Review Study among Traditional LSB, Proposed Modified LSB and DWT Steganography Algorithm

Soukaena H. Hashem,Ph.D,(Asst.Prof.)* Eman Taleb Zghaer*

Abstract

The art of steganography is to hiding the secret information inside other information. There are four steganography Medias (video, audio, text and image) which have different containers. The digital image is one of the most popular kind uses in the internet. This paper a comparison among traditional Least Significant Bit (LSB), proposed modified LSB and Discrete Wavelet Transform (DWT) techniques of steganography are made using the MSE and Peak-SNR measures. Also the capacity between cover image and secret message is play effective way to achieve good quality, that will gives good way to choose best cover that is suitable to hide the specific secret message (Text), thereby achieve good result of MSE and PSNR. The experimental work taken different image formats with different size and use different size of secret message. The obtained results show that; the proposed modified LSB is the best in both basic measures MSE and PSNR, where the traditional LSB is the best in measure of capacity and the DWT is the best in measure of security.

Keywords: Steganography, Digital Image, LSB, DWT, Spatial domain and Frequency domain.

***University of Technology**

1. Introduction

In communication this day people are sharing information between them by using the internet communication. In this time the malicious parties try to eavesdropping on the confidential information [1]. The security of the information is increasing during to the rapid development in the techniques of the internet telecommunication. The research in the field of information hiding is increasing during to the application of copyright, protection, secret communication, etc. The steganography and cryptography are the major fields which work on the security and hiding information [2]. Steganography is a science to hide data which cover text, image, audio, video and many other [3] . The main reason of using steganography is to protect the information data from the hackers [4] . In this paper a steganography method to hide a secret message in a cover image was proposed. This method is depending on embedding secret message bits by using two method (LSB and modified LSB) and selected best method between them. The DWT approach applied in the proposed work to compare with LSB in terms of security and quality.

The rest of this paper is organized as: section 2 describes the related work, section 3, describes the proposed method. While section 4, illustrates the experimental results, section 5, and describes the conclusions. Finally the future work is in section6.

2. Steganography

Steganography is the art of hiding a file, message, image, or video within another file, message, image, or video. The word steganography combines the words steganos meaning "covered, concealed, or protected", and graphein meaning "writing". It is a way of hiding message or secret data into image which cannot be detected by Human Visual System (HVS) [5] . The main motive of steganography is to keep the data safe from the notice of hackers. There are two fundamental characteristics which must be used in Image steganography, these are: Quality of an image and Security of image [4].

3- Methods of Steganography

Steganography methods can be classified mainly into categories,

3.1 Substitution method (LSB)

Substitution method where the secret message can be substituted by the redundant parts of the cover (spatial domain) [6] . The substituted of the least significant bit (LSB) is an example of the techniques of spatial domain. The idea of the LSB is to direct replacement of unused or noisy bits of the cover with the bits of secret message. The technique of LSB is the most preferred method till now used for hiding data due to its simplicity to implementation, which offers a higher capacity of hiding and to provide an easy way to obtain on a higher quality of stego-image control, but it has a lower response to modification for the stego-image, as low imperceptibility and low compression and filtering [7]. In Traditional LSB the bits of secret message is embedded in the first position of red, green and blue. So every pixel it uses to embed three bits of secret message. Figure (1) explains the traditional LSB in details.

