Journal of Iraqi Al-Khwarizmi (JIKh) Volume:6 Issue:2 Year: 2022 pages: 57-68

An Image Steganography By using 2 D Integer Wavelet Packet Based on Adaptive Non Maximal Suppression

[1]Sally A. Mahdi, [2]Maisa'a Abid Ali Khodher
Computer Sciences/University of Technology-Iraq, Bagdad-Iraq
[1]cs.19.68@grad.uotechnology.edu.iq.
[2]110044@uotechnology.edu.iq.

Published online 29-11-2022

Abstract: - The advancement of digital data has this leads to rising information security requirements. To protect the privacy and confidentiality, technology. One of the technologies capable of shielding data from unauthorized capture is digital steganography. This paper presents combined between spatial domain and transform domain, also using the secret key for sharing between two parties. Discrete Wavelet Packet (DWPT) in digital image steganography is a well-known technique that is more consistent with the Human Visual System (HVS). However, any loss of information may be caused by the DWPT floating point. So Integer Wavelet Packet Transform (2D IWPT) by using Lifting Haar scheme to give good results and without losing data. In spatial domain using LSB and MSB for hiding information by control pixels' position by using secret-key (Adaptive non-maximal suppression) and sharing between two parties. The result of this paper when applying on the different image gives a high PSNR of 78.430 and less MSE of 0.01when inserting message 1000 bits and reduction value PSNR of 49.7 and MSE of 0.69 when inserting message 823567 bits and measure entropy is the close value for cover image and stego –image then this method is more security for the attacker or unauthorized person.

Keywords: - Steganography, IWPT, LSB, MSB, ANMS.

1- Introduction

The internet is providing a lot of advantages to humans, particularly to exchange or get information, working, learning, and so on. Privacy of data and security are the problems of internet. A lot of approaches were utilized to provide security including digital signatures, steganography, cryptography, and watermarking [1]. Steganography comes from Greek words and indicates hidden writing, as "stegano" refer to "covered", while "graphy" refer to "writing" [2]. Image stenography has two major techniques according to its domain, spatial domain, and the transform domain uses spatial domain techniques such as Least Significant Bit (LSB). etc. To hide secret information in the frequency domain [3]. which provides improvements in the data hiding capacity as well as security of the secret data [1]. Also in transform domain using integer wavelet transform (IWT) is a more efficient method to hide secret information without distortion [4]. In this paper using steganographic technique based on IWPT by the use of a lifting haar scheme and adaptive non-maximal suppression. IWPT return all text without loss data. The embedded coded message is barely detectable by the human visual system (HVS) due to the inclusion of more embedding bits in the strong block (contain key points) than the weak block (does not contain key points), high payload is hidden by using LSB and MSB due to the proposed Adaptive non-maximum suppression.

The proposed method of the paper is organized as follows: literature review which are related to the proposed method is given in Section 2. Section 3 introduced about integer wavelet transform by using lifting haar scheme. In Section 4 is clarified feature extraction and adaptive non maximal suppression. Factors Effective Steganographic Method in section 5. Section 6 describes the proposed embedding and extraction procedures. In Section 7, experimental results are presented, and, finally, the paper is concluded in Section 8.

2. Literture Review

Below some of the research which are related to the proposed method. in this part, some of the previous works will be illustrate, which are related to image steganography technique spatial domain and transform domain.

- **In 2018**, K. Gaurav, et. al. have proposed a novel steganography algorithm based on the technique of local reference edge detection and exclusive disjunction (XOR) is suggested. Local reference pixels identified by the Canny edge method and optimized by the morphological dilation operator have embedded the hidden message bits in the sharp regions. The pre-defined pixel sets in the stego image are easily identified with less computational complexity. In terms of protection and capacity, the embedding algorithm improved with bit plane-dependent XOR coding technique, making the least possible changes in edge pixel LSB bits. The current edge-based steganography techniques provide greater imperceptibility, but the embedding capacity techniques are relatively limited. The result of the peak-signal-to-noise Ratio between (49.5251 _ 57.2413) and Mean Square Error between (0.7253_ 0.1227) [5].

