B(a,b)} < G_B \end{cases} \quad (7)$$

The secret message insertion procedure for the wavelet block steganography algorithm is illustrated in Figure 2.

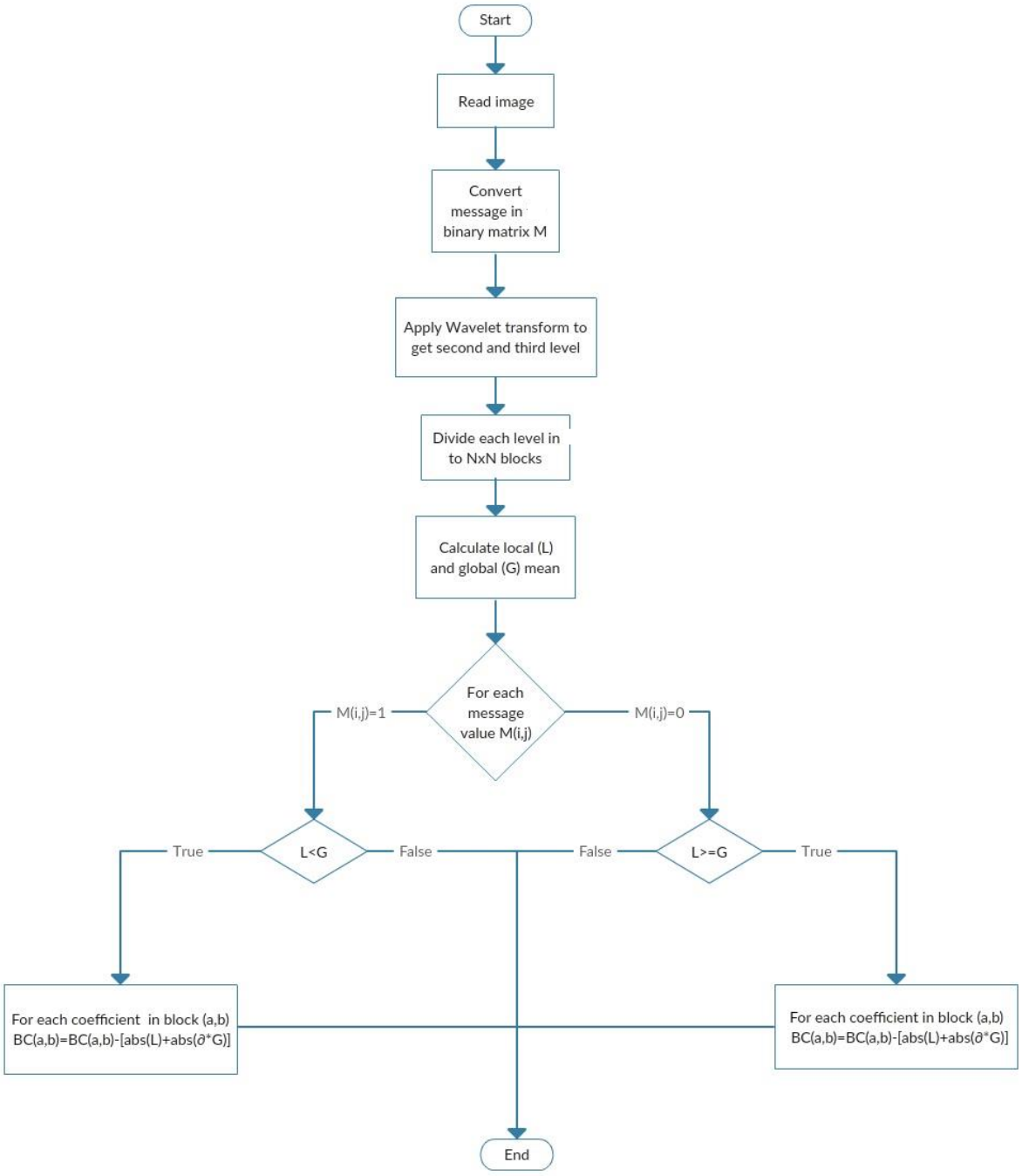

Figure 2: Secret message insertion procedure for the wavelet block steganography algorithm.

IV. EXPERIMENTAL RESULTS

To evaluate the proposed algorithms BOSS database is used. It contains 10000, 512×512 gray scale images. We used BOSS database for both algorithms. In order to measure the invisibility of the proposed algorithm, three error metrics are used, PSNR, Mean Square Error (MSE) and Mean SSIM (MSSIM) [19]. The PSNR demonstrates the value of the peak error, however MSE shows the cumulative squared error among the original and modified images. Low error is indicated by a small value of MSE. MSE is computed by using Equation 8:

$$MSE = \frac{\sum_{XY}[I_1(x,y) - I_2(x,y)]^2}{X \times Y} \quad (8)$$

while PSNR is computed by using Equation 9:

$$PSNR = 10 \times \log_{10}\left(\frac{R^2}{MSE}\right) \quad (9)$$

where R is the maximum gray scale value of a pixel in the image under consideration.