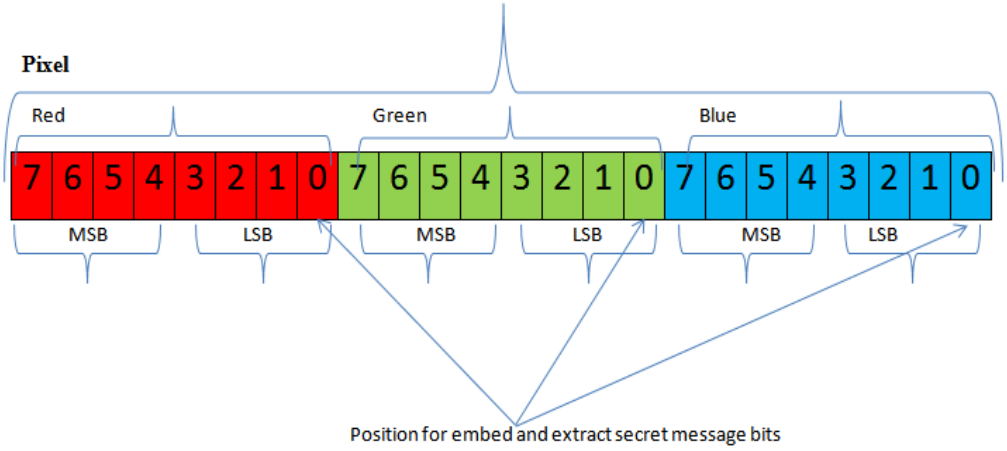


Figure (1): Explains the spatial operation for LSB

3.2 Transform method (DWT)

The techniques of transform domain embed the secret information in the transform space of the frequency domain [6], where the techniques of transform domain to overcome the imperceptibility and robustness problems which found in the techniques of LSB substitution. There are many transformations that could be used to hiding data, and the following techniques of transforms were the most widely used these are; discrete cosine transforms (DCT), discrete wavelet transforms (DWT), discrete Fourier transforms (DFT) [7]. Best technique of them was DWT techniques. Because the wavelet coefficient separates the low and high frequency information in the basis of the pixel to pixel .The approach of DWT was used by the “Haar DWT”, where it was the simplest approach of the wavelet transform. Time the domain in the DWT approach was passed across low- pass and high- pass filters and the low and high frequency coefficient of wavelet which generating by using the difference values and amended of the two values of pixel consecutive. The Haar DWT operate on the result of the cover image in the formation of four sub-bands, namely the horizontal band (HL), approximate band (LL), diagonal band (HH), and the vertical band (LH) . The approximate band was contained the most important information of the spatial domain image but the other bands were contained the higher frequency information such as edge details see figure (2) and figure (3) [7].

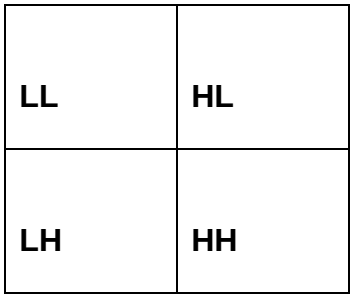


Figure (2): Sub bands formed after applying Haar DWT [8]

Original Image **DWT representation**

Figure (3):shows the 4 sub-bands that are formed after applying 1-level Haar DWT on a 2-dimensional image [8].

4. Related work

Some of related works are listed below;

1. Manjula1 G.R., et al.in 2015 [9], present a method to embeds a secret (color image) into a cover (color image). A 2-3-3 LSB insertion method has been used for image steganography.

2. Mazumder J.A. et al., in 2014 [12],
present a high security steganographic technique using DWT and optimized message dispersing method. Here has been used Haar wavelet transformation which decomposes the cover image into high frequency and low frequency information and high frequency information contains information about the edges, corners etc. of the image where secret information have been dispersed. The high frequency of RGB color components it uses to hide secret message. Depending upon the length of the secret message this algorithm start from the last column of each and top to bottom of the RGB components.To measure the imperceptibility of the proposed steganography method we have used MSE and PSNR. Have been taken for these experiment four images formats: PNG, BMP, JPEG and TIFF have been taken and the secret message of sizes starting

from 2 KB to 20 KB has been inserted and evaluated their corresponding MSE and PSNR using standard method. Besides the analysis of MSE and PSNR the message insertion and the message extraction time has been evaluation. The experimental result shows that the MSE and Capacity are improved with acceptable PSNR compared to other methods.

3. Gupta H. et al., in 2013 [10], offered two techniques in image steganography (image domain, transform domain). For image demain when employ LSB algorithm this lead to minimize the MSE values and making the PSNR values greater when the amount of bits substitution large.

