Received: October 1, 2021. Revised: December 3, 2021.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Image Steganography Technique Based on Integer Wavelet Transform Using Most Significant Bit Categories

Nisreen I. R. Yassin[1]* **Enas M. F. El Houby[1]**

[1]*Systems & Information Department, Engineering Division, National Research Centre, Dokki, Cairo 12311, Egypt*
* Corresponding author's Email: nisreen.yassin20@gmail.com

Abstract: In this paper, an image steganographic technique based on Integer Wavelet Transform (IWT) is proposed. The cover image is transformed using IWT to suppress the secret message into the high frequency bands HH, LH, and HL of the cover image. The coefficients of these bands are labelled into six categories according to their most significant bits (MSBs). All coefficients from different bands which belong to the same category are collected. The embedding process starts from the highest category and continues to the next category by controlling the number of coefficients to match the size of the secret message. The test results show that an average PSNR of 54 dB is achieved with a message size of 67.7 kb which considered reasonable result compared to other steganographic techniques. Up to 70% embedding rate can be provided with average PSNR of 47 dB with full reversibility and perfect reconstruction of data.

Keywords: Data hiding, Integer wavelet transform, Steganography.

1. Introduction

Currently, huge amount of data is transmitted and received through the Internet every second all over the world because of the massive development of the information and communication technology. Protecting these data from unauthorized access has become a crucial problem which leads to evolve the technology of information security. The unauthorized access done by an attacker can influence, interrupt, or disturb the data. To overcome this problem, researchers of information security proposed many solutions such as cryptography and data hiding [1].

Data hiding proposes an alternative for communicating securely and without letting the adversary discover that communication is happening. The idea of the process is hiding information in a cover medium as communicating a normal photograph. Data hiding comprise two fields, digital watermarking and steganography. The purpose of steganography is to hide a secret message within a cover medium where it is difficult to detect that a secret message exists. An image steganography system is composed of two processes which are the embedding process and extraction process. The cover image and secret message are the inputs of the embedding process, which create a stego image as an output. The secret message is extracted from the stego image in the extraction process.

The steganography application domain can be classified into spatial and transform domains. Hiding data in the spatial domain is performed by directly modifying the values of the pixels of the image. This method achieves a high embedding capacity, however its robustness against attacks is relatively low. The transformation domains like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Integer Wavelet Transform (IWT), and Discrete Fourier Transform (DFT) are less prone to malicious attacks, so transform domain is recommended especially if the capacity of the payload is small. As the methods based on the transform domain have a low embedding capacity compared to the spatial domain, the image quality remains relatively high. Selecting the embedding domain and the regions of the image that are less subject to image processing operations are important

for hiding information and generating high-quality stego image.

The most prevalent embedding method is LSB based embedding where the LSB of each pixel in the cover image is used to hide the bits of the secret message [2]. This embedding method benefits from the fact that LSBs are considered as random noise so they are not sensitive to any changes happens on the image. In this method, the embedding of the secret bits occur depending on the bits which have minimum weight so the value of original pixel will not be affected. Alteration of LSB does not produce image distortion and the stego-image appears congruent to the cover-image if the number of secret bits equals the number of pixels in cover image. But, if the number of secret bits transcends three bits for each pixel, high distortion in cover image will be occurred [3, 4]. To minimize the distortion occurred by LSB and increase the capacity of pixels, hybrid techniques based on LSB and IWT are improved. Also, Embedding the secret message in the edge regions of the image makes the human vision system (HVS) unable to detect its existence [5]. This paper presents a hybrid image steganography technique based on LSB and IWT. The three detail bands HH, HL, LH contain the edge area of the image so they are used for embedding secret data without causing high distortion to the image. The MSB categories are selected from these detail bands to embed the secret message. Concealing data in MSB categories grantees high payload capacity and reduces the possibility of detection. The rest of the paper is organized as follows. A literature review is described in Section 2. The methodology of the proposed technique is discussed in Section 3. Results and comparative analysis are presented in Section 4. The conclusion is concluded in Section 5.

2. Literature review

Recently, many steganographic methods were evolved by researchers trying to maximize the embedding capacity with preserving the visual quality of the stego images. In this section, several state of the art methods in spatial domain and frequency domain are discussed.

