An Adaptive Steganographic Technique Based on Integer Wavelet Transform

R. O. El Safy
Faculty of Engineering
Benha University

H. H. Zayed
Faculty of Computers
Benha University

A. El Dessouki
Chairman of the National Authority for
Remote Sensing and Space Sciences

Abstract-**Steganography gained importance in the past few years due to the increasing need for providing secrecy in an open environment like the internet. With almost anyone can observe the communicated data all around, steganography attempts to hide the very existence of the message and make communication undetectable.**

Many techniques are used to secure information such as cryptography that aims to scramble the information sent and make it unreadable while steganography is used to conceal the information so that no one can sense its existence. In most algorithms used to secure information both steganography and cryptography are used together to secure a part of information.

Steganography has many technical challenges such as high hiding capacity and imperceptibility. In this paper, we try to optimize these two main requirements by proposing a novel technique for hiding data in digital images by combining the use of adaptive hiding capacity function that hides secret data in the integer wavelet coefficients of the cover image with the optimum pixel adjustment (OPA) algorithm. The coefficients used are selected according to a pseudorandom function generator to increase the security of the hidden data. The OPA algorithm is applied after embedding secret message to minimize the embedding error. The proposed system showed high hiding rates with reasonable imperceptibility compared to other steganographic systems.

Keywords-**Steganography, adaptive algorithm, spatial domain, integer wavelet transform, discrete wavelet transform, optimum pixel adjustment algorithm.**

I. INTRODUCTION

Steganography is the art and science of hiding secret data in plain sight without being noticed within an innocent cover data so that it can be securely transmitted over a network. The word steganography is originally composed of two Greek words *steganos* and *graphia*, which means "covered writing". The use of steganography dates back to ancient times where it was used by romans and ancient Egyptians. The interest in modern digital Steganography started by Simmons in 1983 [1] when he presented the problem of two prisoners wishing to escape and being watched by the warden that blocks any suspicious data communicated between them and passes only normal looking one. Any digital file such as image, video, audio, text or IP packets can be used to hide secret message. Generally the file used to hide data is referred to as cover-object, and the term stego-object is used for the file containing secret message.

Among all digital file formats available nowadays image files are the most popular cover objects because they are easy to find and have higher degree of distortion tolerance over other types of files with high hiding capacity due to the redundancy of digital information representation of an image data.

There are a number of steganographic schemes that hide secret message in an image file; these schemes can be classified according to the format of the cover image or the method of hiding. We have two popular types of hiding methods; spatial domain embedding and transform domain embedding.

The Least Significant Bit (LSB) substitution is an example of spatial domain techniques. The basic idea in LSB is the direct replacement of LSBs of noisy or unused bits of the cover image with the secret message bits. Till now LSB is the most preferred technique used for data hiding because it is simple to implement offers high hiding capacity, and provides a very easy way to control stego-image quality [2] but it has low robustness to modifications made to the stego-image such as low pass filtering and compression [3] and also low imperceptibility. Algorithms using LSB in grayscale images can be found in [4, 5, 6].

The other type of hiding method is the transform domain techniques which appeared to overcome the robustness and imperceptibility problems found in the LSB substitution techniques. There are many transforms that can be used in data hiding, the most widely used transforms are; the discrete cosine transform (DCT) which is used in the common image compression format JPEG and MPEG, the discrete wavelet transform (DWT) and the discrete Fourier transform (DFT). Examples to data hiding using DCT can be found in [7, 8]. Most recent researches are directed to the use of DWT since it is used in the new image compression format JPEG2000 and MPEG4, examples of using DWT can be found in [9, 10]. In [9] the secret message is embedded into the high frequency coefficients of the wavelet transform while leaving the low frequency coefficients subband unaltered. While in [10] an adaptive (varying) hiding capacity function is employed to

978-1-4244-3778-8/09/$25.00 ©2009 IEEE

determine how many bits of the secret message is to be embedded in each of the wavelet coefficients. The advantages of transform domain techniques over spatial domain techniques are their high ability to tolerate noises and some signal processing operations but on the other hand they are computationally complex and hence slower [9]. In all proposed techniques for steganography whether spatial or transform the key problem is how to increase the size of the secret message without causing noticeable distortions in the cover object. Some of these techniques try to achieve the high hiding capacity low distortion result by using adaptive techniques that calculate the hiding capacity of the cover according to its local characteristics as in [5, 7, 9, 10].