4. Arora S.et al., in 2013 [11] in this paper new method is applied in image steanography for color image by using edge detection. In this proposed work, the secret message (text) hide in the edge of the color image after detect edge of an color image by make scanning work in window of size 3*3.

5. Ghasemi E. et al., in 2011 [3], offered the application of frequency domain (discrete Wavelet Transform) and artificial intelligent algorithm (Genetic Algorithm).the cover image segmentation in 4*4 blocks by using (DWT) and the genetic algorithm based in mapping function is applied to hide secret message in DWT coefficients. After hide the secret message the best pixel adjustment is utilized. For high robustness frequency domain was applied and, Genetic Algorithm and best Pixel Adjustment was applied for best mapping function this lead to reduce the MSE between the cover-image and the stego-image.

5. Proposed Work

In this current research work; some techniques in spatial domains and transform domains will be taken in consideration; these are,see figure (4):

1. Traditional LSB
2. Proposed modified LSB (LSB (RGB))
3. Discrete Wavelet Transform

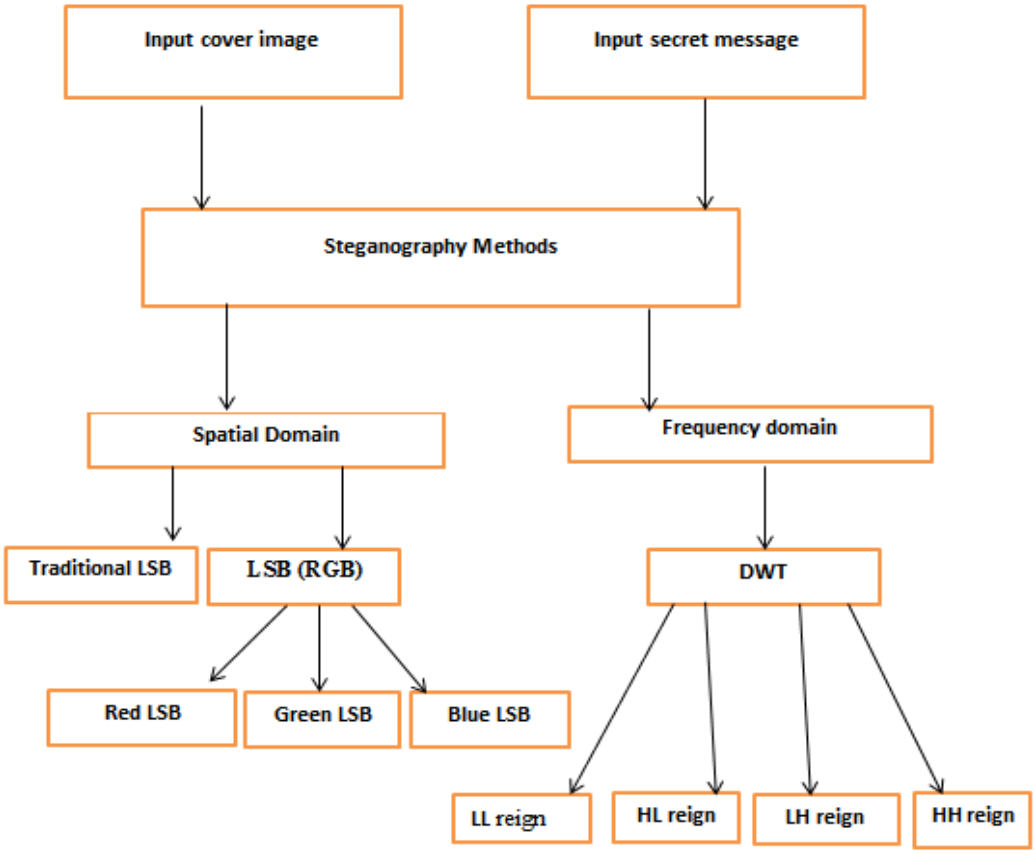


Figure (4) : General block diagram for the Review Study amongTraditional LSB, Proposed Modified LSB and DWT Steganography Algorithms.