(SSIM) give a clearer understanding of imperceptibility specially when modeling the human visual system in applications like compression and data hiding.

A. Spatial Domain Steganography Results

a. Imperceptibility Analysis

To find out the most optimal bit plane to insert the hidden information, we inserted the hidden information into each bit plane and carried out objective and subjective analysis of the stego-images. We noticed that the hidden information is imperceptible in bit planes 1-4 as illustrated in Figure 3.

Figure 3: Hidden information insertion into each bit plane, with ($\partial = 0.1$)

b. Experimental Result of MSE

Figure 4 shows the average MSE for all tested images for all bit planes with different values of the force insertion (∂). We noticed that MSE values for bit planes 1-5 are relatively lower than the bit planes 6-8. This indicates that we can safely insert the hidden information in bit planes 1-5 for these values of ∂.

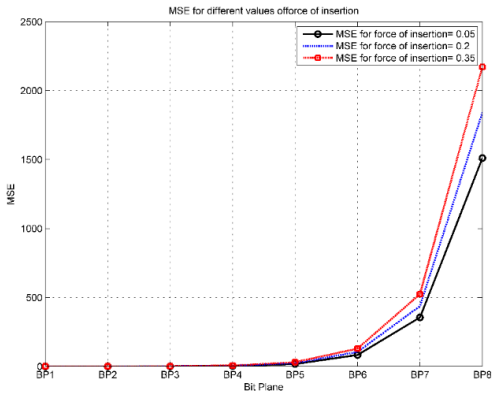

Figure 4: Average MSE of all tested images (10000 images) for all bit planes with $\partial = (0.05, 0.2 \text{ and } 0.35)$.

c. Experimental result of PSNR

Figure 5 shows the average PSNR values for all tested images for all bit planes with different values of the force insertion (∂). As high PSNR values indicate low distortion, we can conclude that bit planes 1-5 are the most suitable to insert the hidden information.

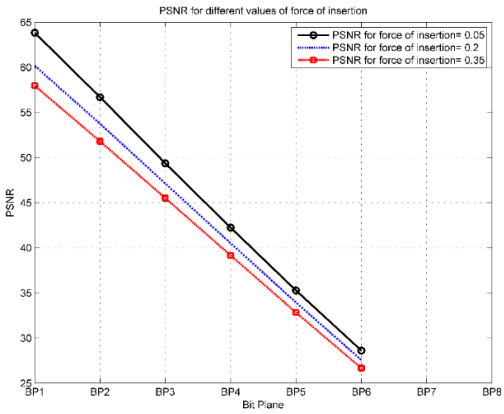

Figure 5: Average PSNR for all tested images (10000 images) for all bit planes with $\partial = (0.05,0.2,0.35)$

d. Experimental result of MSSIM

Although MSE and PSNR are very simple and conventionally accepted tools to measure signal fidelity yet in practice, we observe that tools like the Structural SIMilarity (SSIM) index give a clearer understanding of imperceptibility specially when modeling the human visual system in applications like compression and data hiding.

Figure 6 shows the Mean SSIM for all images and all bit planes with different values of the force insertion (∂). The MSSIM results confirm our initial analysis that bit planes 1-5 are the most suitable to insert the hidden information in terms of imperceptibility.

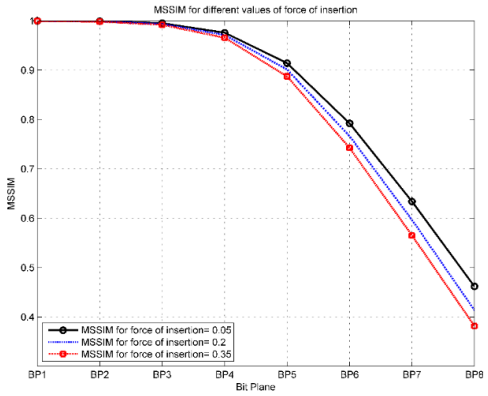

Figure 6: Mean SSIM for all images (10000 images) and all bit planes with $\partial = (0.05, 0.2 \text{ and } 0.35)$.

B. *Frequency Domain Steganography Results*

a. Imperceptibility analysis

In the frequency domain, we used second and third level of wavelet transform and did the insertions with different values of Alpha (Alpha1 correspond to level 3 and Alpha2 correspond to level 2 of the DWT). We noticed that the hidden information is imperceptible as illustrated in Figure 7.