- **In 2018,** Atta and Ghanbari2, et al. have proposed a steganography algorithm is based on the wavelet packet decomposition (WPD) and neutrosophic set. First, an original image is decomposed into wavelet packet coefficients. Second, the generalized parent-child relationships of spatial orientation trees for wavelet packet decomposition are established among the wavelet packet sub-bands. An edge detector based on the neutrosophic set named (NSED) is then introduced and applied on several sub-bands. This leads to classifying each wavelet packet tree into edge/non-edge tree to embed more secret bits into the coefficients in the edge tree than those in the non-edge tree. The embedding is done based on the least significant bit substitution scheme. Experimental results demonstrate that the proposed method achieves higher embedding capacity with better imperceptibility compared to the published steganographic methods. The result of the proposed method is illustrated measurements PSNR and MSE in each (RGB) channel which is the result of peak-signal-to-noise Ratio between (51.78-58.81) and the result of Mean Square Error between (0.1087-0.4363) when using Lena image and other image [6].
- **In 2018,** P. Maniriho, et al. have suggested a digital image steganographic technique which is developed based on pixel block, reduced difference expansion (RDE) and constant base point which is intended to enhance the quality of the stego image while achieving a good embedding capacity. According to the experimental results. The result of the proposed method is illustrated measurements PSNR which is the result of peak-signal-to-noise Ratio between (27.72 - 48.27) when using different image [7].
- **In 2018**, W. Elmasry, et al. have proposed method. Firstly, the code word is created with secret data and its CRC-32 checksum, then Gzip compresses the code word just before AES encrypts it, and finally adds it to the encrypted header information for further processing and then embeds it into the cover picture. The Fisher-Yates Shuffle algorithm for selecting the next pixel position is used to embed the encrypted data and header information operation. Different LSBs (least significant bits) of all the color channels of the selected pixel are exploited to hide one byte. The result of the proposed method is illustrated measurements PSNR and MSE which is the result of peak-signal-to-noise Ratio between (42.1145 - 63.2094) and Mean Square error between (3.996- 0.0311) when using lena and baboon image [8].

3. Integer wavelet transform

It is a kind of second generation in wavelet. It is proven that lifting schemes can be used to implement all classical wavelets. IWT has the following benefits when compared to Discrete Wavelet Transform (DWT): DWT transform coefficients are the floating point values, rounding these values to integer results in losing their perfect property of reconstruction. However, the lifting schemes in IWT maps integer to integer without rounding errors. They are easy to understand, implement and invert and fast [6][9].

3.1 Forward Lifting Scheme: - This scheme splits the signal in to an even and odd index. The odd and even samples could be correlated using Haar transform or their own values. So the wavelet coefficient could be calculated using actual samples, odd samples and the prediction, this method is called lifting scheme. After prediction step, the update step must be performed. In the last step the odd elements must be substituted by the difference and the even elements by the averages. Since the lifting scheme ends up to some integer coefficients it will be reversible. The total number of coefficients before and after transformation will be the same for this method.

3.2 Reverse Lifting Scheme: - By specifically reversing the operations of the forward transform with a merge operation instead of a split operation and the reverse lifting scheme, the reverse transform gets back the original signal [10].

4- Feature Extraction

Most image processing techniques aim to extract certain features that are used in various applications like pattern recognition, template matching, object tracking, etc. [11]. To extract key points of an image, there are so many techniques like Harris corners, SIFT, MSER etc. The Harris corners method usually detects numerous key points that would be clustered, redundant and noisy. To regulate the density of characteristics in the image and to improve the spatial distribution. ANMS (Adaptive Non-Maximal Suppression) is a most effective detector that assures well-distributed key points and generally, it has more control over the density of features throughout the image [12].

- **Adaptive Non Maximal Suppression (ANMS)**

ANMS does the aforementioned jobs (better key point distributions) by defining a parameter called correctness strength and also key points coordinates. ANMS has variations in details, but the first version was proposed by Matthew Brown CVPR-2005. It simply defines a suppression radius r and set it to zero, then it will be increased gradually until a certain number of desired key points are acquired like 3x3 points.

The Global maximum is the top of the list which will never be suppressed by any radius. Interest points are applied to the list as the suppression radius decreases from infinity. Nevertheless, once a point of interest emerges, it will always be on the list because if the key point is the maximum in a bigger circle then it will be bigger than any maximum coming from its sub-circles ŕ < r.

In practice, we robustify the non-maximal suppression by requiring that a neighbor has a sufficiently larger strength. Thus, the minimum suppression radius ri is given by practically to make algorithm more robust the non-maximal suppression needs to be checked against its neighbors and it must have larger strength sufficiently. Therefore, the minimum suppression radius ri is given by

$$r_i = min_j \left| x_i - x_j \right|, \quad f(x_i) < c_{robust} f x_j, x_j \in I \quad \ldots (1)$$

Where xi is the key points coordinate and i is the key points coordinate list. C robust is a constant value (0.9) that will assure neighbors have a much higher strength to be suppressed [12] [13] [14].

5. Factors Effective Steganographic Method

Measuring image quality requires a comparison of cover image results and stego image and common measurements that are used (Peak Signal-to-Noise Ratio, Mean Square Error, payload).