Verma et al. [6] converted the secret data into a set of two-digit decimal values. A digit in the set is hidden in RGB cover pixel by modifying the pixel's digits to the nearest possible pixel value. This scheme provides higher payload and good imperceptibility. Swain in [7] proposed two steganography techniques, the first based on quotient value differencing, and the second based on pixel value differencing with modulus function. Large amount of information is concealed using this method. Chakraborty et al. [8] proposed an adaptive technique for predictive edge image steganography. Modified median edge detector was used to predict the selected area from the grayscale cover image to embed the binary data. The proposed technique affords low embedding rate where the maximum payload is 61656 bits. Islamy and Ahmad [9] proposed an image steganography method based on prediction error histogram. Although, the histogram is segmented into sections to increase the embedding capacity, still limited number of bits is offered. Maniriho and Ahmad [10] presented a data hiding method using difference expansion and modulus function. The method selected smooth areas of the cover image to embed the secret data. The proposed method increased the embedding capacity and keep a high quality of the stego image. Sajasi et al. [11] proposed a hybrid steganography technique using chaotic encryption to embed secret data in LSB of cover images. High quality stego images are provided with a payload capacity of 131072 bits. Chandrasekaran and Sevugan [12] presented a steganography algorithm for medical images. The secret data are concealed in middle and high frequencies of Haar transform. High embedding capacity of 0.8 bpp was achieved. Valandar et al. [13] proposed an image steganography method based on IWT using 3d sine chaotic map. The chaotic map is used to select where the secret message is embedded. The algorithm embeds one bit of secret message in one coefficient of LL subband of cover image which resulted in limiting embedding capacity. Miri and Faez in [5] introduced a method for image steganography based on IWT. They classified the frequency coefficients based on their magnitude. Then, they embedded the secret massage into HH subband and if it is not sufficient, another detail band is selected to embed more data. This method embeds the secret data in all edge pixels starting from diagonal pixels. A PSNR of 53.68 with message size of 67.7kb using 512x512 cover image was achieved. Emad et al. [14] proposed a steganography method that hides secret text in the approximation band of IWT of cover image by using LSB substitution. Low full payload capacity equals to 8192 digits is granted. Due to embedding in approximation coefficients, depressed value of PSNR is achieved. Safy et al. [15] improved the data hiding capacity by proposing a steganographic approach based on IWT and optimal pixel adjustment. Embedding capacity of 47% is achieved but with very low PSNR value of 31.8 dB. Al-Dmour and Al-Ani [16] proposed an edge detection method using non-overlapping blocks, where the corner coefficients of each block are used to identify the edge strength of

the block. In this method, there are edge indicator coefficients separated from secret transporter coefficients which affords error free data extraction but low embedding capacity. The afforded embedding rate was 50% with 48.45 dB using IWT.

3. Proposed method

In image steganographic methods, it is required to effectively hide the secret message, so areas which are less sensitive to the human visual system must be identified. Wavelet transform is able to identify these areas in the cover image through frequency bands decomposition which include information of sharp transitions, edges and textures.

Haar DWT is the simplest and the most generic method for transforming image from spatial domain to frequency domain. HDWT computes the average and difference of each two consecutive pixels of the image in the horizontal direction then in the vertical direction as described in Eqs. (1) and (2). While the inputs to HDWT is a sequence of integers of pixels, the produced outputs are floating point coefficients (due to the division by two in Eq. (1)), which require high computations and cause losing of data in the invers operation as described in Eqs. (3) and (4).

$$S_{1,n} = \left(S_{0,2n} + S_{0,2n+1}\right)/2 \quad (1)$$

$$D_{1,n} = S_{0,2n+1} - S_{0,2n} \quad (2)$$

$$S_{0,2n} = S_{1,n} + D_{1,n}/2 \quad (3)$$

$$S_{0,2n+1} = S_{1,n} - D_{1,n}/2 \quad (4)$$

Where S refers to smooth, D refers to detail, and n is an index. $S_{0,2n}$ and $S_{0,2n+1}$ are two consecutive pixels of the cover image. The subscripts 0 and 1 correspond to the level of HDWT where, 0 refers to original pixel and 1 refers to the first level of HDWT.

On contrast, IWT converts integers to integers and avoids floating-point coefficients [17]. Therefore, the loss of the image data is totally avoided and complete reversibility is conducted. IWT can be computed using HDWT by rounding the obtained average as described in Eqs. (5) and (6). But, when invers IWT is applied as described in Eqs. (7) and (8), an error resulted from the rounding of these coefficients which may produce data loss and perfect extraction of embedded data may not be achieved [18].

$$S_{1,n} = \left\lfloor \left(S_{0,2n} + S_{0,2n+1}\right)/2 \right\rfloor \quad (5)$$

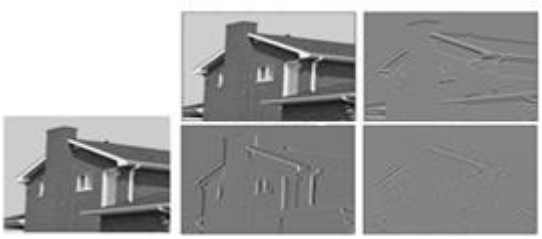

Figure. 1 Shows the output sub bands of IWT

$$D_{1,n} = S_{0,2n+1} - S_{0,2n} \quad (6)$$

$$S_{0,2n} = S_{1,n} - \left\lfloor D_{1,n}/2 \right\rfloor \quad (7)$$

$$S_{0,2n+1} = S_{1,n} + \left\lfloor \left(D_{1,n} + 1\right)/2 \right\rfloor \quad (8)$$

Therefore, another method to perform IWT without losing invertibility is the lifting scheme. Lifting scheme uses simple truncation to implement IWT through two steps: first, computation of the difference between two consecutive pixels then in the next step, the computed difference is used to calculate the average as described in Eqs. (9) and (10). Also, lifting scheme allows direct invers of IWT as described in Eqs. (11) and (12) [5, 18].

