A High Capacity Embedding Scheme Based on Graph Theory Randomness and Bit Difference for Covert Communication

Ahmed Kamel Abbas[1] and Ahmed Toman Thahab[2]

[1]Department of Electronic and Electrical Engineering, University of Kerbala, Kerbala Iraq
[2]Department of Biomedical Engineering University of Babylon, Babylon, Iraq
ahmkam@yahoo.com, toeahmed@gmail.com

Abstract: Stenographic techniques are hiding methods that are used in secret communications to transmit secret data inside a carrier media. In this paper, a new image steganography technique based on graph theory and bit difference is proposed. Secret image is divided into blocks and randomized based on graph theory. The cover image is divided into four blocks and each secret image pixel is grouped into four two-bit groups and concealed inside the cover media. The embedding algorithm is based on a modified version of bit difference which is considered more secure. The proposed method is applied in the spatial and transform domain using Integer wavelet transform (IWT) since, IWT is less distortional in retrieving images compared to the discrete wavelet transform (DWT). Performance analysis of the proposed scheme is tested using peak signal to noise ratio (PSNR) and embedding capacity using various cover image formats such as (TIFF, PNG, BMP, and JPEG). Results show that the proposed scheme is superior over several embedding schemes in terms of capacity and visual symmetry.

Keywords: Bit differencing, Embedding Capacity, Image Format, PSNR, Graph theory.

1. Introduction

Over the past years, data transmission over the globe has been at a phenomenal rate [1]. Meanwhile, the advanced forgery tools and the corruption of data introduced by intruders impose that transmitted data security against unauthorized intruders is a priority and essential in the world of digital transmission [2]. Cryptography is a widely used mechanism for information encryption where data is scrambled in a form that becomes ambiguous to eavesdroppers. However, encrypted data appeals intruder’s attention and exposes data to potential attack. Data hiding is a process used to conceal confidential data to an extent that the presence of data existence is undetected. According to information hiding, data hiding is classified into two major categories; watermarking and steganography [2]. Both categories are related to each other in terms of concealing confidential data but both rely on different intents. Watermarking conceals small secret payloads such as small images, messages, and secret company logos for intellectual property of the author [3]. In contrast, steganography conceals the fact that secret message exist in the transmitted data with large embedding payloads [4]. Essentially, any stenographic method consists of three major components: The cover file where secret information is concealed; the secret data and the stego-output houses the secret information. Image steganography can be further classified into spatial domain embedding and frequency domain embedding. Spatial domain embedding means embedding the secret information by altering the pixel intensity of the cover image, however, it is considered simple and low complexity. Frequency domain embedding is transforming the image, using a signal transform, to a more suitable form for embedding, however embedding in the frequency domain is computational exhaust and secret information is not exactly retrieved at the receiver side [4].

Steganography has become under the scope of researchers for the last decade and it is considered as a viable research area since the communication of multimedia content is through social media and implemented with low cost devices [4]. A widely used pioneering embedding technique known as the least significant technique (LSB) embeds secret data in the spatial

Received: November 26th, 2018. Accepted: November 26th, 2019
DOI: 10.15676/ijeei.2019.11.4.11

domain. This technique replaces the bits of the immediate right code-word and replaces them with the most significant bits of the secret binary data. Authors [5], proposed an embedding method using bit differencing. The method determines the difference between two bits namely no.5 and no. 6 to hide secret message. If the difference result is not equal to the confidential information bit, the bit no. 5 is transverse. A peak signal to noise ratio (PSNR) of 51.1803 and payload of 262144 bits was achieved. The main disadvantages of method in [5] are security fragile and low capacity. LSB techniques are improved by combining other techniques such as encryption and source coding. Authors in [6] encoded the secret data using huffman encoding method and embedding in the cover image using the standard LSB method. Although the technique achieved a high visual quality with an embedding capacity of quarter the size of the cover image, the processing time required by the scheme is high. Authors in [7], proposed a bit inversion method to improve the PSNR of the stego image. After LSB steganography, some least significant bits of a cover image are inverted. The method also randomizes the selection of cover image pixel using Ron Code (RC4) in order to enhance security.

Frequency domain embedding [8] uses powerful transforms such as discrete cosine transform (DCT) and discrete wavelet transform (DWT) since these transforms localize frequency domain bands for cover media to embed secret data resulting a stego-output less noticeable to the Human visual system (HVS)[9]. However, wavelet transform is considered in image steganography than other transforms, numerous researches have been based on discrete wavelet transform (DWT). [10] Proposed a steganography algorithm to embed secret data using DWT. A haar type DWT is applied on secret and cover image. The algorithm also finds a similar match between cover block and message block. The method presents high security features and good visual symmetry between the cover and stego image but the search for similar match between blocks is considered computational exhaust.

Authors in [11] proposed a steganography technique using encryption and signal transform. A cover image is divided into four frequency bands using DWT. A threshold calculation based on image statistics is applied to exploit redundancy in the cover image. The secret message is divided into sub arrays and encrypted using RC4 algorithm. The embedding process implies a simple replacement of DWT coefficients of the encrypted secret message in the previously specified DWT of the cover image. Drawback of this method is hard ware resources requirements such as memory and processor speed.