1) Mean Square Error (MSE): - It is a measure between cover image and stego image C (x, y) and S (x, y) is calculated by using the following equation: -

$$MSE = \frac{\sum_k \quad [C(x,y) - S(x,y)]^2}{x * y} \qquad \textbf{(2)}$$

Where x is represented number of rows and y is the number of columns inside the cover image [15].

2) Peak Signal-to-Noise Ratio (PSNR): -The PSNR of the cover image and stego image is calculated by using the following equation

$$PSNR = 10log_{10}\left(\frac{R2}{MSE}\right) \qquad \textbf{(3)}$$

The maximum image pixel value is 'R', that the R=2b-1, b is represented bit bottom of the cover image, MSE is represented Mean Square Error. PSNR measurement is done in decibels(db). To compare the results of the same restored image, PSNR is used as a good measure.

3) Capacity (Payload): - It is the scale of the information in original image that may be changed. However, the integrity of the cover image is not affected. Payload depends on the full no. of bits according to pixel and the range of bits embedded in every pixel. Where the payload is in bits per pixel (BPP) and the maximum capacity (MHC) is to hide in percentage.

$$payload = no.of\ secret\ message\ bits\ /size\ of\ cover\ image \quad (4)$$

4) Histogram: - The histogram evaluates number of events of a definite density pixel value in the entire image. The number of pixels varies with a change in the density value due to a change in the LSB pixels, better to be the differences in histogram less between the cover image and the Stego image because these changes can be used to reveal the secret message in steganalysis [16].

5) Information entropy: - Measure security of steganography system by using entropy. Let $e_1, e_2, e_3, \ldots e_n$ be n possible element with probabilities $p(e_1), p(e_2), p(e_3)$ .The entropy is given as :-

$$H(e) = \sum_{i=1}^{n-1} p(e_i) log_2 p(e_i) \quad (5)$$

This comparison produces an evaluation of the average minimum no. of bits that are needed to encode a sequence of bits based on the frequency of the symbol.

6) Correlation coefficient: - The measurement of correlation coefficient r is compute to the range and trend of the linear set of two randomize variables. If two variables are near regarding, the value of correlation coefficient is near to value of 1. If the value coefficient is near to 0, two variables are not regarding. The value of coefficient r can be calculated using the following equation [17].

$$\mathbf{r=} \frac{\sum_i (x_i - x_m)(y_i - y_m)}{\sum_i \sqrt{\sum_i (x_i - x_m)^2} \sqrt{\sum_i (y_i - y_m)^2}} \quad \textbf{……(6).}$$

6. Proposed Method

In this proposed method using 2 D Integer wavelet packets (lifting haar scheme) because this method solves problem floating value in Discrete wavelet packet so convert values to an integer but not using truncating process because this auxiliary data leads to a reduction in the capacity of hiding as well as visual quality and the loss of data, therefore, it is using lifting haar scheme to return all data .When the input data is in the form of an integer, perfect reconstruction is possible while applying Inverse transform. The difference between Integer Wavelet Packet Transform (IWPT) and Discrete Wavelet Packet Transform (DWPT), the LL (Low-Low) sub-band in the case of Integer Wavelet Packet Transform appears to be a close copy with the smaller scale of the original image, while in the case of DWPT resulting LL sub-band is distorted. It uses 1 level and divided in to 4 sub-band, the lowest frequency is used in the proposed method because it contains information of image close to the original image for detect corners and hidden information in LL part. The stego image LL can withstand compression and no loss of data while retrieving. So embedded secret text in these corners by using modified LSB and MSB.

6.1 Hiding phase

This method implemented in three stages.

1- Strong Corner Detection Stage: -

Corners are being detected in the image by using Harris detector and ANMS adopted to control the number of Harris points in the image and better distribution of key points such that they are equally distributed of key points across the image and the best result from Harris. The purpose here is to ensure that the non-max suppression region is adaptive. Thus it was implemented it to consider only those interest points that have as high a corner value and are far away from each other as possible that is a local maximum in the 3x3 pixel region. Once have these points, then it was select the points that are greater than the average of corners scores of all pixels in the image.

This is achieved to limit the number of computation. When find the radius around each pixel where it has the greatest corners score i.e. The radius taken is the distance till the nearest interest point of greater corners score by using equation (1). Firstly, converts image LL into the greyscale and applies Harris function and uses adaptive algorithm in approximate LL based on radius=3, after detect corner, so determining these key points position or

coefficient coordinate CC in to LL colors (RGB) because it must have used this color image original for hiding text. Algorithm (1) is used to implement ANMS.

hm 1: ANMS algorithm
Input: Cover Image **Output**: Interest point detected by ANMS strong point
Begin Nstrong: number of local maxima **Step1**: Read cover image **Step2:** Perform 1level Integer wavelet packet using lifting haar algorithm. **Step3**: Apply Harris corner on Image LL after convert image to grey scale. **Step4**: Divide image into 3*3 windows **Step6**: Map each CC from grey scale Image LL in to color image LL **End**