5.1 Spatial LSB (Proposed)

In spatial domain will show two techniques; **Traditional LSB** and proposed modified LSB which is termed **LSB (RGB)**.

In LSB (RGB), the bits of secret message is embedded is only in blue or green or red part. In red LSB will take red part and convert to binary and show the first bit and decide:

To embed secret message bits:

If red (0) =0 Then

Red (1) = secret message bit

Else

Red (2) = secret message bit.

To extract secret message bits:

If red (0) =0 then

Secret message= red (1),

Else

Secret message= red (2).

Example (1), Figure (5 (a and b)), algorithm (1) explain the modified LSB in details.The Green LSB and Blue LSB is the same the context of action Red LSB.

Example (1): Simple example of proposed modified LSB

Suppose secret message =01100001

Cover = 01110010, 11000101, 00110111, 00010111, 01001101, 00110011, 00101110, 01000011.

For embedding:

01110010 ⟶ 01110010

11000101 ⟶ 11000001

00110111 ⟶ 00110011

00010111 ⟶ 00010011

01001101 ⟶ 01001001

00110011 ⟶ 00110111

00101110 ⟶ 00101110

01000011 ⟶ 01000011

Stego = 01110010, 11000001, 00110011, 00010011, 01001001, 00110111, 00101110, 01000011

For extraction:

01110010 ⟶ 1

11000001 ⟶ 0

00110011 ⟶ 0

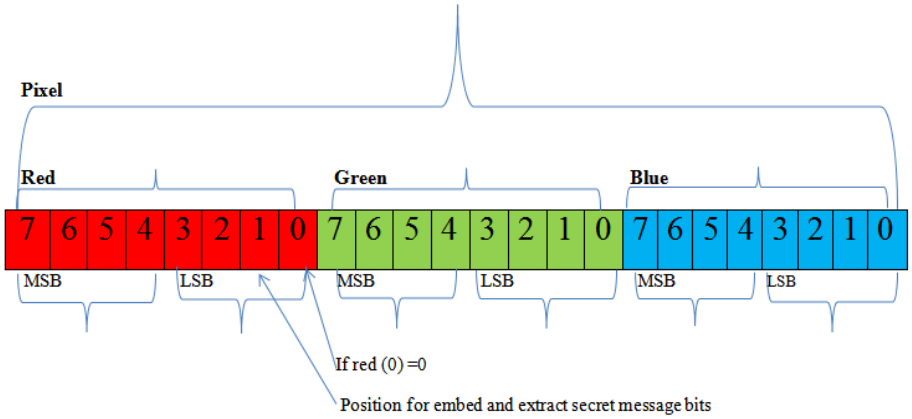
00010011 ⟶ 0

01001001 ⟶ 0

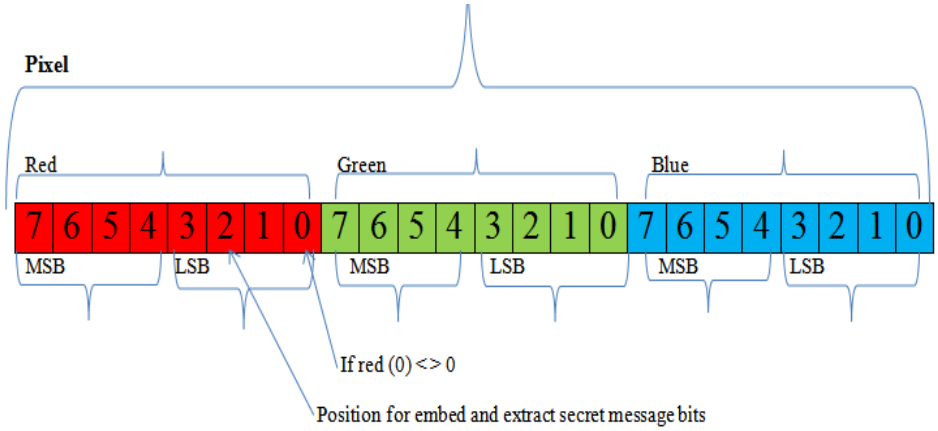
00110111 ⟶ 1

00101110 ⟶ 1

01000011 ⟶ 0
Secret message= 01100001



(a)



(b)

Figure (5(a, b)): LSB (RGB) embedding and extraction algorithm for RED channel

Algorithm (1): Proposed LSB (RGB) Steganography

1- Embedding Algorithm

Input: Secret Message to be embedded, Cover Image.