Authors in [12] used an integer wavelet transform to hide secret data inside an image cover using graph theory technique. Secret data is embedded in a random manner in order to increase security. The method uses three different keys, the first key is to select the sub-bands of the wavelet transform and the second key is to select the coefficients and the third key is to determine the bit length. The maximum average PSNR is 50.627dB for a payload of 147456 bits. While an average PSNR of 33.874dB for a payload of 589824 bits. The secret data is a simple row data embedded using a formula of LSB. LSB is considered as a fragile security algorithm for embedding secret data. In addition the paper and most research literature does not investigate the image cover formats of embedding.

This paper proposes a steganography technique which is a combination of modified version of bit differencing and graph theory based randomness. Instead of utilizing the graph theory on the sub bands and number of bits as in [12], the proposed method applies randomness based on graph theory on the secret image blocks. This procedure allows the secret image data to be more secure if hackers are suspicious of secret data embedding. Moreover embedding using bit difference is more robust to mild compression ratios than LSB since it depends on the sixth and fifth bits not the immediate right bit of the secret pixel. Cover images of various formats are not investigated in most steganography literature papers. This paper will also investigate various image cover formats.

The rest of the paper organized as follows: Section two explains the bit differencing technique. Section three presents the randomness generated by graph theory. Section four explains the hiding and recovery phases. Section five gives the results of some tests for the proposed steganography algorithm and comparison with the related algorithms. Finally, section six concludes the entire paper.

2. Bit Difference Technique

The pioneering technique in steganography is LSB [13], [14]. An 8-bit binary value vector $[b_1\ b_2 \ldots b_8]$ represents a value in decimal in the range of 0-255[15]. The bits b_5,b_6, b_7,b_8 are considered as least significant bits, while bits b_1,b_2,b_3,b_4 are considered as most significant bits. If a value of $[s_1, s_2]$ is embedded in the least significant bits, the value will alter to a value with less error than embedding in the most significant bit (MSB) as shown in example below:
Let x= $[11011001]_2$ is a 8-bit binary value. If a secret data of $[10]_2$ is concealed in [x] in LSB bits, the output S= $[11011010]_2$ which is a value of $(218)_{10}$ an error of $(218)_{10}$-$(217)_{10}$= 1 unit. If the secret data was to be embedded in the MSB, the output value S= $[10011001]_2$ which is a value of $(153)_{10}$ an error of $(217)_{10}$-$(153)_{10}$= 64 unit error. The drawbacks of this technique are its security compromise; LSB is considered as fragile technique. Since it embeds in the least significant bits, it cannot stand attacks such as compression attacks. LSB also embeds the secret bits through direct substitution. A more advanced version of the LSB is the "Bit difference technique". The technique does not embed secret data in the immediate-right of the cover pixel vector. The following steps are for one bit embedding using bit difference:

1. Find difference between b_i and $b_{i+1.}$
2. If : the difference between b_i and b_{i+1} is equal to the secret data,
   then do not change b_i , otherwise transverse $b_{i.}$

The Extraction operation is the inverse of the above operation:

1. Find the difference between b_i and $b_{i+1.}$
2. If : the difference between b_i and b_{i+1} is equal to b_i,
   then b_i the secret bit , otherwise the secret bit is the transverse of b_i .

Because embedding is in the b_i bit and undependable on direct substitution, the technique is more robust against compression attacks and more secure against hackers to intrude the data.

3. Graph Theory and Random Selection

A graph theory concept used in image processing fields especially in image segmentation and computer vision [16]. Graph G consists of a non-empty finite set V(G) of elements called vertices (or nodes), and a finite set E(G) of distinct unordered pairs of distinct elements of V(G) called edges[16]. In this paper, the pixels of image considered as vertices and connection between pixels is the edges of graph. The concept of graph can be exploited in steganography to change the order of secret image pixels randomly before embedding the data in the cover. At the receiver side the same algorithm must be applied to extract the secret data from cover image. The algorithm below shows the steps of create reversible random path between image pixels based on graph theory. The variable M defines the complexity level of randomness between pixels in cover image. If the M = 1 (level one encryption), the random path algorithm applied on image blocks only, if M = 2 (level two encryption) the same algorithm is applied in blocks and pixels in each block. The two level encryption is more secure, more complex, and take extra processing time compared to level one encryption.

- Encryption Algorithm:
  1. select cover image and isolate the RGB layers
  2. for each layer split the image into 8x8 blocks
  3. create the encryption mask (the mask dimensions equal to the block dimension) by following the steps below:
     - Let the size of mask is 8 x 8:
       - The number of pixel in block L = 64 = number of vertex.
       - The number of edges in block E = L – 1 = 63.
     - Select four random numbers (X, Y, N, n) Taking into consideration the following conditions:

- $X + Y = E$
- $N <= E / 2$
- $n <= \sqrt{E}$

- Generate S1 as: S1 = [1+N, ...,X+N]
  - Generate S2 as: S2 = [Ascending order of odd numbers in s1, descending order of even numbers in s1]
  - Generate S3 as S3 = $[N^{q}. N-1^{q}. N-2^{q}. \dots. 0^{q}]$, where Nq means repeated (N) q times, the q = Y / N and total number of elements in S3 must be equal to Y.
  - Generate R1 = [1 , 2 , ... , X+Y], R2 = [S2 , S3], R3 = R1+R2
  - Generate mask by taking the elements of R2 and R3 respectively without repeating. Label each connection starting from 1, the last connection must equal to E, that means the graph is completed and connected.