2- Embedding Stage: -

After complete determine key points position in approximate LL. Each block has been verified whether it contains key points or not, depending on the threshold, which is not static due to the discovery of the number of key points varies from one image to the other. Strong block is determined based on threshold, when Blocks contain key points so (the number of key points large than a threshold value) have been determined which detected by using ANMS. As for the rest, the blocks that have not been exposed are blocks that do not contain Adaptive (weak block). Moreover, the data has been included in both types in order to increase security and give strength to the secret key, as well as the difference in the inclusion in the Corner and Smooth also, it is difficult for the hacker to discover the places of inclusion in the strong block. Compute dynamic threshold based on equation (7) and (8).

$$\text{Number of block} = \frac{Size\ of\ Image\ LL}{Adaptive\ window(3*3)} \quad \ldots \textbf{(7).}$$

$$\text{Threshold} = \frac{no.keypoints}{no.of each\ block\ calculate} \quad \ldots \textbf{(8)}$$

The secret text will be embedded in strong and weak block, so strong block is dependent on threshold and used modified LSB and MSB for embedding. It is taken last 3 bit from MSB and applied condition if MSB contains last 3 bit is (000) will be replaced first 3 bit from LSB with secret text to embed in dark region more than light region. However, if contain MSB one in last 3bit such as (001,100,101,010,111) so will be replacement 2 bit from first LSB with encryption text.

When the block was weak, the secret text would be hidden in all block points by used also MLSB and MSB, so take the last 3 bit from MSB and apply condition if MSB contains last 3 bit is (000) will be replaced first 1 bit from LSB with secret text. However, if contain MSB one in the last 3bit such as (001,100,101,010,111) so will be replacement second bit from LSB with text.

The center of the block is changed by used the red color and blue color because the receiver wants to know two types of block that contain key point or not, so used two-color red and blue. When the block was strong, replace first bit in LSB by 1 in red color and replace first bit in LSB by 0 in blue color, the text is not hidden in these colors red and blue. When the block was weak, replace the first bit in LSB by 0 in red color and replace first bit in LSB by 1 in blue color. So that the recipient can know the embedded points and extract the text. Figure (1) shows the implementation of the embedding stage. Algorithm (2) was used for clarify embedding text based on ANMS.