$$D_{1,n} = S_{0,2n+1} - S_{0,2n} \quad (9)$$

$$S_{1,n} = S_{0,2n} + \left\lfloor D_{1,n}/2 \right\rfloor \quad (10)$$

$$S_{0,2n} = S_{1,n} - \left\lfloor D_{1,n}/2 \right\rfloor \quad (11)$$

$$S_{0,2n+1} = D_{1,n} + S_{0,2n} \quad (12)$$

Using lifting scheme to perform IWT ensures finite integers coefficients. Therefore, reversibility and perfect reconstruction of the data are achieved. IWT decomposes the image into four sub bands, the first sub band is low-frequency sub band (LL) and the other three sub bands are high-frequency which are LH, HL, and HH. Fig. 1 shows the output sub bands of IWT. The proposed scheme contains two stages which are embedding the secret data in the cover image and the extraction of it from the stego image. The required steps to conceal and extract the secret data are presented in the next subsections.

3.1 Embedding the secret data

The proposed method depends on hiding the secret data in the edges of the cover images. The edges' coefficients strength can be identified by their magnitude value. Therefore coefficients with higher magnitude, provide higher opportunities to embed more data in these coefficients without affecting the

visibility of the image. Most of the research articles which depend on IWT conceal the secret message in the HH sub-band firstly and if this band is not sufficient, the rest of the secret data are embedded in LH then HL. The idea behind the proposed method is to embed the secret message in the three bands at the same time by distributing it through the edged coefficients. The coefficient is represented by eight bits. The last (eighth) bit of the coefficient starting from right is the sign bit (0 means a positive coefficient while 1 means a negative coefficient). The rest of the bits represent the strength of the coefficient, and its capacity to afford data hiding. The coefficients have been categorized according to their value and so their data embedding capabilities. The first bit with value of "1" before the sign bit which is called the most significant bit (MSB) specifies the category of the coefficient. Fig. 2 illustrates different categories of coefficients, the first coefficient in the figure represents "category 7", where the first bit containing value of "1" before the sign bit is in the seventh bit, so the coefficients of this category are greater than or equal to 64 (equivalent to 2^7). The (*) sign means that the bit value may be 0 or 1. The second coefficient represents "category 6", so the coefficient of this category is greater than or equal 32, and so on until "category 2", where the coefficient of this category is greater than or equal 2. The data embedding starts from the first LSB of each category and continues toward the sign bit then stops before the MSB of each category. The change in MSB results in distortions in the image and error in the extracted data at the receiver side. Also, whenever the stopping is further from MSB, the image quality after embedding is better while the embedding capacity is less, it depends on the secret size. Therefore, the earlier the extent is, the further it is from the MSB causing better quality and less distortion.

As mentioned, category 7 can conceal more data than other categories, so the proposed idea is based on embedding in category 7 of the selected sub-bands (HH, LH, and HL) first, then proceeding to category 6 of the same selected sub-bands and so on according to the secret message size. Also, the number of LSBs that is embedded in each category according to the selected extent depends on the message size. Fig. 3 illustrates the development of embedding process through different categories within various sub-bands. The embedding capacity E_{cap} can be calculated by summing the embedding capacities of different categories. Where the embedding capacity of each category is calculated by the multiplication of the number of coefficients in that category by the embedding bits in each coefficient of that category. Eq. (13) represents the embedding capacity E_{cap}.

$$E_{cap} = \sum_{c=7}^{2} Cof_c \times B_c \quad (13)$$

Where Cof_c refers to the number of coefficients in the category c, B_c refers to the number of embedding bits in the category c. Steps of the embedding process are described as follows.

1- The secret message is converted into a binary vector SM. A binary random sequence SK is generated which is used as a secret key for the steganography process. The size of SK is equal to the size of SM.
2- A gray scale image CI of size $M \times N$ is used as a cover image in which SM is concealed. First level IWT is applied on CI to decompose the image into four frequency sub-bands which are LL, HL, LH, and HH. The detailed sub-bands HH, LH, and HL are selected to conceal the secret message.
3- For each selected sub-band, categories from category 7 (C_7) to category 2 (C_2) are identified based on the MSB of each coefficient in the selected sub-bands. For example, the coefficient value 71 in binary [01000111] belongs to C_7, where bit number 7 from the right is equal to 1. Category 6 contains all coefficients that bit number 6 from the right (b_6) is equal to 1, and so on for all categories. Original positions of all coefficients collected from the categories are saved.
4- Concatenate the corresponding categories from the selected sub-bands to form one group for each category starting from high edged sub-bands. For example, category C_7 contains [C_{7HH}, C_{7LH}, C_{7HL}], C_6 contains [C_{6HH}, C_{6LH}, C_{6HL}] and so on for all categories.
5- Embedding starts from C_7 through C_2 according to the size of the secret message. The XOR function is used for the embedding process, where the stego bit (S_i) is achieved by replacing the LSB value of the coefficient in the category with the result obtained from applying XOR function between the secret message bit (SM_i) and the secret key bit (SK_i), as indicated by Eq. (14).

$$S_i = SM_i \oplus SK_i \quad (14)$$

The number of embedded bits in each category is controlled by the size of the secret message and the embedding efficiency. The embedding process is done gradually starting by LSBs from C_7 then C_6 and so on continuo through the next categories till the secret message is finished. Embedding

efficiency decreases sharply whenever the number of the used LSBs of C_7 and C_6 increase so, the maximum number of LSBs which can be used from these categories is four. Less numbers of LSBs are used from the other categories such as C_3 and C_2 (one bit). Therefore, different bit groups can be selected to embed the secret message.