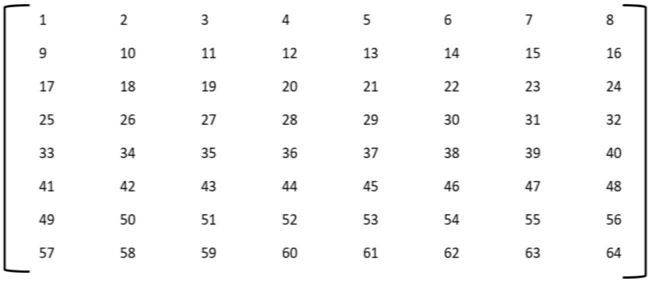
1. Apply the generated mask to every block of current layer in cover image.
2. Repeat the steps above for every layer of image.
3. The output is encrypted cover image.

To increase the randomness of encrypted cover image, which produced from above algorithm the following steps, can be applied:

- Transpose the encrypted cover image.
- switch between columns: R(: , I) & R(: , I + n)
- Switch between rows: R (I, :) & R (I + n, :)

The figure below show the Lena image before and after encryption by using the proposed algorithm in one level encryption and two level encryption.

For example, if a block index shown below is input, let X = 30, y = 33, N = 7, and n = 2



$$\text{Block Index} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 \\ 25 & 26 & 27 & 28 & 29 & 30 & 31 & 32 \\ 33 & 34 & 35 & 36 & 37 & 38 & 39 & 40 \\ 41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 \\ 49 & 50 & 51 & 52 & 53 & 54 & 55 & 56 \\ 57 & 58 & 59 & 60 & 61 & 62 & 63 & 64 \end{bmatrix}$$

S1 = [8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37]

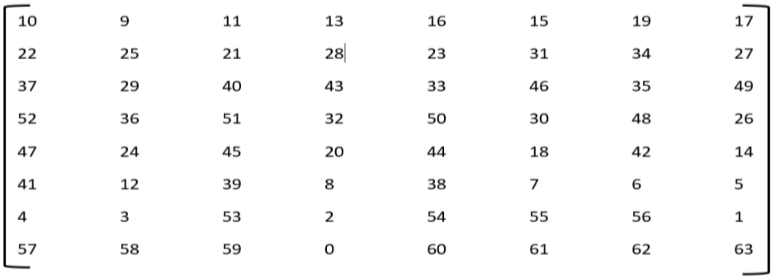
S2 = [9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 36, 34, 32, 30, 28, 26, 24, 22, 20, 18, 16, 14, 12, 10, 8]

S3 = [7, 7, 7, 7, 6, 6, 6, 6, 5, 5, 5, 5, 4, 4, 4, 4, 3, 3, 3, 3, 2, 2, 2, 2, 1, 1, 1, 1, 0, 0, 0, 0]

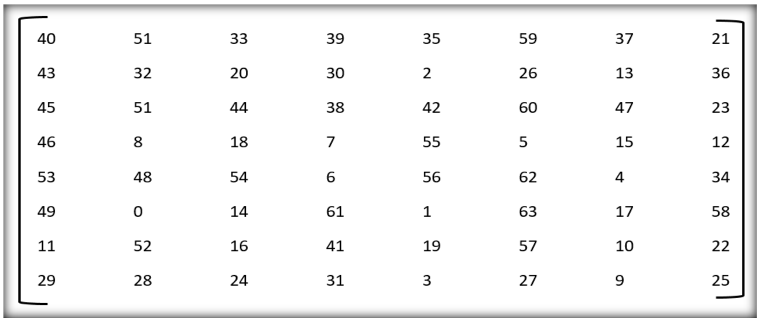
R1 = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

R2 = [9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 36, 34, 32, 30, 28, 26, 24, 22, 20, 18, 16, 14, 12, 10, 8,7, 7, 7, 7, 6, 6, 6, 6, 5, 5, 5, 5, 4, 4, 4, 4, 3, 3, 3, 3, 2, 2, 2, 2, 1, 1, 1, 1, 0, 0, 0, 0]

R3 = [10, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 52, 51, 50, 49, 48, 47, 46, 45, 44, 43, 42, 41, 40, 39, 38, 38, 39, 40, 41, 41, 42, 43, 44, 44, 45, 46, 47, 47, 48, 49, 50, 50, 51, 52, 53, 53, 54, 55, 56, 56, 57, 58, 59, 59, 60, 61, 62, 63].