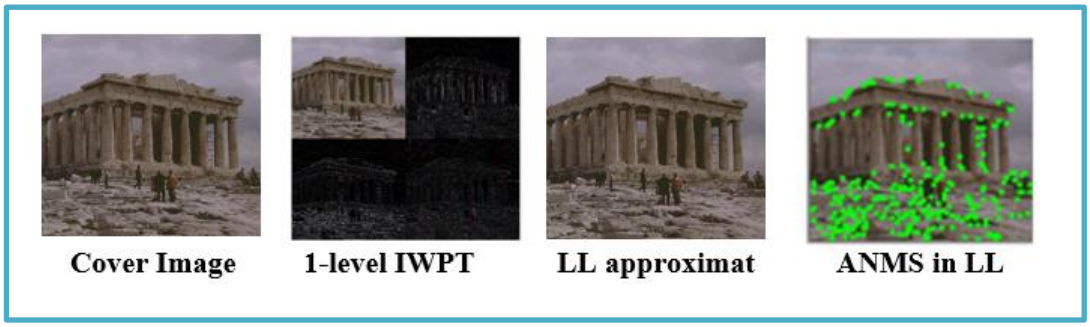


Figure (1): The implementation of the embedding stage

lgorithm 2 : Embedding text based ANMS

Input: Cover Image, Encryption text
Output: Stego_Image

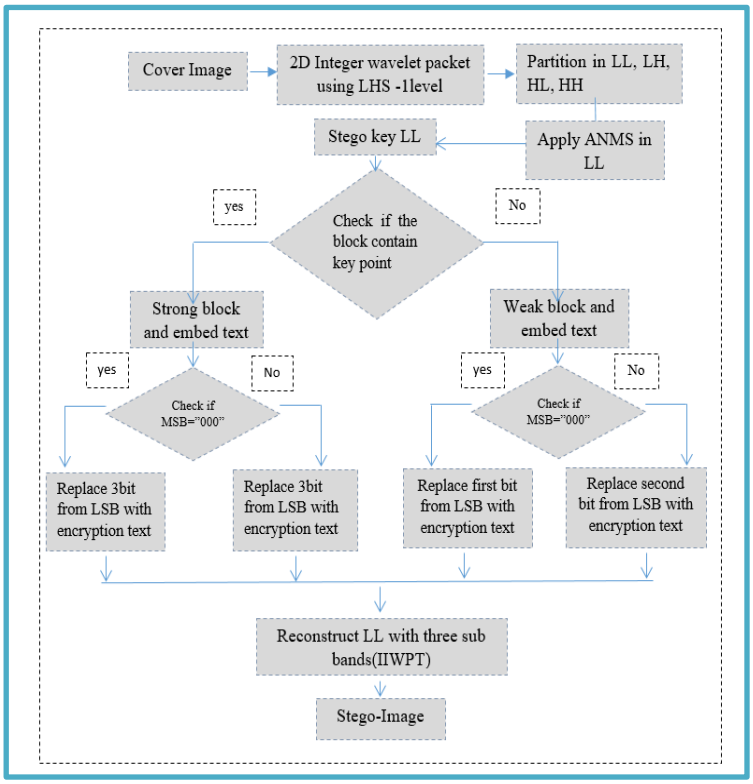
Begin
N strong=number of strong key point
Step1: Read cover Image and text.
Step2: perform algorithm1 in LL and obtain ANMS image
2.1 Calculate no of block based on equation (7)
2.2 Compute threshold based on equation (8)
2.3 If Nstrong > threshold value
Set corresponding it strong Block (ANMS block)
Else it corresponding it weak block
End If
Step3: Indicate the block status of Image (LL), get center pixel in each block
First bit from LSB in Red and Blue
If the block is strong then
Set its corresponding bit to 1in Red and Set its corresponding bit to 0 in Blue
Else Set its corresponding bit to 0 in red and Set its corresponding bit to 1 in Blue
End If
Step4: Embedding list strong block and weak block
For each block in image LL do
4.1 If the block is strong **then**
If MSB="000" then
Embed 3 bits in the 3 LSB of each block pixels.
Else Embed 2 bits in the 2 LSB of each block pixels
End If
Else
4.2 If block is weak then
If MSB="000" then Embed in first LSB 1 bit of each block
Else Embed in second LSB 1 bit of each block
End If
End If
End If
End For

Step5: Reconstruct stego LL with sub bands image LH, HL, HH(IIWPT)

End.

3- Inverse Integer Wavelet Packet (IIWPT) by using Reverse (LHR) Stage.

The last phase reconstructs image Inverse integer wavelet packet(IIWPT) by using LHS Reverse steps (Inverse update, Inverse predict, Merge) and send Stego-Image to receiver over secure transmition. Illustrate in figure1 the flowchart of embedded of ANMS and MLSB.



6.2 Extraction phase

Extracting phase was the reverser of the Embedding step, after applying 2D Haar Integer wavelet packet (IWPT) on Stego Image in 1 level (4 sub bands) LL, HL, LH, HH, only LL used for extract secret text.

It would check only center pixel (red and blue) in all block in LL extract the text by the same method in hiding phase for each strong and weak block. If the center pixel (red=1 and blue=0) so this block is strong

The text would be extracted, where was used MLSB and MSB, which take last 3 bit from MSB and apply condition if MSB contains last 3 bit is (000) will be extracted first 3 bit from LSB, but if contain MSB one in the last 3bit such as (001,100,101,010,111) so will extract 2 bit from first LSB but when check center pixel,(red=0 and blue=1) so this is weak block ,extracted the text by taking last 3 bit from MSB and apply condition if MSB contains last 3 bit is (000) will be extracted first 1 bit from LSB but if contain MSB one in the last 3bit such as (001,100,101,010,111) so will be extracted a second bit from LSB ,as explained in Figure (3). Algorithm (3) implements extracting text based ANMS and MLSB.