However, the steganographic transform-based techniques have the following disadvantages; low hiding capacity and complex computations [11, 12]. Thus, to get over these disadvantages, the present paper proposes an adaptive data hiding technique joined with the use of optimum pixel adjustment algorithm to hide data into the integer wavelet coefficients of the cover image in order to maximize the hiding capacity as much as possible. We also used a pseudorandom generator function to select the embedding locations of the integer wavelet coefficients to increase the system security.

The remaining of the paper will be organized as follows. Firstly, we will provide a brief introduction to integer wavelet transform. Secondly we will describe the proposed steganographic system. Then, we will discuss the achieved results; and finally we will conclude the paper and suggest future improvements to the system.

II. INTEGER WAVELET TRANSFORM

Generally wavelet domain allows us to hide data in regions that the human visual system (HVS) is less sensitive to, such as the high resolution detail bands (HL, LH and HH), Hiding data in these regions allow us to increase the robustness while maintaining good visual quality. Integer wavelet transform maps an integer data set into another integer data set. In discrete wavelet transform, the used wavelet filters have floating point coefficients so that when we hide data in their 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 lead to the failure of the data hiding system [11]. To avoid problems of floating point precision of the wavelet filters when the input data is integer as in digital images, the output data will no longer be integer which doesn't allow perfect reconstruction of the input image [12] and in this case there will be no loss of information through forward and inverse transform [11]. Due to the mentioned difference between integer wavelet transform (IWT) and discrete wavelet transform (DWT) the LL subband in the case of IWT appears to be a close copy with smaller scale of the original image while in the case of DWT the resulting LL subband is distorted as shown in "Fig. 1".

Lifting schemes is one of many techniques that can be used to perform integer wavelet transform [13] it is also the scheme used in this paper. The following is an example showing how we can use lifting schemes to obtain integer wavelet transform by using simple truncation and without losing invertibility [13].

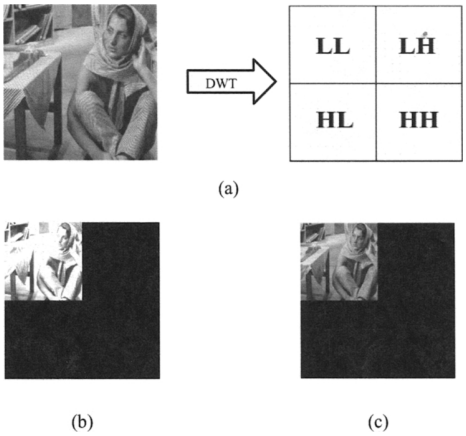


Figure 1. (a) Original image Lena and how it is decomposed using wavelet filters (b) One level of 2DDWT decomposition and (c) One level of 2DIWT decomposition

The Haar wavelet transform can be written as simple pairwise averages and differences [13]:

$$s_{1,n} = (s_{0,2n} + s_{0,2n+1}) / 2$$
$$d_{1,n} = s_{0,2n+1} - s_{0,2n} \quad (1)$$

Where $s_{i,l}$, $d_{i,l}$ are the n^{th} low frequency and high frequency wavelet coefficients at the i^{th} level respectively [11].