Output: Stego_image.

Step1: Read Secret Message to be hidden and Cover image.

Step2: Find ASCII for each character of secret message.

Step3: Convert ASCII into binary.

Step4: Convert the channel that is used to embed secret message into binary.

Step5: Check first position from channel that is used to embed secret message if equal zero embed secret message bits in second position otherwise embed secret message bits in third position.

Step6: End

2- Extraction algorithm

Input: Stego_image.

Output: Secret Message

Step1: Read stego_image

Step2: Convert the channel that is used to embed secret message into binary.

Step3: Check first position from channel that is used to extract secret message bits if equal zero extract secret message bits from second position otherwise extract secret message bits from third position.

Step4: End

5.2 DWT Proposed Work

In this work, several experiments will work on the regions, LL, HL, LH, HH with traditional LSB use for hiding information. This work will use images size equal to 512*512. The result is choosing the best region in terms of security and the best result of MSE and P-SNR.algorithm (2) ,Figure (6), explain hiding with DWT.

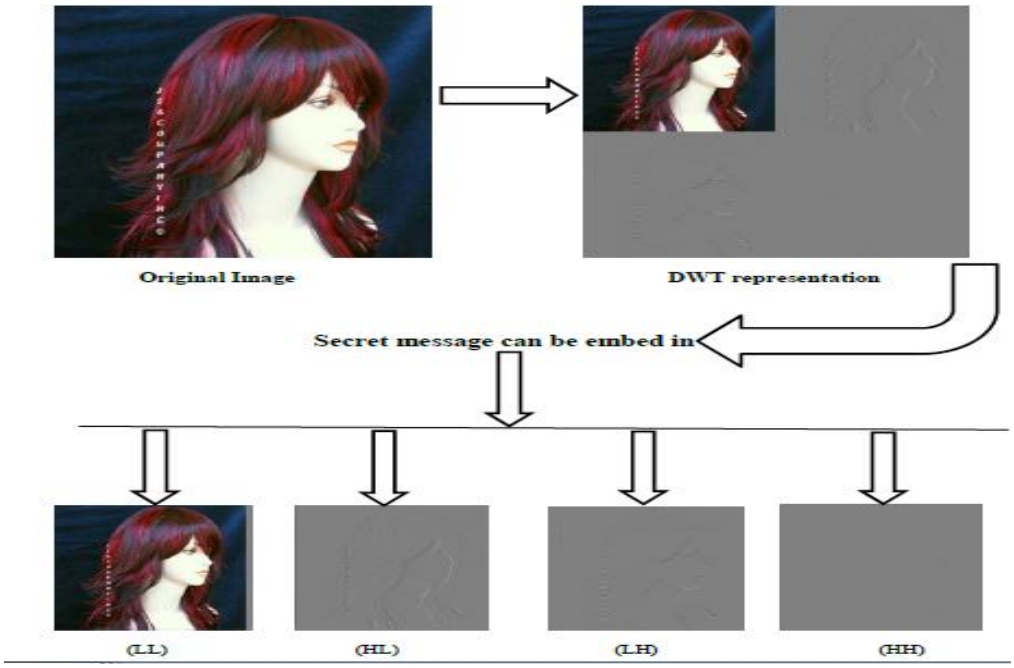


Figure (6): Steganography with DWT

Algorithm (2): DWT Steganography

1- Embedding Algorithm

Input: Secret Message to be embedded, Cover Image.

Output: Stego_image.