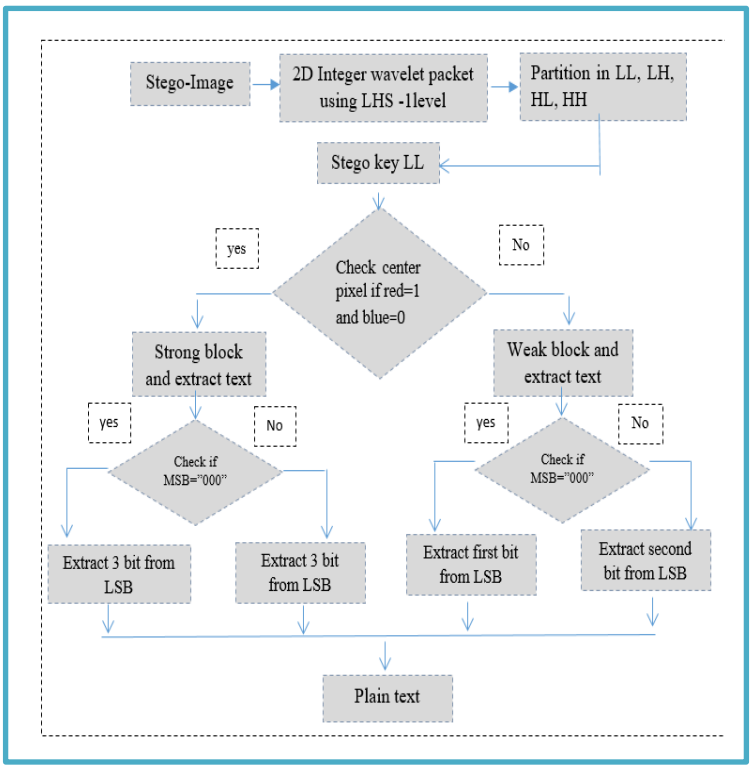


Figure (3): The flow chart of extracted text of ANMS and MLSB

Algorithm 3: Extracting text based ANMS and MLSB

Input: Stego_Image

Output: Encryption text

Begin

Step1: Read Stego_Image

Step2: Perform 1 level IWPT using lifting haar scheme on Stego_Image

Step3: Apply 3*3 window on Stego LL

Step4: Determine Strong block and weak block:

For each block in image **do**

Select the center pixel from each block and check three colors

If the first bit in red =1 and the first bit in blue =0 then

The corresponding block is strong

Else If the first bit in red =0 and the first bit in blue =1 then The corresponding block is weak block

End If

End For

Step5: Extract secret message bits: For each block in image do

If the block is strong then

If MSB="000" then Extract 3 bit from 3 LSB from each block except the center block

Else

Extract 2 bit from 2 LSB from each block except the center block

Else

If the block is weak then

If MSB="000" then Extract 1 bit from first LSB from each block except the center block

Else Extract 1 bit from second LSB from each block except the center block

End If

End If

End If

End If
End For
Step6: Repeat steps from step5 until extract all text
End.

7. Evaluation and Result

The proposed method has been used four factors to evaluate between the cover image and stego image and implement this method in language C# visual studio 2019.The method has experimental on different images , that include dataset in link https://decsai.ugr.es/cvg/dbimagenes/USF-DM.University of South Florida. It is used different formats (BMP, PNG, TiFF, JPEG) and size 512*512 based on using proposed idea (IWPT and ANMS). In figure 4 represent some images from dataset.

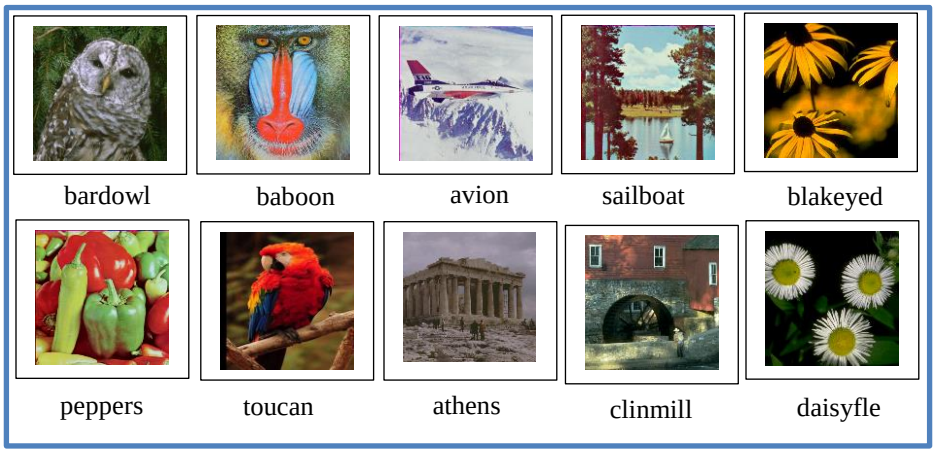


Figure (4): The implementation of the proposed method on different

The method proposal has been used the ANMS method for control distribution corner in image Harris, number of key point (Harris) =11441, where the corner was discovered only strong block in LL. The radius has been chosen r=3, after test from r=5 to r=3, in which the points are good for hiding and dynamic threshold

***Table (1)**: Test radius on the cover image(Athens)*

ANMS	Threshold	Radius
491	0.017	5
637	0.022	4
799	0.027	3

In table (2) represent the result of the proposed method by experiment on three images and different image format and insert message between(1000to515858) bits. Also the value of correlation coefficient is very good.

In table (3) represent the comparison between the proposed method (ANMS and MLSB) without IWPT with other methods when using the same secret message length and image and same payload to compare method is strong or not and when applying proposed method will be very good and gives high PSNR and less MSE according to other methods.