6- After embedding process, stego coefficients are returned to their exact original positions in the detail sub-bands HH, LH, and HL. Invers IWT is applied and the stego image is obtained. Pseudo code1 sums up the steps of the proposed embedding process. A block diagram of the proposed embedding process is shown in Fig. 4.

3.2 Extracting the secret data

The extraction of the secret message requires the stego image and the same secret key used in the embedding process. Fig. 5 shows a block diagram of extraction process which summarizes the following steps:

1. First level IWT is applied on the stego image. Detail sub-bands HH, LH, and HL are obtained.
2. For each selected sub-band, six categories from category n=7 (C_7) to category 2 (C_2) are identified based on the MSB of each coefficient in the selected sub-bands.
3. According to the bit groups selected for different images in the embedding process, the secret message is extracted using XOR function between the secret key and the stego bits of different categories.

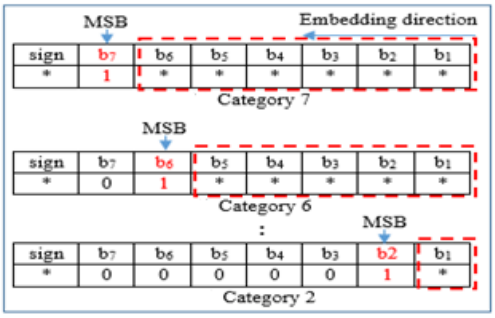

Figure. 2 Different categories of coefficients

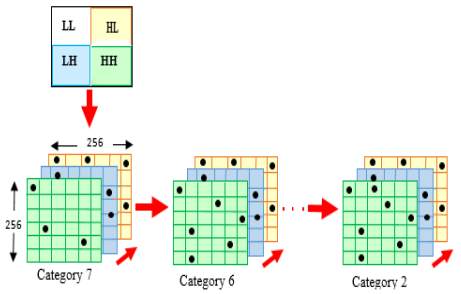

Figure. 3 Embedding process through different categories

1. Input: CI ← cover image, SM ← secret message, SK ← secret key
2. transform CI into 'haar' IWT → (LL, HL, LH, HH)
3. Get HH(m, n); LH(m, n); HL(m, n) coefficient matrixes
4. Convert HH(m, n); LH(m, n); HL(m, n) coefficient matrixes into vectors
5. Initialize Categories ($C_7 – C_2$)
6. For each vector (1: 3)
7. For each coefficient in the vector (1: m*n)
8. Assign the coefficient to the matched category
9. Save the index of the coefficient in the vector
10. End
11. End
12. Get the collected categories of CI with their counts
13. While (SM not empty) && (Categories not full)
14. For each category ($G_7 \rightarrow G_2$)
15. For each coefficient in the category
16. For each bit in selected bit group starting from LSB
17. if SM ⊕ SK = 1
18. Embed 1
19. else
20. Embed 0
21. End
22. Save the modified coefficients in the HH`(m, n); LH`(m, n); HL`(m, n)
23. Apply inverse IWT transform
24. Reconstruct the modified image
25. Get the stego image SI

Pseudo code1. Steps of the proposed embedding process

4. Experimental results

This section demonstrates the empirical evaluation of the proposed method. The implementation was conducted using Matlab®2017 software on an Intel®Core™i7 CPU@1.6GHz computer. Extensive experiments were conducted to evaluate the proposed method using many standard grayscale images. Four 512 x 512 standard images which are Walk Bridge, Boat, House, Lena and Jet were used as cover images [19]. Embedding efficiency and embedding payload are two important factors used to evaluate the proposed steganographic method. Embedding efficiency measures the quality of the stego images. Peak Signal to Noise Ratio (PSNR) is a recognized measure used for comparing variations between the original images and stego images, so it shows the visual quality of the stego images.