Figure 7: Hidden information insertion, with different values of Alpha1 and Alpha2

Similarly, in order to measure and match the invisibility quality of the images, PSNR, MSE and SSIM are used.

b. Experimental result of MSE

Figure 8 shows the average MSE for all tested images with different values of Alpha1 and Alpha2. The results show lower values of MSE with lower values of Alpha1 and Alpha2, so we can safely do insertion with low values of Alpha.

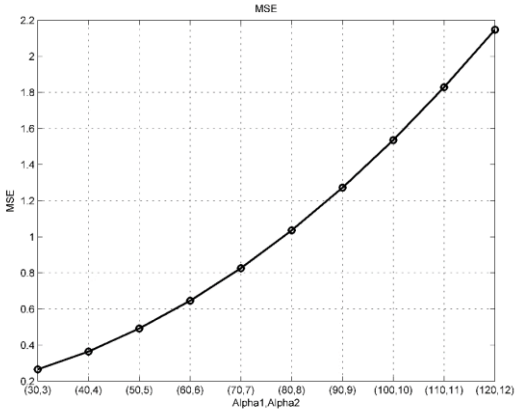

Figure 8 Average MSE of all tested images with different values of Alpha1 and Alpha2

c. Experimental result of PSNR

Figure 9 shows the average PSNR values for all tested images with different values of Alph1 and Alpha2. As high PSNR values indicate low distortion. Figure 9 shows good values of PSNR and we can conclude the lower values of Alpha is better for insertion.

d. Experimental result of MSSIM

Figure 10 shows the Mean SSIM for all images with different values of Alpha1 and Alpha2. The MSSIM results confirm our initial analysis that the lower values of Alpha1 and Alpha2 are more suitable to insert the hidden information in terms of imperceptibility.

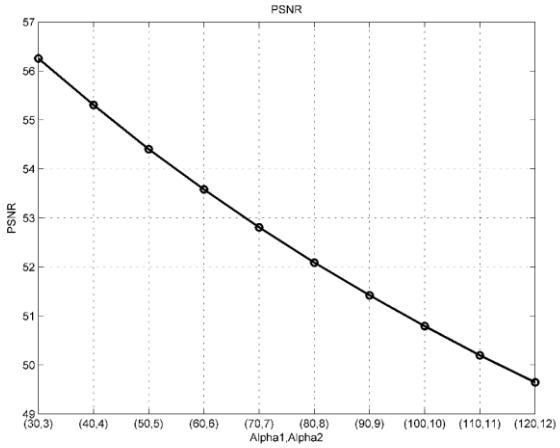

Figure 9: Average PSNR for all tested images with different values of Alpha1 and Alpha2.

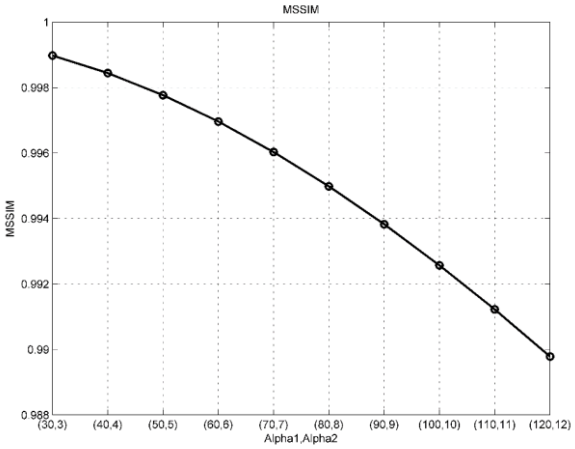

Figure 10: Mean SSIM for all images with different values of Alpha1, Alpha2.

C. Capacity

For the first algorithm, which is in spatial domain the capacity C_s for an X×Y image is given by Equation (10):

$$C_s \approx \frac{1}{2\times N^2} \text{ bits per pixel} \tag{10}$$

where N×N is the block size.

For second algorithm which is in frequency domain the capacity C_f for an X×Y image is given by Equation (11):

$$C_f \approx \frac{d}{2^l \times 2\times N^2} \text{ bit per pixel} \tag{11}$$

where X×Y is image size and N×N is the block size, l is wavelet level and d is number of dimension. In our case N and d are equal to 3.

In case $\frac{d}{2^l}$>1then $C_f > C_s$, i.e., the capacity in frequency domain is better than the capacity in spatial domain.

D. Comparison

Table 1 shows the comparison between the proposed algorithm and similar algorithms found in the literature. The PSNR values for our algorithm show higher imperceptibility when compared with these algorithms, especially for the optimal case.