In table (4) represent the comparison between the proposed method (ANMS and MLSB) with IWPT and other methods when using the same secret message length and image and same payload to compare method is strong or not and when applying proposed method will be very good and gives high PSNR and less MSE according to other methods.

In table (5) represent the proposed method and compare with another method that all values in PSNR and MSE gives good result and high PSNR so the proposed method is the best when compare with another method

In table (6) represent the entropy for peppers and athens (.bmp) in cover image and stego-image (512*512).

Table (2): *- Measurements of the proposed method1(ANMS and MLSB) with IWPT for (PSNR, MSE, correlation) between cover image and stego-image.*

Cover image	**PSNR**	**MSE**	**Correlation coefficient**
bardowl.TFIF(1000) **(22262)** **(515858)**	78.4304 70.6404 49.7241	0.01 0.12 0.69	1.0000 0.9760
Athens.PNG(515858)	50.9528	0.52	1.0000 0.9493
daisyfle.BMP(50346)	60.828	0.10	1.0000 0.9658

Table (3): - *Comparisons between proposed method and other methods.*

Cover image and Capacity bits	**Method name**	**PSNR**	**MSE**
toucan-30000	S.Mangayarkarasai[20]	17.4840	1.2497
	Proposed method	60.2498	0.0772
Lena-981	R. Tavoli [19]	57.81	0.1075
	Proposed method	69.537	0.0072
Baboon(217664)	W. Elmasry[8]	40.0834	6.4575
Baboon(277518)	Proposed method	58.1777	0.50
Lena(16569)	P. Maniriho [7]	48.27	---
Lena(16569)	Proposed method	66.321	---

Table (4): *- Comparisons between proposed method and other methods.*

Cover image	**S. A. Seyyedi method based on IWT [18]**	**R.Atta [6]**	**Proposed method**
	PSNR MSE Capacity	**PSNR MSE Capacity**	**PSNR MSE Capacity**
Avoin.BMP	40.18 6.23 (386830)	38.31 - 84058	58.77 0.65 (417725)
Peppers.PNG	40.64 6.75 40000	39.09 - 82615	52.27 0.38 (114250)
Baboon.BMP	38.07 10.13 50000	39.15 - 84902	54.73 0.22 (86050)

Table (5): *- Comparisons between proposed method and other methods(peppers)*

payload rate	N-bppIWT[5] PSNR	N-bpp IWT[5] MSE	Proposed (PSNR)	Proposed (MSE)
5%	61.37	0.047	65.435	0.04
10%	58.14	0.103	62.862	0.05
25%	52.46	0.369	58.462	0.17

Table (6): *- Measure entropy for cover image and stego-image.*

Cover image	Entropy for cover image	Entropy for stego image
peppers.BMP	7.3388	7.4974
athens.BMP	7.7067	7.4762

At the last evaluate is histogram which is comparisons between original image and stego image will be used peppers image and baboon as shown in figure (5) which is the result stego image same of the histogram of cover image for proposed method so each method contains good result.