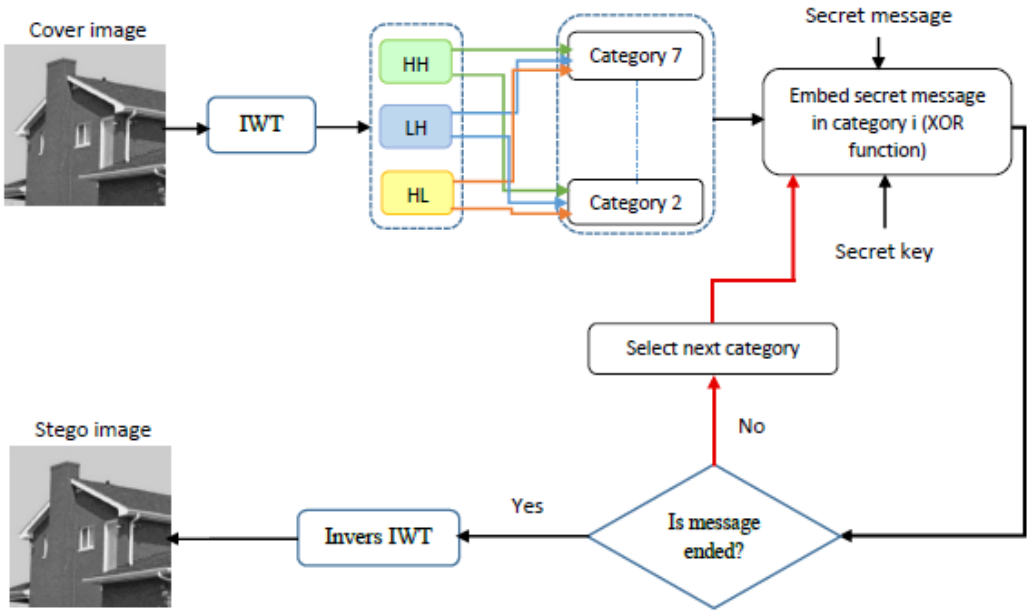

Figure. 4 Block diagram of the proposed embedding process

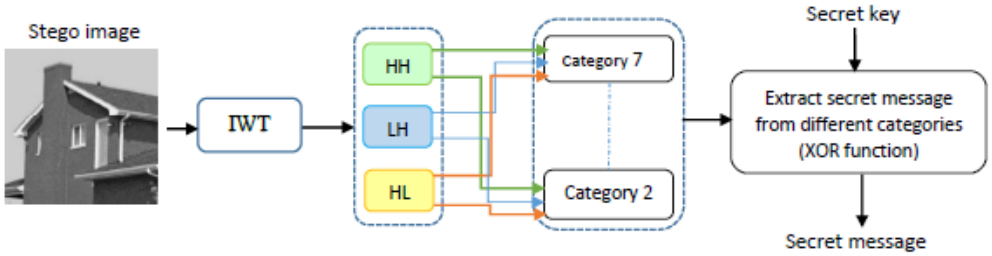

Figure. 5 Block diagram of the extraction process

Figure. 6 Cover images and corresponding stego images Walk Bridge, Boat, Lena, and Jet

As PSNR increases, the quality of the stego image increases. Also, the Mean Square Error (MSE) is the accumulative error between cover and stego images and it is better at decreasing. The PSNR and MSE are defined in Eqs. (15) and (16) [20]:

$$PSNR = 10\log_{10}\left(\frac{(255)^2}{MSE}\right) \quad (15)$$

$$MSE = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[C_I(i,j) - S_I(i,j)]^2 \quad (16)$$

Where 255 is the number of potential pixels in the cover images, C_I is the cover image and S_I is the stego image.

Another quality metric is the Average Difference (AD) which indicates the difference between the

cover image and its stego version, where if the value of AD is 0 then cover and stego images are identical. AD is calculated using Eq. (17) [18]:

$$AD = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} |C_I(i,j) - S_I(i,j)| \quad (17)$$

Embedding payload is the amount of bits embedded in the cover image. Different steganographic methods aim to maximize the embedding payload as possible. Embedding payload (EP) is defined in Eq. (18) [16]:

$$EP = \frac{Number\ of\ embedded\ secret\ bits}{M \times N}\ (bpp) \quad (18)$$

The main idea of the proposed method is based on hiding a secret message in the edges of the image using different pixel categories collected from the three details sub-bands of IWT of the cover image starting from the highest category. In the proposed method, the embedding payload depends on the contained data in the cover image, therefore the embedding rate varies from one cover image to another according to the number of coefficients in each category. Table 1 shows the number of pixels in different categories of the used cover images. Also, the number of bits in the coefficients of each category that used for embedding can be changed. Therefore, different patterns are used for various cover images depending on pixel categories distribution of the images which defines the selected extent for each category. The selected patterns for different images are those that achieved the highest embedding capacity with high PSNR. Table 2 illustrates some used patterns for different images with their MSE, PSNR and AD for different numbers of embedded payload bits. For example, for embedding a payload of 157290 bits in Lena image, the secret message is concealed into the three LSB of all coefficients of categories 7, 6 and 5, then two LSB of all coefficients of category 4, one LSB of all coefficients of category 3, and finally one LSB of some coefficients of category 2 (remainder bits required to convey the payload (R)). Fig. 6 shows the standard cover images used for evaluating the proposed method and the corresponding stego images. It is clear that there is no any visual degradation observed by naked eye in the stego images and their quality is the same as the corresponding cover images. Numerically, the obtained PSNR achieves high and acceptable values, where the minimum value for PSNR to be accepted is 30 dB and the achieved MSE values are very small, therefore the proposed method satisfied the required imperceptibility and quality.