It is obvious that the output of (1) is not integer, the Haar wavelet transform in (1) can be rewritten using lifting in two steps to be executed sequentially:

$$d_{1,n} = s_{0,2n+1} - s_{0,2n}$$
$$s_{1,n} = s_{0,2n} + d_{1,n} / 2 \quad (2)$$

From (1) and (2) we can calculate the integer wavelet transform according to:

$$d_{1,n} = s_{0,2n+1} - s_{0,2n}$$
$$s_{1,n} = s_{0,2n} + \lfloor d_{1,n} / 2 \rfloor \quad (3)$$

Then the inverse transform can be calculated by:

$$s_{0,2n} = s_{1,n} - \lfloor d_{1,n} / 2 \rfloor$$
$$s_{0,2n+1} = d_{1,n} + s_{0,2n} \quad (4)$$

II. PROPOSED SYSTEM

The proposed system is an adaptive data hiding scheme, in which randomly selected integer wavelet coefficients of the cover image are modified with secret message bits. Each of these selected coefficients hide different number of message bits according to the hiding capacity function, the capacity function used is a modified version of the one in [6]. After data insertion we apply optimum pixel adjustment algorithm in [4] to reduce the error induced due to data insertion. The block diagram is shown in "Fig. 2". We can say that the proposed system is classified into three cases of operation according to different applications; Low hiding capacity with good visual quality (high value of peak signal to noise ratio "PSNR"), average hiding capacity with reasonable visual quality and high hiding capacity with low visual quality. We discuss each of these cases in next section.

A. The Embedding Algorithm

The block diagram of the embedding procedure is shown in "Fig. 2".

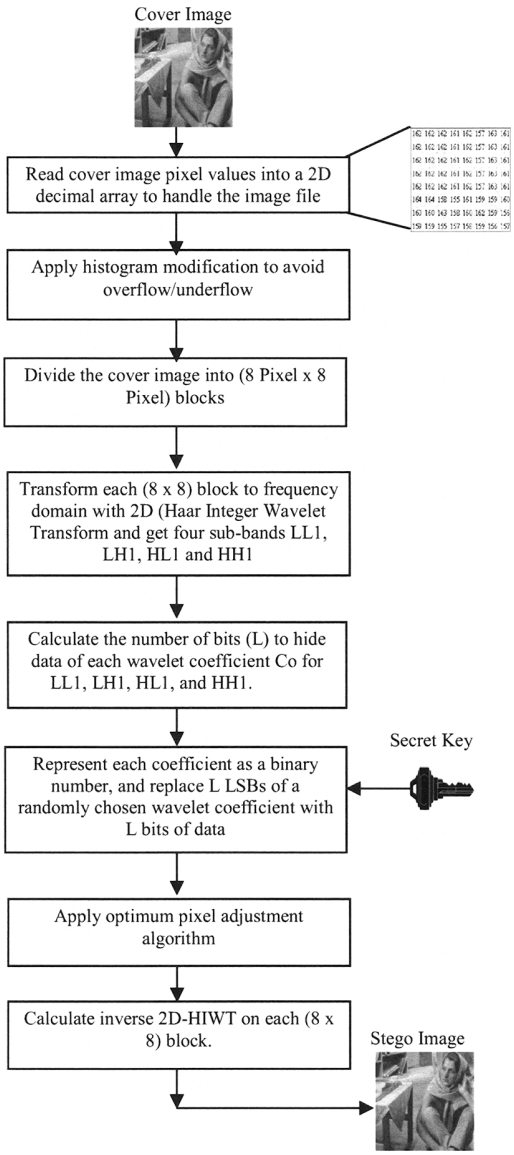


Figure 2. The block diagram of the proposed embedding algorithm

The blocks of the embedding algorithm is explained in the following steps:

Step 1: Read the cover image file into a two dimensional decimal array to handle the file data more easily.

Step 2: histogram modification it is used to prevent overflow/underflow that occurs when the changed values in integer wavelet coefficients produce stego-image pixel values to exceed 255 or to be smaller than 0. This problem was found to be caused by the values near 255 or 0 [10], [14]. The problem can be solved by mapping the lowest 15 grayscale levels to the value of 15 and the highest 15 grayscale levels to the value 240.

