Improvement of Image Steganography Using Discrete Wavelet Transform

Manal K. Oudah [a]*, **Aqeela N. Abed** [b], **Rula S. Khudhair** [c], **Saad M. Kaleefah** [d]

[a] Electromechanical Engineering Department, University of Technology, Baghdad, Iraq.
50030@uotechnology.edu.iq

[b] College of Medicine-Faculty, University of Iraq, Baghdad, Iraq

[c] College of Materials Engineering, University of Babylon Babylon, Iraq

[d] Al-Turath College University/Baghdad, Iraq

*Corresponding author.

A B S T R A C T

Recently the Discrete-Wavelet-Transform (DWT) has been represented as signal processing powerful tool to separate the signal into its band frequency components. In this paper, improvement of the steganography techniques by hiding the required message into the suitable frequency band is presented. The results show that the increase of the message length will reduce the Peak Signal to Noise Ratio (PSNR), while the PSNR increases with the increasing the DWT levels. It should be noted that the PSNR reduction was from -13.8278 to -17.77208 when increasing the message length from 161 to 505 characters. In this context, the PSNR is increased from -13.8278 to 7.0554 and from -17.7208 to 1.7901 when the DWT increased from level (1) to level (2).

1. Introduction

With the development of technologies, life is becoming full of information, so the protection of the information protects life and privacy [1]. Two techniques are used for the protection; the first one is the cryptography, which is the art of using mathematics to encrypt and decrypt the data [2,3]. The second one is the steganography, which is the art of hiding information over different carrier/cover media. The main terms of steganography art are cover media, secret message, and embedding algorithm, where the cover media may be an image, audio, or video file; sometimes called as "host" where the secret message is hidden within it; the resulting product is astego-image [4,5]. The drawback of using cryptography is that anyone knows there are data was encrypted. While for using

the steganography the drawback is the limitation of hidden information is limited by the size of the cover media used [6].

Steganography can be done in two type's domains [7,8,9] these are; spatial and frequency domain, where, in the spatial domain technique the secret message is embedded directly in pixels of the image. The intensity values of the pixels are alerted to get desirable enhancement [10]. The most common and simplest steganography method is the Least Significant Bit. It is a spatial domain substitution process where the secret message is hidden in the least significant bit pixels of the cover image; two types of LSB insertion according to some bits in an image. For an 8bit image, the required message is embedded in the 8th bit of each byte. For 24 bit image like RGB color image (Red, Green, and Blue) the required message is embedded in three bits in every pixel where each pixel is represented by (256,256,256) different colors [11]. Embedding the required massage by using the LSB technique can be easily destroyed by filtering, compression or a less than size transmutation or perfect format. So, this technique is not safe for sending a required message [12,13,14].

Frequency domain or transformation technique based on the covert the cover image from the spatial domain into frequency coefficients by manipulation of the orthogonal transform of the image through using different transformation techniques like (Digital Cosine Transformation DCT, Digital Wavelet Transformation DWT). The required message is hidden into the specific frequency coefficients of the image. After the modification, the coefficients are transformed back to the spatial domain to generate stage-image. Using DCT allows to separate the image into three spectral sub-bands (low, middle and high) without impacting to its visual quality, the required message is embedded in the middle-frequency band to avoid visual distortion, the high and low-frequency bands not used for avoiding DCT coefficient value of 0. Frequency domain techniques provide flexibility, hiding a large amount of data with the highest security, safe to send a required message; these are its added advantages. Using DWT technique steganography over DCT technique has more advantages [15].

2. Discrete Wavelet Transform (DWT)

Wavelet domain technique is a mathematical tool for hierarchically decomposing an image. It is based on small waves named wavelets of limited duration and varying frequency. When DWT is performed on the 2-D image, then 2-D filters in both dimensions process the image. It performed in the vertical and horizontal direction, the vertical filtering divided the image into two vertical halves, with the first half storing the average coefficients, and the second vertical half stores the detail coefficients. After that, horizontal filtering result four sub-bands within the array defined by filter output. In other word, it operates on the image pixels by calculating the differences and the sums of adjacent elements of pixels; the image/ color plane is decomposed into four non-overlapping sub-bands. Further, DWT applies on LL1sub-band to reach N level. At this stage, the result of DWT is 3N+1 sub-bands. Consisting of (LLV), (LHV), (HLV) and (HHV), where, "v" is ranging from 1 to "N". Figure 1 shows the result of computing the DWT transform of the whole image [7,10,12].