Histogram analysis is done to discover the difference between the cover image and the corresponding stego image according to histogram. It shows the distribution of the secret message over the channels of the histogram of the cover image. It is difficult to locate the position of the secret message in the stego image if the difference between histograms is low. Fig. 7 shows the histogram of Lena cover image and its corresponding stego images at embedding rates 20%, 40%, and 60%. It is clear that the similarity between the histogram of the cover image and the histograms of the stego images is very high. To evaluate the proposed technique according to the literature, results of [16, 5] are used for comparison according to PSNR, MSE, and embedding capacity. Unlike [16], the proposed method uses all coefficients in the cover image for carrying secret data. By this way, the embedding capacity is increased by 20% than [16] with a good average PSNR of 47 dB as illustrated in Fig. 8. In [5], the secret message is embedded in the LSBs of all edge coefficients of HH sub-bands in a horizontal way and if the secret is not finished, the next detail matrix is used. However, in the proposed technique, the embedding depends on the edge coefficients collected from all detail bands which increased the imperceptibility. Also, the maximum message size achieved by [5] is 67.7 kb, while an acceptable PSNR is achieved with higher embedding rates using the proposed method. Table 3 illustrates the quality of the stego images as an average of the PSNR and MSE for the proposed technique and researches [5] and [16]. It is clear that the quality of the stego images of the proposed technique outperforms the quality of the proposed techniques in [5, 16]. Table 4 presents a comparison between the proposed technique and other state of the art steganographic techniques according to embedding capacity and imperceptibility using the common used images.

Table 1. Number of pixels in different categories of used images

	C_7	C_6	C_5	C_4	C_3	C_2
Boat	877	4672	16302	39498	50878	43148
Walk Bridge	1516	12387	32580	45485	43675	31750
Lena	271	2591	9402	23938	47644	54190
Jet	1076	3680	9078	17292	33275	50932

Table 2. Used patterns of used images

Image	Secret payload (bits)	Used pattern	MSE	PSNR	AD
Lena	13107	C_7*2+C_6*2+R	0.053	60.866	0.0430
	26214	C_7*2+ C_6*2+ C_5*2+ R	0.137	56.763	0.0952
	52429	C_7*2+ C_6*2+ C_5*2+C_4*1+ R	0.200	55.117	0.1496
	78643	C_7*3+ C_6*3+ C_5*2+ C_4*2+ R	0.392	52.192	0.2560
	104860	C_7*3+ C_6*3+ C_5*2+ C_4*2+ R	0.453	51.564	0.3107
	131072	C_7*3+ C_6*3+ C_5*2+ C_4*2+ C_3*1+ R	0.520	50.963	0.3603
	157290	C_7*3+ C_6*3+ C_5*3+ C_4*2+ C_3*1+ R	0.798	49.108	0.4663
	183500	C_7*4+ C_6*4+ C_5*3+ C_4*3+ C_3*1+ R	1.617	46.041	0.6630
Walk bridge	13107	C_7*2+ R	0.044	61.616	0.0402
	26214	C_7*2+ C_6*1+ R	0.071	59.564	0.0657
	52429	C_7*2+ C_6*1+ C_5*1+ R	0.1534	56.2719	0.1393
	78643	C_7*2+ C_6*2+ C_5*1+ R	0.2743	53.7485	0.2213
	104860	C_7*2+ C_6*2+ C_5*1+ R	0.3622	52.5408	0.2932
	131072	C_7*2+ C_6*2+ C_5*2+ R	0.5917	50.4099	0.4148
	157290	C_7*2+ C_6*2+ C_5*2+ C_4*1+ R	0.6511	49.9942	0.4573
	183500	C_7*3+ C_6*3+ C_5*2+ C_4*1+ R	1.1315	47.5941	0.6018
Boat	13107	C_7*2+ C_6*1+ R	0.037	62.4017	0.0339
	26214	C_7*2+ C_6*2+ R	0.106	57.8609	0.0857
	52429	C_7*2+ C_6*2+ C_5*2+ R	0.239	54.3322	0.1753
	78643	C_7*3+ C_6*3+ C_5*1+ C_4*1+ R	0.369	52.4525	0.2430
	104860	C_7*3+ C_6*3+ C_5*2+ C_4*1+ R	0.475	51.3637	0.3111
	131072	C_7*3+ C_6*3+ C_5*2+ C_4*2+ R	0.792	49.1418	0.4559
	157290	C_7*3+ C_6*3+ C_5*2+ C_4*2+ R	0.843	48.8701	0.4996
	183500	C_7*3+ C_6*3+ C_5*2+ C_4*2+ C_3*1+ R	0.912	48.5278	0.5469
Jet	13107	C_7*2+ C_6*1+ R	0.049	61.2228	0.0430
	26214	C_7*2+ C_6*2+ C_5*1+ R	0.105	57.9112	0.0817
	52429	C_7*2+ C_6*2+ C_5*2+ C_4*1+ R	0.222	54.6541	0.1568
	78643	C_7*3+ C_6*3+ C_5*2+ C_4*2+ R	0.553	50.7007	0.2773
	104860	C_7*3+ C_6*3+ C_5*2+ C_4*2+ C_3*1+ R	0.612	50.2584	0.3239
	131072	C_7*3+ C_6*3+ C_5*3+ C_4*3+ C_3*1+ R	1.367	46.7711	0.4991
	157290	C_7*4+ C_6*4+ C_5*4+ C_4*3+ C_3*1+ R	3.162	43.1310	0.7134