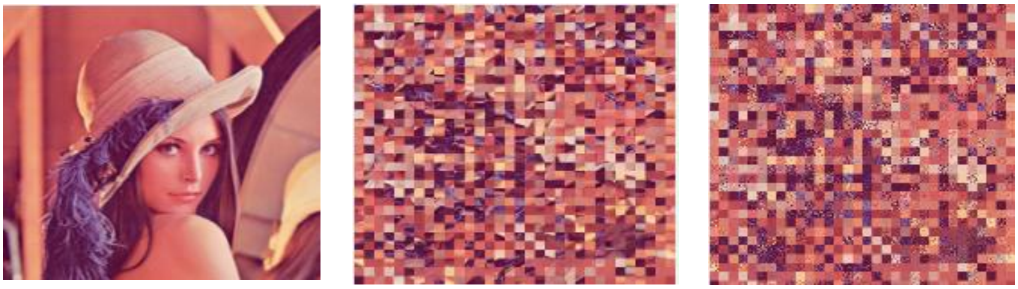


$$\text{Encrypted Block Index} = \begin{bmatrix} 10 & 9 & 11 & 13 & 16 & 15 & 19 & 17 \\ 22 & 25 & 21 & 28 & 23 & 31 & 34 & 27 \\ 37 & 29 & 40 & 43 & 33 & 46 & 35 & 49 \\ 52 & 36 & 51 & 32 & 50 & 30 & 48 & 26 \\ 47 & 24 & 45 & 20 & 44 & 18 & 42 & 14 \\ 41 & 12 & 39 & 8 & 38 & 7 & 6 & 5 \\ 4 & 3 & 53 & 2 & 54 & 55 & 56 & 1 \\ 57 & 58 & 59 & 0 & 60 & 61 & 62 & 63 \end{bmatrix}$$



$$\begin{array}{l}\text{Encrypted Block Index} \\ \text{after swapping between} \\ \text{pixels according to n}\end{array} = \begin{bmatrix} 40 & 51 & 33 & 39 & 35 & 59 & 37 & 21 \\ 43 & 32 & 20 & 30 & 2 & 26 & 13 & 36 \\ 45 & 51 & 44 & 38 & 42 & 60 & 47 & 23 \\ 46 & 8 & 18 & 7 & 55 & 5 & 15 & 12 \\ 53 & 48 & 54 & 6 & 56 & 62 & 4 & 34 \\ 49 & 0 & 14 & 61 & 1 & 63 & 17 & 58 \\ 11 & 52 & 16 & 41 & 19 & 57 & 10 & 22 \\ 29 & 28 & 24 & 31 & 3 & 27 & 9 & 25 \end{bmatrix}$$

If an input image is input to the algorithm, there will be two randomness of blocks; simple and complex:



Cover image

Simple randomness

Complex randomness

Figure 1. Cover and random block images

The algorithm in the receiver side needs the same values of X, Y, N, and n to decrypt the encrypted image.

4. Integer Wavelet Transform

Wavelets are zero average value functions over a finite interval. A function is superposed of set of basis functions or wavelets. Discrete wavelet transform (DWT) divides an input image to equal localized frequency bands with logarithmic scale [18]. Images in the DWT domain possess less detectable variations resulting in four frequency band matrices: low-low band (LL), low-high (LH), high-low band (HL), and high –high (HH) band. The LL band known as “the approximation band” harvests the highest pixel value and possesses the low frequency contents of the images [18]. The rest of the bands possess the contents of high frequency bands. A lifting scheme is utilized for integer wavelet transform resulting in an integer coefficient [17]. Equation.1 &2&3[19], [15] illustrates the process:

$$IN_j\ ({}_O),\ IN_j\ (e): \qquad (1)$$

$$d_{j-1} = IN_j\ (0) - floor\ (Pro\ \{IN_j\ (e)\}) \qquad (2)$$

$$A_{j-1} = IN_j\ (e) + floor\ (Upd\ \{IN_j\ (o)\}) \qquad (3)$$

Where, *IN:* is an input vector of pixels, (*IN (o)*) and (*IN(e)): are* odd and even pixels respectively, (*Pro*) and (*Upd*) are the prediction and update functions which are dependable on the wavelet filter type (eg. Haar, Daubechies2, Daubechies3), and *floor (y)* is an approximation function that determines the largest integer less or equal to the value y. Since detail and approximation coefficients resulting from the LWT are integers, the rounding error in the conventional DWT is eradicated which makes the hiding process using LWT less distortional.

5. Proposed Image Steganography

The present section explains the image steganography algorithm. As stated in section two, two types of random selection can be applied; simplex and complex. This must be stated in the algorithm at the transmitter and receiver side by choosing the type of randomness through randomness selection option. The embedding method is implemented in spatial domain and transform domain using bit differencing as an embedding process. The method requires that the size of the secret image is one half the cover images, both of the secret and cover are square image media. If the images are not square in dimension, they must be resized in a resize pre-embedding process.

A. Spatial Embedding: Embedding is in the spatial domain without using a transform.

The embedding process using bit differencing. Figure. (2) Shows the block diagram for the spatial domain embedding.