Using DWT is very suitable to recognize the region in the cover media (image) where the secret message can be hidden effectively. The nice feature of DWT method is that the transform is equal to its inverse, it computes the data energy in relocated at the top left-hand corner of the resulting image; the size of the square which contains the important information will be reduced by a factor of 4 after each transform of DWT. Figure 2 shows the image Lena after 2 DWT transform [7]. The required message will be extracted from the corresponding embedding frequency band of cover media/color plan [10].
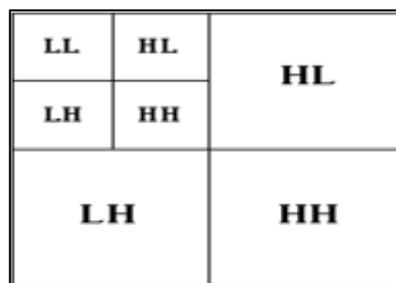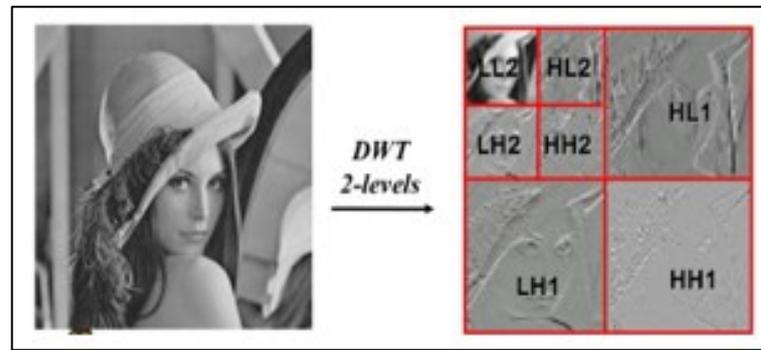

Figure 1: Sub band Images

Figure 2: The image Lena after 2 DWT transform

3. Proposed Technique

In this research, double Wavelet transforms have been presented. The secret text is transformed to its Corresponding wavelet coefficients so the cover image. The proposed technique steps are the following:
- Read the cover image.
- Transform the cover to its wavelet coefficients using 2D DWT.
- Read the secret text.
- Substitute each character in the secret text to its corresponding ASCII code.
- Transform the ASCII code values to the wavelet coefficients using 1D DWT.
- From step 2, take the HL and HH wavelet coefficients as cover coefficients, which are used, later in the hiding process.
- Classify the HH wavelet coefficients of the cover to: coefficients > 0, coefficients=0 and coefficients<0 then save the positions of the three coefficients types.
- Classify the wavelet coefficients of the text (obtained from step 5) to: coefficients > 0, coefficients =0, coefficients<0.
- Substitute the HH wavelet coefficients of the cover with the wavelet coefficients of the text in way ((cover wavelet coefficients>0) = (text wavelet coefficients>0), (cover wavelet coefficients=0) = (text wavelet coefficients=0), and (cover wavelet coefficients<0) = (text wavelet coefficients<0)). From this step, the stego-pixels are generated.
- Save the message length within HL (1,1).
- Find the rows of HL matrix that contains coefficients>0 to hide the positions of stego-pixels.
- Generate the stego-image by applying the inverse wavelet transform on the LL, LH, stego-HL, and stego-HH wavelet quarters.
The proposed steganography technique, which is based on DWT2, is shown in Figure 3.

4. Data Analysis

Figure 3 represents the flow chart with the results of the proposed technique steps. From this Figure, it is clear the LL and HH of DWT coefficients of the cover image and ASCII code of the message which wants to hide it. In this context, Table1 represents the peak signal to noise ratio (PSNR) with level 1,2 of DWT against the message length.

From Table 1, it is clear the reduction of the PSNR of the cover image when the message length is increased as in Figure 4 because the hidden message is represented as noise to the image. While this in a higher level of DWT, where, when returning the image to its original size the PSNR will be increased. In addition, there is another advantage of using DWT over other technique like FSK [5], where the DWT offer mother than two security levels.
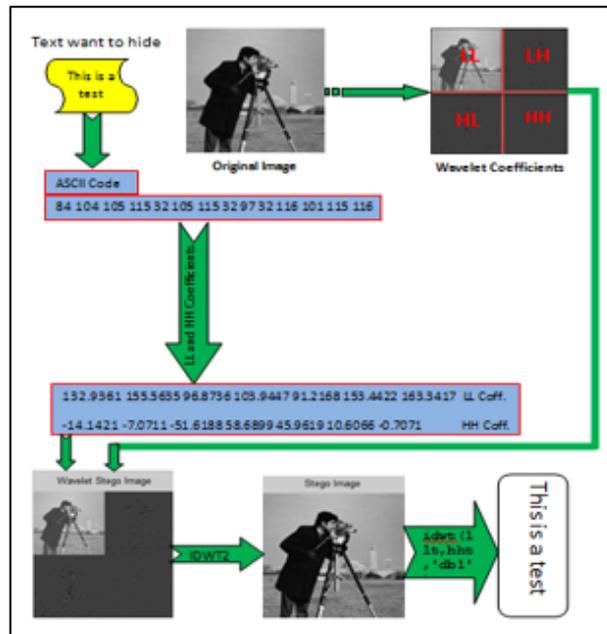
Figure 3: Proposed steganography technique