Step 3; divide the cover image into 8x8 non overlapping blocks. By this division each 8x8 block can be categorized as a smooth or complex block.

Step 4; (Integer wavelet Transform): transform each block to the transform domain using 2D Haar integer wavelet transform resulting LL1, LH1, HL1 and HH1.

Step 5; Calculate hiding capacity (number of bits to be used in hiding message bits) of each coefficient, we used a modified version of the hiding capacity function in [10]. The length of LSBs of wavelet coefficients (L) is determined according to [10]:

$$L = \begin{cases} k+3, if Co \geq 2^{k+3} \\ k+2, if\, 2^{k+2} \leq Co < 2^{k+3} \\ k+1, if\, 2^{k+1} \leq Co < 2^{k+2} \\ k, if Co < 2^{k+1} \end{cases}, 0 \leq k \leq 4 \qquad (5)$$

Where, Co is the absolute value of wavelet coefficients and k is the minimum length to be used in each coefficient.

From experiments we found that as we lower the bits used to hide the secret message in the LL subband the resulted distortion in the stego-image becomes lower; so that we modified this hiding capacity function by using different ranges for k for the LH, HL and HH subbands where its values are form 1 to 4. For the LL subband the value of k is equal to 0 and in some cases the bits used is fixed to only bits to enhance the stego-image quality.

Form experiments of different values of k we divided the system into 3 cases of operation depending on the requirements of the user; these cases are:

Case 1: k = 1 for LH1, HL1 and HH1 subbands, while using 2 bits for embedding data in LL1 subband

This case provides low hiding capacity with high visual quality of the stego-image.

Case 2: k = 3 for LH1, HL1 and HH1 subbands, while using 2 bits for embedding data in LL1 subband

This case is for applications requiring average hiding capacity with reasonable visual quality.

Case 3: k = 4 for LH1, HL1 and HH1 subbands, while k = 0 for LL1 subband)

Case 3 is considered as the worst case of data embedding where it is used when the high visual quality of the stego-image is not important and the user requires only high hiding capacity.

Note that we dropped the case of k=2 because it provided no significant improvements to the results obtained by k=1 or k=3.

To realize how we use the hiding capacity function; for example, If L=3, then the three least significant bits of the wavelet coefficient will be replaced with three bits of the message data.

Step 6: Embed L bits of message into the corresponding randomly chosen coefficients. Random selection of coefficients provides more security where the sequence of the message is only known to both sender and receiver by using a previously agreed upon secret key.

Step 7: Apply optimal pixel adjustment algorithm, while taking into consideration that each modified coefficient stays in its hiding capacity range where each value of L is calculated according to the absolute value of the wavelet coefficients any significant change in this value will produce different value of L to be calculated at the receiver.

The main idea of using the optimum pixel adjustment (OPA) algorithm is to minimize the error difference between the original coefficient value and the altered value by checking the right next bit to the modified LSBs so that the resulted change will be minimal.

For example, if a binary number 1000 (decimal number 8) is changed to 1111 (decimal number 15) because its three LSB's were replaced with embedded data; the difference from the original number is 7. This difference in the original value is called the embedding error. By adjusting the fourth bit from a value of 1 to a value of 0, the binary number now becomes 0111 (decimal number 7) and the embedding error is reduced to 1 while at the same time preserving the value of the three embedded bits.

The algorithm we used in [4] is the final step in the proposed scheme, where it can minimize the error by half. The main idea of OPA is to check the bit right next to the last changed LSBs It is used to decrease the error resulted after insertion of message bits. The algorithm according to [6] depend on calculating the difference (δ_i) between original value P(x, y) and the modified value P'(x, y)

$$\delta_i (x, y) = P_i'(x, y) - P_i(x, y) \quad (6)$$

After calculating the (δ_i), the algorithm modifies the changed value in the following manner:

Case 1 ($-2^k < \delta_i < -2^{k-1}$)