Step1: Read Secret Message to be hidden and Cover image.
Step2: Find ASCII for each character of secret message.
Step3: Convert ASCII into binary.
Step4: Stratify 2D-HaarDWT to the cover image, and the result will be four sub-bands (lowlow (ll)- high low (lh)- low high (hl) high high (hh)).
Step5: Convert the band that is used to embed secret message into binary.
Step6: Embed the Secret message only in LL or HL or LH or HH by using traditional LSB.

Step7: ApplyInverse Discrete Wavelet Transformation (IDWT).
Step8: End.

2- Extraction algorithm

The same sequence of steps in embedding algorithm performed with some changes in step 6 perform extraction process rather than embed , step 7 not necessary to implement, finally the process is continued until all secret message is extracted entirely from the cover.

6- Evaluation Parameters

There are two attributes are used to measure steganography techniques, imperceptibility and capacity [9].

6.1 Imperceptibility Stego-image quality

To calculate the imperceptibility of steganography two metrics are used. This metrics indicates how similar (or different) the cover image compared with stego _image [12].This metrics are: PSNR (peak signal to noise ratio) and MSE (mean square error) are calculated for all the standard images. [11].

Mean squared Error (MSE) is one of the important measurements that commonly used to measure the quality and quantity of errors between the original image and the stego image. Small value of MSE means best result (good quality) for stego_image [12].

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(f(i,j) - f'(i,j))^2 \qquad \textbf{Eq1}$$

Where f (i, j) is the original image and f' (i, j) is the stego-image, M and N is dimensions of image.

Peak Signal-to-Noise Ratio (PSNR) is used to calculate quality between original image and stego-image.[12].

PSNR= 10. Log $((255)^2$/MSE) **Eq. 2**

6.2 Payload /Hiding Capacity

The other important type for steganography is a capacity, is a cofactor to achieve good quality. There is a relationship between digital cover and secret message depending on the capacity, if a few cover capacity and large capacity secret message the result is great distortion and poor quality, and if a large cover capacity and little capacity secret message the

result is little distortion and best quality. In proposed work will determine the number of byte for cover image and secret message and select cover appropriate to hide secret message. The following figure (7) explains it in details.

Capacity of cover image in byte:

Number of pixel = M*N

Number of byte= Number of pixel * 3

Secret message in byte:

Convert secret message into binary bit

Secret message in byte=number of secret message

Determine Number of bytes required to hide secret message bits: (Traditional LSB)

1-Number of pixel =M*N

2-Number of byte (cover) = Number of pixel * 3

3-Convert secret message into binary bit

4-Secret message in byte=number of secret message in bit/8

5-Number of byte (cover) > Number of secret message in byte

6-Number of byte required to hide secret message bits= Number of secret message in bit

7-Number of pixel required to hide secret message bits= Number of secret message in bit/3

Determine Number of bytes required to hide secret message bits: (RGB)

1- Number of pixel=M*N
2- Number of byte= Number of pixel * 3
3- Convert secret message to binary bit
4- Secret message in byte=number of secret message in bit / 8
5- Number of byte (cover)> Number of secret message in byte
6- Number of pixel required to hide secret message bits >= Number of secret message in bit

Figure (7): Explains capacity calculation

7- Experimental Result

In image steganography there are many methods used to hide secret data in image. In this paper a comparison among traditional Least Significant Bit (LSB), proposed modified LSB and Discrete Wavelet Transform (DWT) techniques of steganography are made using the MSE and Peak-SNR measures. In the result shown in table (1) LSB (RGB) is giving best result in every time. In LSB (RGB) gives similar results with some varying little in result. The result of LSB (RGB) is depending on cover image selected and measure of how much red, green and blue color in the image. In the result shown in table (2) DWT based hiding methods all sub-bands gives similar results with some varying little in result. In the result shown in table (3) and table (4) capacity in traditional LSB provide high capacity because every pixel use to hide three bits of secret message ,where LSB(RGB) require capacity higher than traditional LSB because every pixel require to hide one bit of secret message (hide in red or green or blue). To solve this problem of capacity a larger images must be used to hide secret message.