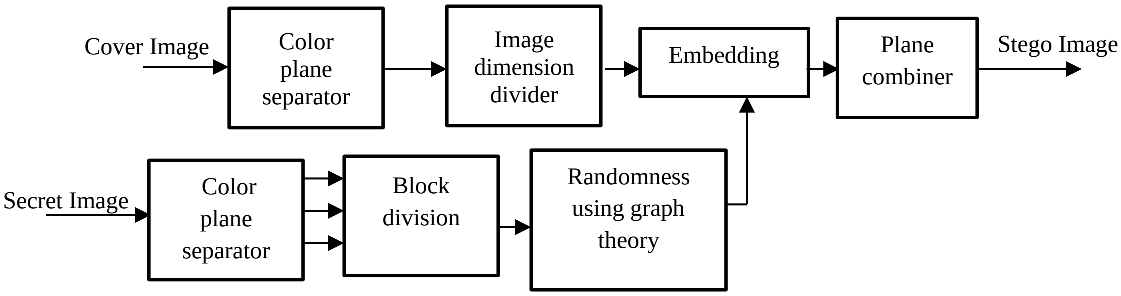


Figure. (2) Block diagram of spatial embedding image steganography.

The embedding process in spatial domain as follows:

1. Select the type of randomness; simplex or complex.
2. Read color cover, secret image and value of X, Y, N, n.
3. Separate the cover and secret image color planes according to their format.
4. Divide the cover image into four equal blocks.
5. Divide the secret image into 8*8 block size.
6. Apply graph theory randomness algorithm for randomizing the blocks of secret image.
7. Each secret pixel is converted to 8 bit binary value; each binary value pixel is divided into four two bit groups.
8. The Embedding is conducted row by row of the secret image and for each color plane: Find the difference between the 5th bit and 6th bit, if the difference is equal to the secret data, do not change the bit otherwise change the 6th bit.
9. Combine the color planes and produce the stego-image.

The extraction process in spatial domain as follows:

1. Read stego image and value of X, Y, N, n.
2. Separate the stego image color planes according to their format.
3. Divide the stego-image into four equal blocks.
4. Convert each pixel of the four blocks into 8bit binary value.
5. Extract the secret two bits from each pixel of the four equal blocks using bit difference.

6. Arrange the order of the four two bit group of each binary value of the secret image pixels.
7. Apply the inverse operation of graph theory randomness algorithm to de-randomize the blocks of secret image.
8. Combine the color planes and produce the secret image.

B. Frequency Embedding: Concealing confidential data in the frequency domain is more secure than spatial domain embedding. LWT localizes low and high frequency bands with various resolutions. The graph theory is used as a random as in the spatial domain to scramble the blocks of secret image before embedding. Randomizing secret data blocks is done by either modes; simple or complex. Figure. 3 shows the image steganography block diagram using frequency domain. The following are the steps for embedding the secret data in the frequency domain:

1. Select the type of randomness; simplex or complex.
2. Read color cover, secret image and value of X, Y, N, n.
3. Apply 2D-LWT on each color plane producing LL, LH, HL, HH sub bands.
4. Divide the secret image into 8*8 block size.

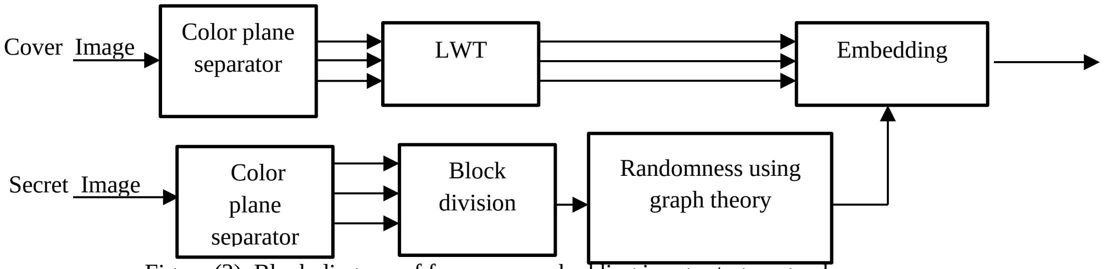


Figure (3). Block diagram of frequency embedding image steganography

5. Apply graph theory algorithm for randomizing the 8*8 blocks of secret.
6. Sign of each secret pixel is preserved and then converted to 8 bit binary value.
7. Bits from b_1…….b_6 are taken from the secret binary pixel.
8. Each binary value pixel [b_1……..b_6] is divided into three two bit groups.
9. The Embedding is conducted row by row of the secret image and for each color plane, the LL band will not be embedded:

Embedding in LH, HL bands: Find the difference between the 5th bit and 6th bit, for each pixel of the bands; if the difference is equal to the secret data, do not change the bit otherwise change the 6th bit.

Embedding in HH band: two bits are stored in the HH band since it houses high frequency components. The first bit is embedded such as in the LH &HL bands. An extra bit is embedded by finding the difference between the 7th bit and 8th bit, if the difference is equal to the secret data, do not change the bit otherwise change the 8th bit.

10. Reorder the bands of the LWT and apply Inverse LWT.
11. Combine the color planes and produce the stego-image.

The extraction process in frequency domain is as follows:

1. Read stego image and value of X, Y, N, n.
2. Separate the stego image color planes according to their format.
3. Apply two-dimension LWT on each layer of the color planes.
4. Extract the LH, HL, and HH bands and convert each pixel to its binary value and preserve the coefficient's sign
5. Extract the secret two bits from each band in the frequency using bit difference.
6. Arrange the order of the three two bit group of each binary value of the secret image pixels.