If $P_i'(x, y) < 256 - 2^k$

Then $P_i'(x, y)^* = P_i'(x, y) + 2^k$

Else $P_i'(x, y)^* = P_i'(x, y)$

Case 2 ($-2^{k-1} \le \delta_i \le 2^{k-1}$)

$P_i'(x, y)^* = P_i'(x, y)$

Case 3: $2^{k-1} < \delta_i < 2^k$

If $P_i'(x, y) \ge 2^k$

Then $P_i'(x, y)^* = P_i'(x, y) - 2^k$

Else $P_i'(x, y)^* = P_i'(x, y)$

Step 8: finally, calculate the inverse integer wavelet transform on each 8x8 block to restore the image to spatial domain.

B. The Extraction Algorithm

At the receiver uses the extraction algorithm to obtain the secret message. The block diagram of the extraction algorithm is shown in "Fig. 3".

As we can see from "Fig. 3" the extraction procedure is a blind process since it requires only the secret key from the receiver. It is also simpler than the embedding procedure.

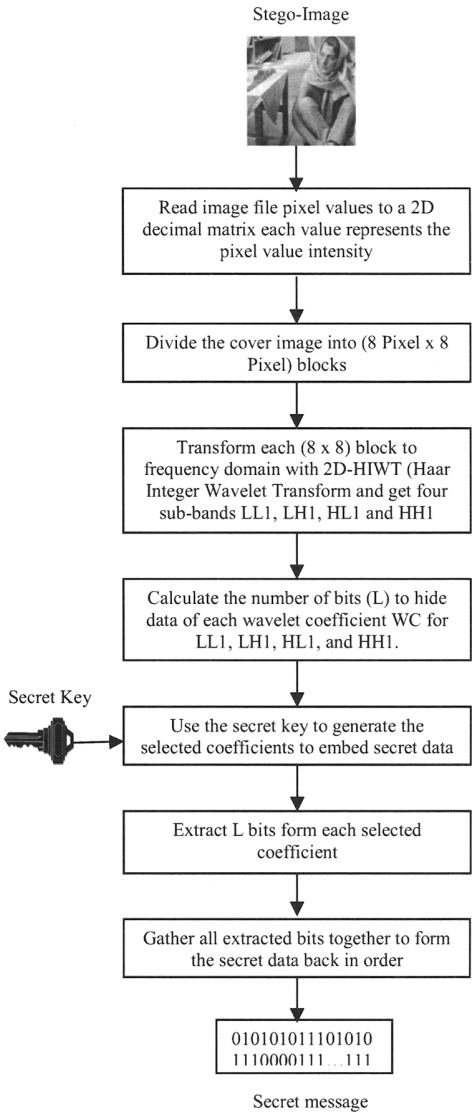


Figure 3. The block diagram of the extraction algorithm

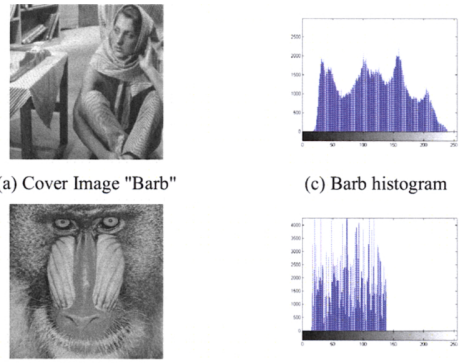
III. EXPERIMENTAL RESULTS

The proposed system was applied to two typical 512x512 8-bit grayscale images shown in figure 2, "baboon" and "barb"; it achieved satisfactory results against other systems using wavelet transform.

The program was implemented using Matlab 7.4 running on 1.73G dual core processor under Windows Vista.

The secret message to embed is a randomly generated binary stream with the same length as the calculated hiding capacity.

"Fig. 4" shows the original cover images along with their histogram analysis which will be used later to compare it with the ones of the resulting stego-images to test for imperceptibility.