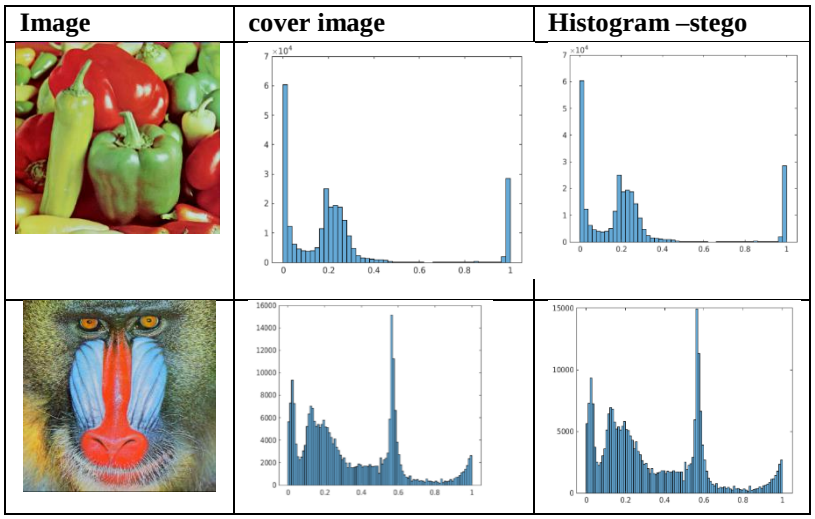


Figure (5): -The measurement of the histogram

8.Conclusion

The proposed used lifting scheme (integer wavelet packet), The lifting scheme has a faster implementation and it allows for the construction of second wavelets. Hence, these transforms are suitable for data embedding which can offer higher embedding capacity and better visual quality. This is the reason for propose Integer Wavelet Packet Transform (IWPT) over Discrete Wavelet Packet Transform (DWPT). The first sub-band of the IWPT was used (LL)because this part contains the most considerable information on the spatial domain image. Generally, low frequency (LL) is least affected by noise as compare to high frequency. So for high robustness against noise, the LL has been selected to hide the secret message and also gives good results with retrieves the entire text. And the secret key (ANMS) has been the results of this proposed method were high in terms of PSNR values, where the result was between (78.430 – 52.27) as well as the capacity was high as the result of the PSNR is not less than the (49.7) in the maximum capacity ratio of the image, and this means that this method is strong and the quality of the image was not affected also high payload when the combination between the spatial domain and the transform domain has been done (IWPT and LSB).

Reference

[1] Y. P. Astuti, E. H. Rachmawanto, and C. A. Sari, *"Simple and secure image steganography using LSB and triple XOR operation on MSB,"* in *2018 International Conference on Information and Communications Technology (ICOIACT)*, 2018, pp. 191–195.

[2] C. K. GS, "*The Various Applications of securing Communication Data with the help of Steganography.",* Vol.4, pp.247-250, 2018.

[3] M. S. Taha, M. S. M. Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, *Combination of Steganography and Cryptography:* A short Survey," in *IOP Conference Series:Materials Science and Engineering*, 2019, vol. 518, no. 5, p. 52003.

[4] S. A. Seyyedi, V. Sadau, and N. Ivanov, "*A Secure Steganography Method Based on Integer Lifting Wavelet Transform.,"* IJ Netw. Secur., vol. 18, no. 1, pp. 124–132, 2016.

[5] K. Gaurav and U. Ghanekar, "*Image steganography based on Canny edge detection, dilation operator and hybrid coding,"* Journal of Information Security and Applications, vol. 41. pp. 41– 51, 2018.

[6] R.Atta and M. Ghanbari*, "A high payload steganography mechanism based on wavelet packet transformation and neutrosophic set," J. Vis. Commun. Image Represent.*, vol. 53, pp. 42–54, 2018.

[7] P. Maniriho and T. Ahmad, "*Enhancing the Capability of Data Hiding Method Based on Reduced Difference Expansion.,"* Eng. Lett., vol. 26, no. 1, 2018.

[8] W. Elmasry, "*New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check*," Sādhanā, vol. 43, no. 5,pp. 1–14, 2018.

[9] T. Singh, S. Chopra, H. Kaur, and A. Kaur*, "Image compression using wavelet and wavelet packet transformation,"* IJCST, vol. 1, no. 1, 2010.

[10] T. G. Shirsat and V. K. Bairagi, *"Lossless medical image compression by integer wavelet and predictive coding," ISRN Biomed. Eng.*, vol. 2013, 2013.

[11] G. Kumar and P. K. Bhatia*, "A detailed review of feature extraction in image processing systems,"* in 2014 Fourth international conference on advanced computing & communication technologies, pp. 5–12, 2014.

[12] C. S. Prakash, H. Om, S. Maheshkar, and V. Maheshkar, *"Keypoint-based passive method for image manipulation detection,"* Cogent Eng., vol. 5, no. 1, p. 1523346, 2018.

[13] O. Bailo, F. Rameau, K. Joo, J. Park, O. Bogdan, and I. S. Kweon, *"Efficient adaptive non-maximal suppression algorithms for homogeneous spatial keypoint distribution," Pattern Recognit. Lett.*, vol. 106, pp. 53–60, 2018.

[14] R. Szeliski, *Computer vision: algorithms and applications*. Springer Science & Business Media, 2010.

[15] Y. Inan, "*Assesment of the Image Distortion in Using Various Bit Lengths of Steganographic LSB,"* in ITM Web of Conferences, 2018, vol. 22, p. 1026.

[16] G. Maji, S. Mandal, S. Sen, and N. C. Debnath, "*Dual image based LSB steganography,"* in 2018 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom), 2018, pp. 61–66.

17] A. ALabaichi, M. A. A. Al-Dabbas, and A. Salih*, "Image steganography using least significant bit and secret map techniques.," Int. J. Electr. Comput. Eng.*, vol. 10, 2020.

[18] S. A. Seyyedi and N. N. Ivanov, "*High payload and secure steganography method based on block partitioning and integer wavelet transform*," 2014.

[19] R. Tavoli, M. Bakhshi, and F. Salehian, *"A New Method for Text Hiding in the Image by Using LSB," Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 4, pp. 126–132, 2016.

[20] S. Mangayarkarasi and P. Sujatha, *"A Steganographic Method for Digital Images Using Harris Method,"* Int. J. Pure Appl. Math., vol. 114, no. 12, pp. 267–276, 2017.