Table 1
PSNR comparison

Algorithm	Covered image	PSNR dB
[13]	Lenna	34.17
[13]	Baboon	33.98
[11]		37.8
[17]	BOSS database	Best result- 57
Proposed algorithm in spatial domain	BOSS database	Best result- 65
Proposed algorithm in frequency domain	BOSS database	Best result- 56

V. CONCLUSION

The results and analysis show that the wavelet domain steganography has good invisibility but the capacity is low. On the other hand, the spatial domain gives better results for capacity for the proposed algorithms. The analysis using

MSE, PSNR and SSIM show that imperceptibility is lower in the case of the spatial domain. The results show optimum location and insertion force are important to insert secret information in a stego-image. The lower values of force of insertion are more suitable to insert the hidden information in terms of imperceptibility. The current work is a step forward in direction of finding the best bit planes and wavelet level to insert hidden information in chaotic manner.

REFERENCES

[1] V. Nagaraj, V. Vijayalakshmi, and G. Zayaraz, "Overview of Digital Steganography Methods and Its Applications," Int. J. Adv. Sci. Technol., vol. 60, pp. 45–58, 2013.

[2] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography. Morgan Kaufmann, 2007.

[3] H.-W. Tseng and C.-C. Chang, "High capacity data hiding in JPEG-compressed images," Informatica, vol. 15, no. 1, pp. 127–142, 2004.

[4] E. Ghasemi, J. Shanbehzadeh, and N. Fassihi, "High capacity image steganography using wavelet transform and genetic algorithm," in Proceedings of international multiconference of engineers and computer scientists, 2011, vol. 1, pp. 16–18.

[5] S. Ahani and S. Ghaemmaghami, "Colour image steganography method based on sparse representation," IET Image Process., vol. 9, no. 6, pp. 496–505, 2015.

[6] S. Sarreshtedari and S. Ghaemmaghami, "High Capacity Image Steganography in Wavelet Domain," in 2010 7th IEEE Consumer Communications and Networking Conference (CCNC), 2010, pp. 1–5.

[7] D. E. Walia, P. Jain, and N. Navdeep, "An Analysis of LSB & DCT based Steganography," Glob. J. Comput. Sci. Technol., vol. 10, no. 1, May 2010.

[8] D. Bandyopadhyay, K. Dasgupta, J. K. Mandal, and P. Dutta, "A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain," Int. J. Secur., 2014.

[9] A. Singh and H. Singh, "An improved LSB based image steganography technique for RGB images," in 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2015, pp. 1–4.

[10] B. Debnath, J. C. Das, and D. De, "Reversible logic-based image steganography using quantum dot cellular automata for secure nanocommunication," IET Circuits Devices Syst., vol. 11, no. 1, pp. 58–67, 2017. [11] J. Bai, C.-C. Chang, T.-S. Nguyen, C. Zhu, and Y. Liu, "A high payload steganographic algorithm based on edge detection," Displays, vol. 46, pp. 42–51, Jan. 2017.

[12] Shreyank N Gowda, "Block Based Least Significant Bit Algorithm for Image Steganography," presented at the Annual Int'l Conference on Intelligent Computing, Computer Science & Information Systems, Thailand, 2016.

[13] A. Nag, S. Ghosh, S. Biswas, D. Sarkar, and P. P. Sarkar, "An image steganography technique using X-box mapping," in 2012 International Conference on Advances in Engineering, Science and Management (ICAESM), 2012, pp. 709–713.

[14] S. Sharma, V. K. Yadav, and S. Batham, "Zero Distortion Technique: An Approach to Image Steganography Using Strength of Indexed Based Chaotic Sequence," in Security in Computing and Communications, Springer Berlin Heidelberg, 2014, pp. 407–416.

[15] Shivani, V. K. Yadav, and S. Batham, "A Novel Approach of Bulk Data Hiding using Text Steganography," Procedia Comput. Sci., vol. 57, pp. 1401–1410, Jan. 2015.

[16] B. S. and K. L. Sudha, "Text Steganography using LSB insertion method along with Chaos Theory," ArXiv12051859 Cs, May 2012.

[17] Y. Wang, W. Chen, Y. Li, W. Wang, and C. T. Li, "HPS: Histogram preserving steganography in spatial domain," in 2014 International Workshop on Biometrics and Forensics (IWBF), 2014, pp. 1–4.

[18] S. E. Jero and P. Ramu, "Curvelets-based ECG steganography for data security," Electron. Lett., vol. 52, no. 4, pp. 283–285, 2016.

[19] Yusra A. Y. Al-Najjar, Dr. Der Chen Soong "Comparison of Image Quality Assessment: PSNR, HVS, SSIM, UIQI" in International Journal of Scientific & Engineering Research, Volume 3, Issue 8, August-2017