(a) Cover Image "Barb" (c) Barb histogram

(b) Cover Image "Baboon" (d) Baboon histogram

Figure 4. Three cover images used in system simulation and their corresponding histogram

The performance of the proposed technique is evaluated according to two widely used aspects [2]:

1. *Imperceptibility/Stego-image quality*

This aspect measures how much difference (distortion) was caused by data hiding in the original cover, where the higher the stego-image quality, the more invisible the hidden message. We can judge the stego-image quality by using Peak Signal to Noise Ratio (PSNR). The PSNR for an image of size MxN is calculated by (7)

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \quad (7)$$

and

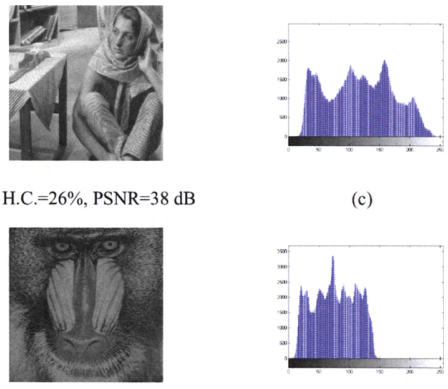
$$MSE = \left(\frac{1}{MxN}\right)\sum_{x=1}^{M}\sum_{y=1}^{N}(p(x,y)-p'(x,y))^2 \quad (8)$$

The *MSE* is the Mean Square Error, *P(x, y)* stands for the image pixel value in the cover image and *P'(x, y)* is for the pixel value at position (*x, y*) in the image after inserting secret message. A high value of PSNR means better image quality (less distortion), it is recorded that in grayscale images that the human visual system (HVS) can not detect any distortions in stego-images having PSNR that goes beyond 36 dB.

2. *Payload/ Hiding Capacity*

The hiding capacity indicates of how much data can be hidden within a cover image without making obvious degradation in the cover image quality. Due to the importance where it has no meaning that an algorithm hides large amount of data and produce large distortion in image quality. So we can say that a steganographic technique is an addition if it proves increase in payload while maintaining an acceptable visual quality of stego-image or improve the stego-image quality at the same hiding capacity level or if it can improve both [2].

"Fig. 5" shows the resulting stego-images along with their histogram when applying case1 (k=1 for the three subbands LH1, HL1 and HH1, while using two bits for embedding secret data in LL1 subband) of embedding a randomly generated binary stream. The hiding capacity (H.C.) is calculated for each image as a percentage of the cover image size. The values of H.C. ranges from (22% to 30%). Also the PSNR is calculated for each stego-image and it ranges form (37 dB to 40 dB); which are far above the threshold for the HVS of 36 dB.



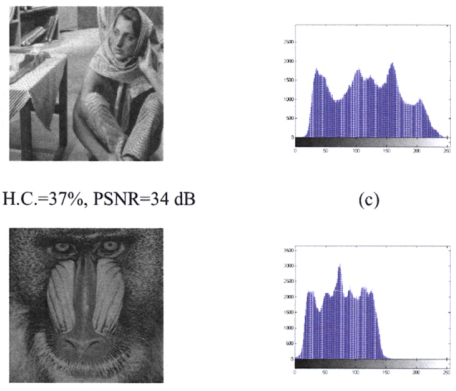
(a) H.C.=26%, PSNR=38 dB (c)

(b) H.C.=30%, PSNR=37 dB (d)

Figure 5. Output stego-images of Case 1 for embedding data and their corresponding histograms

Comparing the resulting stego images and their histograms with the ones in "Fig. 4" we can see that there is no significant change in Barb histogram. Unlike barb image we can see that the Baboon histogram is changed significantly due to the large number of edges in the original image although it does not affect the visual quality of the resulting stego-image.

"Fig. 6" and "Fig. 7" show the corresponding results for case 2 (k = 3 for LH1, HL1 and HH1 subbands, while using 2 bits for embedding data in LL1 subband) and case 3 (k = 4 for LH1, HL1 and HH1 subbands, while k=0 for LL1 subband) respectively.