7. Apply the inverse operation of graph theory algorithm to de-randomize the 8*8 blocks of secret image.
8. Combine the color planes and produce the secret image.

6. Results and Discussion

Experimental results are presented in this section. One of the most essential parameters of steganography is correlation between the stego and cover image. Generally, the peak signal to noise ratio (PSNR) is a dependable image metric in most of the literature for assessing visual symmetry between two metrics. PSNR depends on the mean square error between the stego and cover image as in equation. (4)& (5) [20], [21]:

$$PSNR = 10\, log_{10}\left(\frac{(255)^2}{MSE}\right) \tag{4}$$

$$MSE = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}(\widehat{im} - im)^2 \tag{5}$$

Where: $\widehat{\text{im}}$ and im are the stego and cover pixels respectively. N: is the total number of pixels in a square image.

Since the embedding data is a secret image, PSNR is also calculated for the reconstructed image. Other parameters such as capacity and processing time and complexity are also essential parameters for performance assessment. As stated in section four, the proposed algorithm uses bit difference. The method is also utilized in the spatial and frequency domain. Two input images (cover and secret) images are input to the algorithm. The dimension of the cover image is 512*512 and the dimension of the cover image is 256*256. All the experiments below are run on complex random mode using MATLAB 2016B. The algorithm is experimented with various image file formats and embedding sizes. The graph theory provides random distribution of the image block pixels increasing the security features of the algorithm.

1. *Spatial domain Embedding*: In order to compare the performance of the proposed algorithm. The size of the secret image is half the cover image. The quality of the stego-image and reconstructed secret image with various image file formats are shown in table. (1). Embedding the secret image data in the spatial domain in the TIFF, PNG, BMP results in a PSNR range of (45-39dB) and a maximum embedding capacity of 786423 bits. Figure. 5 shows the reconstructed image. The reconstructed image visual symmetry is 29 dB at four embedding bits. While the proposed method has degraded performance in the jpeg cover format. Although a maximum PSNR of 45 dB is accomplished, the reconstructed secret image is subjectively undetectable. Figure 7 shows the PSNR versus payload for thee tiff image format for spatial embedding.

Cover Image color Baboon image 512 X 512

Secret Image color Lena image 256 X 256

Figure 4. Shows the original cover and secret images

2. *Frequency Domain embedding:* The same embedding methods used are used in the frequency domain. The same images are also used in this experiment. Table. (2) shows the visual quality and capacity with various image formats.

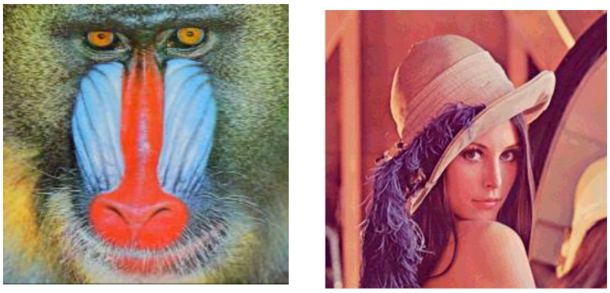
Results stated in table. (2) are for embedding in the frequency domain; the average range of the PSNR is in the range of 50- 41dB for TIFF, PNG, BMP image format and a maximum embedding capacity of 786423 bits. The reconstructed secret image can be detectable in the frequency domain at a maximum PSNR of 29dB. Figure. 6 show the reconstructed image for frequency domain embedding. The jpeg cover image format has degraded performance quality. Although the stego PSNR is in the range of 41dB at high embedding capacity, the reconstructed image quality is highly undetectable. Figure. 8 shows the PSNR versus payload for thee tiff image format for frequency embedding.

Table 1. Shows the PSNR using spatial embedding with various image formats

Stego image format	Number of embedding bits	Payload bits	MSB	
			PSNR Stego	PSNR Recovered
JPEG	1	196608	45.11	5.44
	2	393216	42.04	6.25
	3	589824	40.31	7.14
	4	786423	39.65	9.67
TIF	1	196608	45.11	10.10
	2	393216	42.04	16.67
	3	589824	40.31	22.95
	4	786423	39.65	29.07
PNG	1	196608	45.11	10.10
	2	393216	42.04	16.67
	3	589824	40.31	22.95
	4	786423	39.65	29.07
BMP	1	196608	45.11	10.10
	2	393216	42.04	16.67
	3	589824	40.31	22.95
	4	786423	39.65	29.07

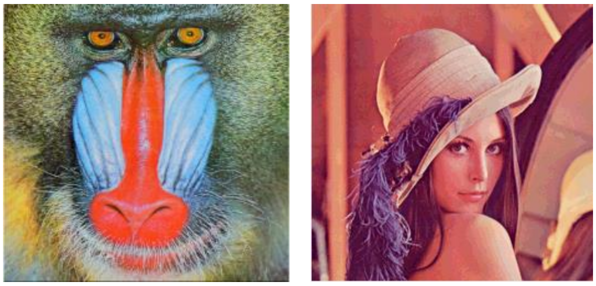
Table 2. shows the PSNR using frequency embedding with various image formats