Table 1: PSNR and DWT levels against the message characters

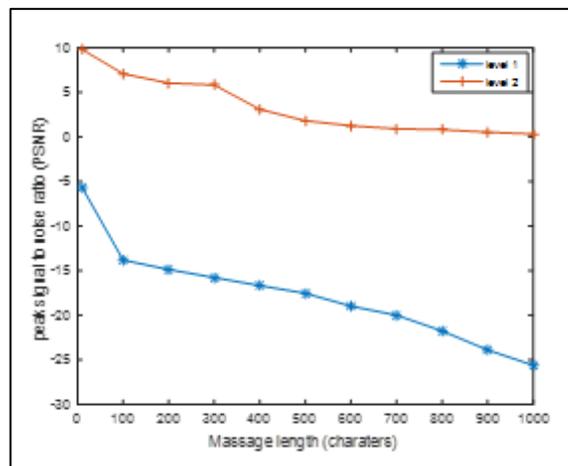| Message Length	PSNR of 1-level DWT	PSNR of 2-level DWT
161 Character	-13.8278	7.0554
505 Character	-17.7208	1.7901

Figure 4: Message length against PSNR

5. Conclusions

This paper has described the DWT2 algorithm as a tool for the hidden message in the cover image. For the sake of comparison, we also evaluated the performance of DWT-1,2 which are used. The results were obtained for the DWT-1,2 approach is indicated a better imperceptibility performance when the message was embedded in the LL2 sub-bands, where the value of PSNR are 7.0554 and 1.7901 for 161 and 505 characters respectively. The average difference between the level 1 and level two of DWT is approximately 20 db. Therefore, the DWT method is the best technique for 2 level 2 hiding message has been concluded, while the percent of the hidden message to the original signal is reduced.

References

[1]   Th. R. Saeed, "A novel steganography with preserving statistical properties," IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 5, No 2, September 2013.

[2]   N. S. Chavan, "Image steganography – an overview," International Journal of Recent Scientific Research Vol. 6, No., 6, pp. 4800-4804, June 2015.

[3]   N. K. Jumaa, "Hiding of random permutated encrypted text using lsb steganography with random pixels generator," International Journal of Computer Applications Vol. 113, No. 13, pp. 0975 – 8887, March 2015.

[4]   M. K. Rao, K. P. Reddy and K. E. Saranya, "Security enhancement in image steganography a MATLAB approach," Middle-East Journal of Scientific Research Vol.23, No. 2, pp. 357-361, 2015 .

[5]   A. Habboush, "FSK modulation based image steganography," Journal of Convergence Information Technology (JCIT) Volume11, Number1, January 2016.

[6]   E.P. Musa and S. Philip, "Secret Communication Using Image Steganography," African Journal of Computing & ICT, Vol. 8, No. 3, September 2015.

[7]   S. Sharma, and U. Kumar, "Review of transform domain techniques for image steganography," International Journal of Science and Research (IJSR), Vol.4, No 5, May 2015.

[8]   M. Mahajan and N. Kaur, "Adaptive Steganography: a survey of recent statistical aware steganography techniques," I. J. Computer Network and Information Security, Vol.10, pp. 76-92, September 2012.

[9]   H.H. Chang, Y. Ch. Chou, Ch. Tseng and Timothy K. Shih, "A High Payload Steganography Scheme for Color Images Based on BTC and Hybrid Strategy," Journal of Computers Vol. 26, No. 2, July 2015.

[10]   D. Baby, J. Thomas, G. Augustine, E. George and Ne. R. Michael , "A novel DWT based image securing method using steganography," International Conference on Information and Communication Technologies (ICICT 2014), Procedia Computer Science 46, pp.612-618, 2015.

[11]   Th. R. Saeed and Sh. A. Elghany, " Efficient adaptive steganography algorithm," International Journal of Pure and Applied Research in Engineering and Technology, Vol. 2, No.1, 2013

[12]   Y. J. Chanu, Kh. M. Singh and Th. Tuithung, "Image Steganography and steg analysis: a survey," International Journal of Computer Applications, Vol., 52, No.2, August 2012.

[13]   Gh. A. Sadi, "Image steganography approach," International Journal of Computer Science and Mobile Computing, Vol.4, No.8, pp.166-169, August 2015.

[14]   H. Patel and P. Dave, "Steganography technique based on DCT coefficients," International Journal of Engineering Research and Applications," Vol. 2, No. 1, pp.713-717. January 2012.

[15]   E. Ghasemi, J. Shanbehzadeh and N. Fassihi, "High capacity image steganography using wavelet transform and genetic algorithm," Proceedings of the International Multi-Conference of Engineers and Computer Scientists, Vol., I, Hong Kong, March 2011.