Table (1) comparison between different techniques of spatial domain

				LSB(RGB)					
Image size	Message size	LSB	LSB	Red LSB	Red LSB	GreenLSB	GreenLSB	Blue LSB	Blue LSB
		MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
225*255	61 bytes	0.0090	68.5657	0.0049	71.1950	0.0053	70.8287	0.0048	71.2651
512*512	717 bytes	0.0214	67.7688	0.0108	677922	0.0053	67.7729	0.0109	68.7205
600*399	717 bytes	0.0066	69.8808	0.01192	67.3659	0.01197	67.7799	0.0120	67.3085
600*450	193 bytes	0.0018	75.5159	0.0008	76.5964	0.0028	73.6305	0.0031	78.3597
640*640	98 bytes	0.0018	75.3501	0.0009	78.2555	0.0028	78.3997	0.0009	79.2884
612*612	451 bytes	0.0094	68.3757	0.0047	71.3591	0.0048	71.2342	0.0047	71.4033
108*108	79 bytes	0.050	61.0614	0.2753	63.7477	0.0265	63.8856	0.0275	63.7342
168*168	421 bytes	0.1206	57.3145	0.0574	60.5391	0.2582	60.3606	0.0584	60.4674

Table(2) Comparison between LL, LH, HL, HH

Image size	Message size	LL	LL	HL	HL	LH	LH	HH	HH
		MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
512*512	61 bytes	0.0069	69.7346	0.0055	70.6845	0.00692	69.7250	0.0055	70.6845
512*512	98 bytes	0.0113	67.7346	0.0092	68.4708	0.01091	67.7525	0.0092	68.4708
512*512	193 bytes	0.0240	64.3117	0.0219	64.7119	0.0235	64.4063	0.0239	64.3310
512*512	717 bytes	0.0847	58.8503	0.088355	58.9109	0.0848	58.8432	0.0843	58.8675

Table (3) Capacity in traditional LSB

Cover	Number of pixel	Number of byte (cover)	Number of bit (secret Message)	Number of byte required to hide secret message bits	Number of pixel required to hide secret message bits
Cover 1	225*225 50625	151875	1544	1544	515
Cover 2	640*640 409600	1228800	3368	3368	1123
Cover 3	512*512 262144	786432	5736	5736	1912

Table (4) capacity in LSB (RGB**)**

Cover	Number of pixel	Number of byte (cover)	Number of bit (secret Message)	Number of pixel required to hide secret message bits
Cover 1	225*225 50625	151875	1544	1544
Cover 2	640*640 409600	1228800	3368	3368
Cover 3	512*512 262144	786432	5736	5736

Table (5) comparing steganography with DWT and steganography by using Traditional LSB

		DWT		LSB	
Image size	Message size	MSE	PSNR	MSE	PSNR
512*512	61 bytes	0.0069	69.7346	0.0019	75.1812
512*512	98 bytes	0.0113	67.7346	0.00354	72.6360
512*512	193 bytes	0.0240	64.3117	0.0059	70.3627

8.Conclusions

Some of conclusions are reached in this work, these are as follow;

1. The most important factors of steganography quality are MSE and PSNR; the modified LSB (RGB) score higher results than LSB algorithms. Table (1) explains the results.
2. DWT based hiding methods it have been concluded all sub-bands gives similar results with some varying little in result. Table (2) explains the results.
3. The critical factor in steganography is capacity; traditional LSB has higher capacity than modified LSB (RGB) that since the traditional hide in all the bytes of pixel, where the modified hide in one byte for each pixel. Table (3) and table (4) explains the results.
4. By comparing steganography with DWT and steganography by using traditional LSB method will note the results of the MSE and PSNR in traditional LSB is higher from DWT but the security in DWT is much higher than LSB. Table (5) explains the results.

9- Future work

1- Use modified LSB (RGB) with DWT
2- Use some artificial intelligent algorithms with modified LSB (RGB) to increase security.

References

1-Martin D, and Barmawi A. M: **"List Steganography Based on Syllable Patterns",** Electrical Engineering and Informatics (ICEEI), 10-11 Aug. 2015.