Stego image format	Number of embedding bits	Payload bits	MSB	
			PSNR Stego	PSNR Recovered
JPEG	1	196608	50.83	5.44
	2	393216	43.78	6.25
	3	589824	43.39	7.14
	4	786423	41.42	8.07
TIF	1	196608	50.83	10.10
	2	393216	43.78	16.67
	3	589824	43.39	22.95
	4	786423	41.42	29.07
PNG	1	196608	50.83	10.10
	2	393216	43.78	16.67
	3	589824	43.29	22.95
	4	786423	41.42	29.07
BMP	1	196608	50.83	10.10
	2	393216	43.78	16.67
	3	589824	43.28	22.95
	4	786423	41.42	29.07



512 x 512 Stego Image 256 x 256 Recovered image

Figure 5. Spatial Domain, Cover PSNR = 39.65, Recovered PSNR = 29.12, Payload = 786423 bit



512 x 512 Stego Image 256 x 256 Recovered image

Figure 6. Frequency Domain, Cover PSNR = 41.42, Recovered PSNR = 29.07, Payload = 786423 bit

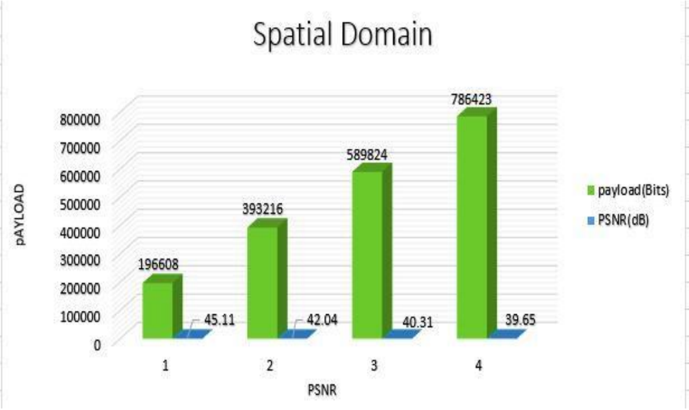


Figure 7. Payload versus PSNR for spatial embedding

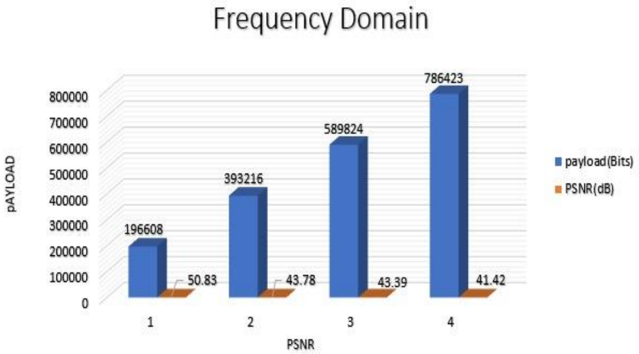


Figure 8. Payload versus PSNR for frequency embedding

A. *Comparison with other Work*

Results of the proposed image steganography are compared with other related work in terms of capacity and visual quality. The work in [12] is highly comparable with the proposed work. Table. (3) Shows a comparison of the algorithm with results in [12]. In [12], an average of the PSNR (APSNR) for the color planes is computed.

Results from the proposed algorithm in the transform domain are superior in terms of visual quality and capacity than the results presented in work [12]. The PSNR for the stego image is 50 dB for an embedding capacity of 196608 bits. While the PSNR for the stego-image is 50.62 dB for a capacity of 147456 bits in [12]. Embedding data with bit difference is more superior than embedding the secret data using the mathematical model of the LSB proposed in [12].

Table 3. Comparison of results between the proposed algorithm and work in [12]

Image	Proposed Algorithm		Work in [12]	
	Capacity	PSNR stego	Capacity	APSNR stego
Lena	196608	50.81	147456	50.62
	589824	43.40	294912	45.79
	786423	41.43	442368	39.75
Baboon	196608	50.83	147456	50.61
	589824	45.77	294912	45.87
	786423	41.13	442368	40.25

7. Conclusions

In this paper, a secure image steganography algorithm is presented using graph theory and bit difference embedding method. The algorithm embeds a randomized secret data inside a cover image with less error data retrieval and less processing time. The proposed scheme results in a high visual quality and high embedding capacity and robust against a mild compression ratio. The utilization of graph theory provides a random distribution of the secret image blocks. If the secret data existence is detected, the hacker cannot access the data unless he possesses the algorithm keys. Results show that secret data embedding in the frequency domain is superior over spatial domain in terms of imperceptibility and embedding capacity. Also, embedding the secret data with the proposed steganography technique in cover image format TIFF, PNG and BMP is more efficient than JPEG compression format since the image is not compressed and data embedding is more efficient. The algorithm can be extended through embedding the secret image data in concentric center rectangles using bit difference in order to resist cropping attacks.