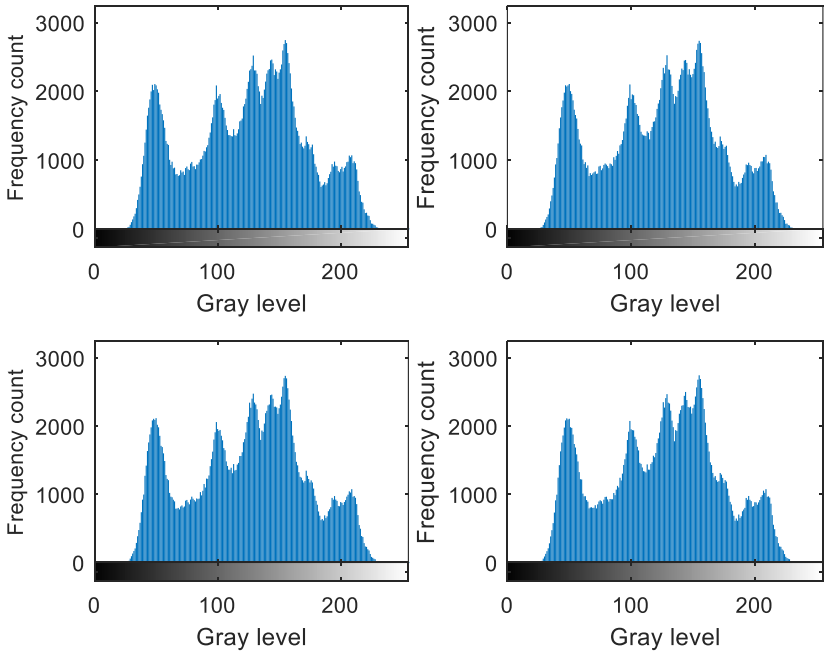

Figure. 7 Original histogram of Lena image and histograms at different embedding rates (20%, 40%, 60%)

Table 3. Comparison between the proposed technique and techniques in literature

Message size (kb)	*[16]*		*[5]*		*Proposed technique*	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
6.3	0.0217	64.76	0.0271	63.80	0.0178	64.1864
12.8	0.0460	61.50	0.0559	60.66	0.0539	60.9532
28.8	0.1328	56.91	0.1360	56.79	0.1227	57.2588
51.2	0.3551	52.62	0.2165	54.78	0.2644	55.0938
67.7	0.6094	50.28	0.2788	53.68	0.2596	54.0934

Embedding in approximation band in [14] degraded the value of PSNR at limited payload capacity. In [13], only one bit of secret data is embedded in the approximation band which increased the PSNR and limited the payload. In [9], embedding is occurred in spatial domain using histogram, this method slightly increased the payload but decreased the PSNR. The proposed technique embeds more than one bit of secret data in each coefficient of detail bands of the frequency transformation of the image which increased the payload with keeping the PSNR at high level. Therefore, it is shown that the embedding capacity of the proposed technique is superior the other techniques with achieving good imperceptibility.

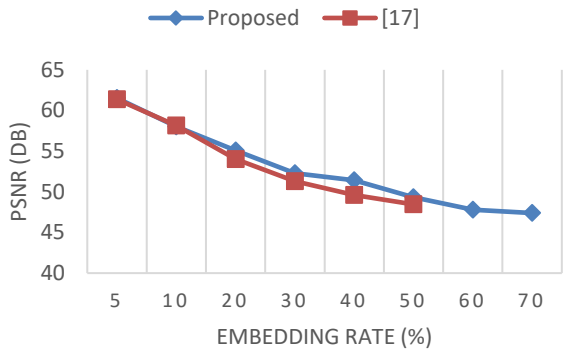

Figure. 8 comparison between proposed technique and [16]

Table 4. Comparison between the proposed and previous techniques

Reviewed studies	**Image**	**Bpp**	**PSNR**
Islamy and Ahmad [9]	Lena	0.4351	> 30
	Boat	0.3524	> 30
Valandar et al. [13]	Lena	0.2500	53.21
	Jet	0.2500	52.68
Emad et al. [14]	Lena	0.2500	35.39
	Boat	0.2500	35.67
	Jet	0.2500	34.70
Proposed method	Lena	0.7000	46.04
	Boat	0.7000	48.52
	Jet	0.6000	43.13

5. Conclusions

Hiding Information in the high frequency sub-bands (LH, HL, and HH) increases the robustness and ensures the visual quality, where the HVS is less sensitive to modifications in these sub-bands. In this paper, IWT was used to hide a secret message in grayscale images. The most significant categories were collected from the three detail sub bands of the transformed cover images. The embedding of the secret message started by occupying the highest categories then the lowest until finishing the size of the secret message. The number of LSBs used from each category was indicated according to the number of coefficients in the category and the message size. XOR function was used to decrease the difference between the cover image and stego. The experimental results showed that the proposed method achieved good performance for high embedding rates (up to 70%) and exceeded methods in the literature. Also, the proposed method can be applied on colour images. For future work, cryptography and steganography techniques can be combined together to enhance the security of data. Also, different transformation domains can be used.