(a) H.C.=37%, PSNR=34 dB (c)

(b) H.C.=38%, PSNR=33 dB (d)

Figure 6. Output stego-images of Case 2 for embedding data and their corresponding histograms

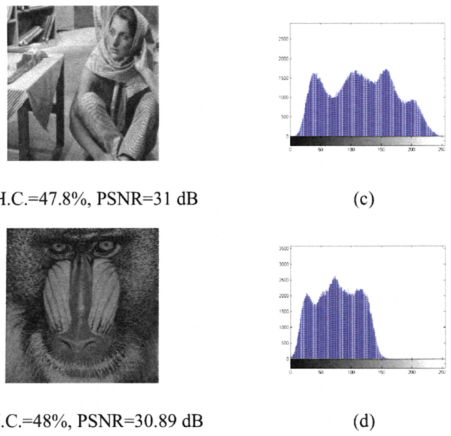


Figure 7. Output stego-images of Case 3 for embedding data and their corresponding histograms.

"Fig. 6" and "Fig. 7" show that the proposed system can give a high hiding capacity of 48% of the cover image size with a PSNR of about 31 dB which gives a reasonable visual quality of the stego-image.

The histogram analysis for both stego-images shows that when the size of secret data increases, the histogram tends to be smoother. This is clear when comparing the histograms in "Fig. 5", "Fig. 6" and "Fig. 7" with the corresponding ones of the original images in "Fig. 4".

According to the obtained results of our system the performance analysis for Lena as a cover image is shown in "Fig. 8". The comparison was made between the two different hiding values of the LL subband the first is when using two bits to embed secret data and the second when k=0.

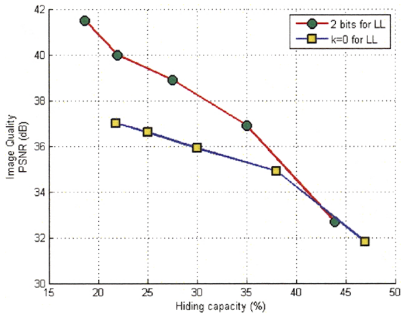


Figure 8. Performance analysis of Lena at the two different values of hiding at LL subband

It is clear form "Fig. 8" that the proposed technique performs better when using lower bits of the LL subband to embed secret data giving much higher PSNR values at the same embedding rate. This is because most data hiding algorithms which are using wavelet domain avoid using LL subband coefficients since it carries the approximations of the image while the other high frequency subbands (LH, HL, HH) contain the details/edges of the cover image.

Table I summarizes the results of this research for the images of Lena and Baboon. It also compares the maximum hiding capacity and the corresponding PSNR of the proposed hiding techniques with the techniques of [10], [14] and [15] (comparing results of Lena image only because it has no complete results for Baboon image). The comparison shows that the proposed technique gives a significant improvement of the hiding capacity on the expense of a slight decrease in the PSNR value.

TABLE I

COMPARISON OF MAXIMUM HIDING CAPACITY ACHIEVED AND THE PSNR OBTAINED BETWEEN OUR SYSTEM AND THE PROPOSED SYSTEMS IN [10] AND [14]

Cover image	Method	Max. H.C. (bits)	Max. H.C. (%)	PSNR (dB)
Lena	Proposed technique	986408	47%	31.8
	Adaptive technique using HDWT [10]	801842	38%	33.58
	Distorionless technique using IWT [14]	85507	4%	36.64
	Pixel Value Difference of IWT coefficients [15]	760958	36%	34.63
Baboon	Proposed technique	1008593	48%	30.89
	Adaptive technique using HDWT [10]	883220	42%	32.69
	Distorionless technique using IWT [14]	14916	0.7%	32.76

To further investigate the imperceptibility of the proposed system we compared the hiding capacity of our system with other systems at the same PSNR value and it showed better results. For example, the system in [15] showed a maximum hiding capacity of 36% of the cover image at a PSNR value of 34.63 dB while our system showed a hiding capacity of 38% of the cover image at the same PSNR.