2- Manjula R.G and AjitDanti: "**A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography In Spatial Domain",** International Journal of Security, Privacy and Trust Management (IJSPTM), Vol 4, No 1, February 2015.

3- Ghasemi E, Shanbehzadeh J, and Fassihi N: **"High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm",** Proceedings of the International Multi Conference of Engineers and Computer Scientists 2011, Vol. I, IMECS March 2011.

4- Kaur N**," Steganography Using Particle Swarm Optimization-A Review",** INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, Kaur, 2(11): November, 2013.

5-Kaul N, and Chandra M: "**A Proposed Algorithm for Text in Image Steganography based on Character Pairing and Positioning",** International Journal of ComputerApplications (0975 – 8887) Volume 126 – No.3, September 2015.

6-Sumathi C.P, Santanam T, Umamaheswar G:" **A Study of Various Steganographic Techniques Used for Information Hiding"** International Journal of Computer Science &Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

7-Jamdar J. S, Shah A. V, Gavali D. D and Kurkute S. L.:" **Edge Adaptive Steganography Using DWT"** International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4,

April 2013.

8- Verma A, Nolkha R, Singh A and Jaiswal G," **Implementation of Image Steganography Using 2-Level DWT Technique**", International Journal of Computer Science and BusinessInformatics, ISSN: 1694-2108 | Vol. 1, No. 1. MAY 2013.

9- Manjula G.R, and AjitDanti, " **A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography In Spatial Domain",** International Journal of Security, Privacy and TrustManagement (IJSPTM) Vol 4, No 1, February 2015.

10- Gupta H, Kumar R, Changlani S,"**Steganography using LSB bit Substitution for data Hiding"**, International Journal of Advanced Research in Computer Science and ElectronicsEngineering (IJARCSEE) Volume 2, Issue 10, October 2013.

11. Arora S, Anand S," **A New Approach for Image Steganography using Edge Detection Method",** International Journal of Innovative Research in Computer and CommunicationEngineering *Vol. 1, Issue 3, May 2013.*

12.Mazumder J.A, Hemachandran K," **Color Image Steganography Using Discrete Wavelet Transformation and Optimized Message Distribution Method"**International Journal ofComputer Sciences and Engineering, Volume-2, Issue-7, 2014.

مراجعة دراسة بين الطرق التقليدية والمقترحة وطريقة DWTمن خوارزميات الاخفاء

أ. م. د سكينة حسن هاشم* ايمان طالب زغير*

المستخلص

اخفاء المعلومات هو فن اخفاء المعلومات السرية داخل معلومات اخرى .توجد انواع مختلفة من تقنيات الاخفاء اهمها (الفيديو , النص , الصوت و الصور وغيرها) . اهم الانواع و الاكثر استخداما في الاخفاء هي الصور الرقمية. بهذا البحث تمت مقارنة بين خوارزميات الاخفاء المختلفة وتم اختيار افضل خوارزمية بالاعتماد على نتائج الجودة حسب مقاييس الخاصه بحاسب الجودة بين الصوره الاصلية(الغطاء)والصوره التي تحتوي على المعلومات السرية. حساب سعة الغطاء هذا يساعد على اختيار غطاء ذو حجم مناسب لحجم الرسالة السرية وذلك لتحقيق جودة عالية وتجنب للتشويش الذي قد يحصل للصورة اذتم استخدام غطاء ذو حجم صغير مقارنةً بالرساله السرية ويؤدي الى سهولة الكشف من قبل المهاجمين. استخدمت صور ورسائل سرية ذو انواع واحجام مختلفة. النتائج المستحصلة وضحت ان الطريقةLSBالمحورة المقترحة هي الأفضل من حيث المقاييس الأساسية MSE,PSNR. بينما ال LSBالتقليدية هي الافضل من ناحية السعة الخزنية وDWTهي الافضل من ناحية الأمن وصعوبة الكشف من قبل المهاجمين.

*الجامعة التكنولوجية