Conflicts of Interest

The authors declare that they have no conflict of interest.

Author Contributions

The conceptualization, methodology, implementation, experiments, supervision and writing—original version preparation are provided by EMFE and NIRY. Writing—review, editing and project administration are provided by NIRY and EMFE.

Acknowledgement

The authors appreciate National Research Centre (NRC), Cairo, Egypt for supporting this work through research project No (12010501).

References

[1] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research", *Neurocomputing*, Vol. 335, pp. 299-326, 2019.

[2] A. Zenati, W. Ouarda, and A. M. Alimi, "SSDIS-BEM: A New Signature Steganography Document Image System based on Beta Elliptic Modeling", *Engineering Science and Technology, an International Journal*, Vol. 23, No. 3, pp. 470-482, 2020.

[3] K. Ntalianis and N. Tsapatsoulis, "Remote authentication via biometrics: a robust video-object steganographic mechanism over wireless networks", *IEEE Transactions on Emerging Topics in Computing*, Vol. 4, No. 1, pp. 156-174, 2015.

[4] A. S. Brandao and D. C. Jorge, "Artificial neural networks applied to image steganography", *IEEE Latin America Transactions*, Vol. 14, No. 3, pp. 1361-1366, 2016.

[5] A. Miri and K. Faez, "An image steganography method based on integer wavelet transform", *Multimedia Tools and Applications*, Vol. 77, No. 11, pp. 13133-13144, 2018.

[6] V. Verma, S. K. Muttoo, and V. Singh, "Enhanced payload and trade-off for image steganography via a novel pixel digits alteration", *Multimedia Tools and Applications*, Vol. 79, No. 11, pp. 7471-7490, 2020.

[7] G. Swain, "Two new steganography techniques based on quotient value differencing with addition-subtraction logic and PVD with modulus function", *Optik*, Vol. 180, pp. 807-823, 2019.

[8] S. Chakraborty, A. S. Jalal, and C. Bhatnagar, "LSB based non blind predictive edge adaptive image steganography", *Multimedia Tools and Applications*, Vol. 76, No. 6, pp. 7973-7987, 2017.

[9] C. C. Islamy and T. Ahmad, "Enhancing Quality of the Stego Image by Using Histogram Partition and Prediction Error", *International Journal of Intelligent Engineering and Systems*, Vol. 14, No. 2, pp. 511-520, 2021.

[10] P. Maniriho and T. Ahmad, "Information hiding scheme for digital images using difference expansion and modulus function", *Journal of King Saud University-Computer and Information Sciences*, Vol. 31, No. 3, pp. 335-347, 2019.

[11] S. Sajasi and A. M. E. Moghadam, "An adaptive image steganographic scheme based on noise visibility function and an optimal chaotic based encryption method", *Applied Soft Computing*, Vol. 30, pp. 375-389, 2015.

[12] V. Chandrasekaran and P. Sevugan, "Applying Reversible Data Hiding for Medical Images in Hybrid Domain Using Haar and Modified Histogram", *International Journal of Intelligent Engineering and Systems*, Vol. 10, No. 4, pp. 126-134, 2017.

[13] M. Y. Valandar, M. J. Barani, P. Ayubi, and M. Aghazadeh, "An integer wavelet transform image steganography method based on 3D sine chaotic map", *Multimedia Tools and Applications*, Vol. 78, No. 8, pp. 9971-9989, 2019.

[14] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed, and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform", *Journal of Systems Engineering and Electronics*, Vol. 29, No. 3, pp. 639-649, 2018.

[15] R. E. Safy, H. Zayed, and A. E. Dessouki, "An adaptive steganographic technique based on integer wavelet transform", In: *Proc. of 2009 International Conference on Networking and Media Convergence*, pp. 111-117, 2009.

[16] H. A. Dmour and A. A. Ani, "A steganography embedding method based on edge identification and XOR coding", *Expert Systems with Applications*, Vol. 46, pp. 293-306, 2016.

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

[18] P. K. Muhuri, Z. Ashraf, and S. Goel, "A Novel Image Steganographic Method based on Integer Wavelet Transformation and Particle Swarm Optimization", *Applied Soft Computing*, Vol. 92, p. 106257, 2020.

[19] *USC-SIPI Image Database. [Online]*. Available: http://sipi.usc.edu/database/database.php?volume=misc.

[20] E. M. E. Houby and N. I. Yassin, "Wavelet-Hadamard based blind image watermarking using genetic algorithm and decision tree", *Multimedia Tools and Applications*, Vol. 79, No. 37, pp. 28453-28474, 2020.