IV. CONCLUSIONS

In this paper we proposed a novel data hiding scheme that hides data into the integer wavelet coefficients of an image. The system combines an adaptive data hiding technique and the optimum pixel adjustment algorithm to increase the hiding capacity of the system compared to other systems. The proposed system embeds secret data in a random order using a secret key only known to both sender and receiver. It is an adaptive system which embeds different number of bits in each wavelet coefficicient according to a hiding capacity function in order to maximize the hiding capacity without sacrificing the visual quality of resulting stego image. The proposed system also minimizes the difference between original coefficients values and modified values by using the optimum pixel adjustment algorithm. The proposed scheme was classified into three cases of hiding capacity according to different applications required by the user. Each case has different visual quality of the stego-image. Any data type can be used as the secret message since our experiments was made on a binary stream of data. There was no error in the recovered message (perfect recovery) at any hiding rate. From the experiments and the obtained results the proposed system proved to achieve high hiding capacity up to 48% of the cover image size with reasonable image quality and high security because of using random insertion of the secret message. On the other hand the system suffers from low robustness against various attacks such as histogram equalization and JPEG compression.

The proposed system can be further developed to increase its robustness by using some sort of error correction code which increases the probability of retrieving the message after attacks, also investigating methods to increase visual quality of the stego-image (PSNR) with the obtained hiding capacity.

REFERENCES

[1] G. J. Simmons, "The prisoners' problem and the subliminal channel," in Proceedings of Crypto' 83, pp. 51-67, 1984.

[2] N. Wu and M. Hwang. "Data Hiding: Current Status and Key Issues," International Journal of Network Security, Vol.4, No.1, pp. 1-9, Jan. 2007.

[3] W. Chen, "A Comparative Study of Information Hiding Schemes Using Amplitude, Frequency and Phase Embedding," PhD Thesis, National Cheng Kung University, Tainan, Taiwan, May 2003.

[4] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, pp. 469–474, Mar. 2004.

[5] K. Changa, C. Changa, P. S. Huangb, and T. Tua, "A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing," Journal of Multimedia, Vol. 3, No. 2, June 2008.

[6] H. H. Zayed, "A High-Hiding Capacity Technique for Hiding Data in Images Based on K-Bit LSB Substitution," The 30th International Conference on Artificial Intelligence Applications (ICAIA - 2005) Cairo, Feb. 2005.

[7] A. Westfeld, "F5a steganographic algorithm: High capacity despite better steganalysis," 4th International Workshop on Information Hiding, pp.289-302, April 25-27, 2001.

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

[9] P. Chen, and H. Lin, "A DWT Approach for Image Steganography," International Journal of Applied Science and Engineering 2006. 4, 3: 275:290.

[10] B. Lai and L. Chang, "Adaptive Data Hiding for Images Based on Harr Discrete Wavelet transform," Lecture Notes in Computer Science, Volume 4319/2006.

[11] S. Lee, C.D. Yoo and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," IEEE Transactions on Information Forensics and Security, Vol. 2, No. 3, Sep. 2007, pp. 321-330.

[12] M. K. Ramani, Dr. E. V. Prasad and Dr. S. Varadarajan, "Steganography Using BPCS to the Integer Wavelet Transformed Image", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.7, July 2007.

[13] A. R. Calderbank, I. Daubechies, W. Sweldens and B. Yeo., "Wavelet transforms that map integers to integers". Applied and Computational Harmonic Analysis, vol.5, no.3, pp.332-369, 1998.

[14] G. Xuan, J. Zhu, Y. Q. Shi, Z. Ni, and W. Su., "Distortionless data hiding based on integer wavelet transform," IEE Electronic Letters, 38(25):1646--1648, Dec. 2002.

[15] J. Liu, M. Shih, "Generalizations of Pixel-Value Differencing Steganography for Data Hiding in Images", Fundamenta Informaticae, vol. 83, no.3, pp. 319-335, 2008.