8. References

[1] Zakir Khan, Mohsin Shah, Muhamad Naeem, Toqeer Mahmood, Shah Khan, Noor Ui Amin, and Danish Shazad,” Threshold –Based Steganography: A novel Technique for Improved Payload and SNR”, *The International Arab Journal of Information Technology*, Vol.13, No.4, 2016, pp380-386.

[2] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," Computer Science Review, vol. 13, 2014, pp. 95-113.

[3] Budiman.G, Suksmono.B. A, and Daundirdjo.D," A modified Multicarrier Modulation Binary Data Embedding in Audio File", *International Journal on Electricl Engineering and Informatics*, Vol.8, No.4, 2016, pp 762-773.

[4] Mehdi Hussein, Ainuddin Wahid Abdul Wahab, Yamani Idna Bin Idris, Anthony T. S.Ho, Ki-Hyun Jung,” Image Steganography in Spatial Domain: A survey” Signal Processing: *Image Communication, Elsevier,* Volume 65, 2018, pp46-66.

[5] Ahmed Ui Islam, Faiza Khalid, Mohsin Shah, Zakir Khan, Toqeer Mahmood, Adnaan Khan, Usman Ali, Muhammad Naeem,” An Improved Image Steganography Technique Based on MSB Using Bit Differencing”, *The Sixth International Conference on Innovative Computing Technology (INTECH)*, 2016, pp-265-269.

[6] R. Das and T. Tuithung, "A novel steganography method for image based on Huffman Encoding," 2012 3rd *National Conference on Emerging Trends and Applications in Computer Science, Shillong*, 2012, pp. 14-18.

[7] N. Akhtar, P. Johri and S. Khan, "Enhancing the Security and Quality of LSB Based Image Steganography," 2013 5th *International Conference and Computational Intelligence and Communication Networks*, Mathura, 2013, pp. 385-390.

[8] Munir. R," A Fragile Watermarking Scheme for Authentication of GIF Images", *International Journal of Electrical Engineering and Informatics*, Vol. 9, No.2, 2017, pp 294-312.

[9] D. Kundur and D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition," *Proceedings of the 1998 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP '98 (Cat. No.98CH36181), Seattle, WA, USA*, vol.5, 1998, pp. 2969-2972.

[10] M. R. D. Farahani and A. Pourmohammad, "A DWT Based Perfect Secure and High Capacity Image Steganography Method," 2013 *International Conference on Parallel and Distributed Computing, Applications and Technologies, Taipei*, 2013, pp. 314-317.

[11] Al-ataby A, Al-naima F. A Modified High Capacity Image Steganography Technique Based on Wavelet Transform. *International Arab Journal of Information Technology*, Vol. 7, No. 4, 2010, pp: 358–364.

[12] V. Thanikaiselvan and P. Arulmozhivarman, "High security image steganography using IWT and graph theory," 2013 *IEEE International Conference on Signal and Image Processing Applications, Melaka*, 2013, pp. 337-342.

[13] S. M. Masud Karim, M. S. Rahman and M. I. Hossain, "A new approach for LSB based image steganography using secret key," *14th International Conference on Computer and Information Technology (ICCIT 2011)*, Dhaka, 2011, pp. 286-291.

[14] W. Luo, F. Huang and J. Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited," in *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 201-214, June 2010.

[15] H. Shahadi, Ahmed T.Thahab and Manaf.M. Ali," Adaptive Embedding Approach in Color Image Carrier for Covert Communication", *Indian Journal of Science and Technology*, Vol. 9 No. 46, 2016, pp: 1-11.

[16] O. Lezoray and Leo Grady," Graph Theory Concept and Definitions used in Image Processing and Analysis, Robin Wilson 1996.

[17] R.O. EI Safy, H. H. Zayed, A EI Dessouki, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform", in Proc. ICNM, 2009, pp. I1-117.

[18] G. Prabakaran. and R. Bhavani., "A modified secure digital image steganography based on Discrete Wavelet Transform," *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, Kumaracoil, 2012, pp. 1096-1100.

[19] Sweldens W. "The lifting scheme: a custom-design construction of biorthogonal wavelets", Applied Computational Harmonic Analysis, vol. 3, no. 2, 1996, pp:186–200.

[20] A. Siddiqui and A. Kaur, "A secure and robust image watermarking system using wavelet domain," *2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence*, Noida, 2017, pp. 599-604.

[21] Shahadi HI and Jidin R, Way WH, "Lossless Audio Steganography based on Lifting Wavelet Transform and Dynamic Stego Key" Indian Journal Science of Technology. 2014; vol. 7, pp 323–34.

Ahmed Kamel Abbas He received his B.sc from University of Kerbala/ Iraq from the Department of Science. He obtained his M.sc from Basrah University/ Iraq in 2014. Currently he is a lecturer at the University of Karbala, Electrical and Electronic Engineering Department. His research interest is Data mining, Image compression and Data base analysis.

Ahmed Toman Thahab He received his B.Sc in Electrical Enginnering from the University of Babylon in2006, and enrolled in the Graduate school of the same universty. He received his M.sc degree in the Communication and Electronic Engineering in 2011. His main study was in video compression based on wavelet Transform.