Open Access
Baghdad Science Journal **Vol.16(4) 2019**

DOI: http://dx.doi.org/10.21123/bsj.2019.16.4.0948

Symmetric- Based Steganography Technique Using Spiral-Searching Method for HSV Color Images

Raheem Abdul Sahib Ogla

Received 20/7/2018, Accepted 3/6/2019, Published 1/12/2019

Abstract:

Steganography is defined as hiding confidential information in some other chosen media without leaving any clear evidence of changing the media's features. Most traditional hiding methods hide the message directly in the covered media like (text, image, audio, and video). Some hiding techniques leave a negative effect on the cover image, so sometimes the change in the carrier medium can be detected by human and machine. The purpose of suggesting hiding information is to make this change undetectable. The current research focuses on using complex method to prevent the detection of hiding information by human and machine based on spiral search method, the Structural Similarity Index Metrics measures are used to get the accuracy and quality of the retrieved image and to improve its perceived quality.

The values of information measures are calculated through practical experiments of (perceptibility, robustness, capacity) by using interpolation technique and structural similarity measures. Experimental results show that the use of these measures (PSNR, MSE, and SSIM) has improved the image quality by 87% and has produced values of PSNR (38-41 dB), MSE = 0.6537 and SSIM= 0.8255. The results also demonstrate a remarkable progress in the field of hiding information and the increasing difficulty of detecting it by humans and machines.

Key words: Hierarchal decomposition Image processing, Information hiding, Security Techniques, Spiral search, Steganography.

Introduction:

The emergence of the Internet with the rapid progress of information technologies, digital contents became an everyday activity of our life. Nowadays, there is a risk that confidential information may be accessed by unauthorized people, being consulted, divulged, modified, destroyed, or sabotaged, affecting its availability and legal access. The massive amount of the chosen information is traveling through the digital networks like many transfer trade transaction digital media, military information and personal private data. The importance of this information justifies the use of different security procedures like cryptography, information hiding, watermark, and others to protect the information from corruption or illegal access. Information hiding provides a reliable communication by embedding secret code into content for intellectual property protection, content authentication, fingerprinting, transmission media.

Computer Science Department, University of Technology, Baghdad, Iraq.
E-mail : 110137@uotechnology.edu.iq

The research in this field has an increasing role because of the sensitivity of the transmitted information. Steganography is a technique to hide information into digital content files to ensure secret communication so that the information can be exchanged through the network safely (1).

The use of hiding algorithms has many risks like algorithm weakness and using strong analysis procedures may help attackers to discover the hidden content. Figure 1 illustrates the main idea of information hiding, that enables analysts to discover the contents of the image by analyzing their contents (2).

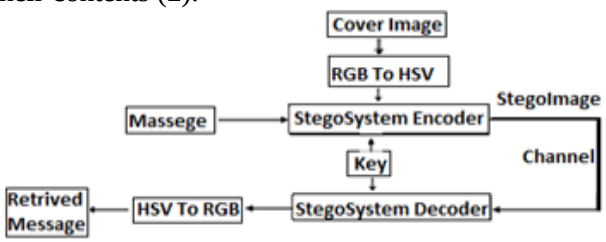

Figure 1. Block diagram for traditional information hiding system (1).

In this research, random locations are chosen to select hosting locations to estimate the area of the cover image. The proposed method is adept at estimating precise random areas of the cover image and ensures precise randomized distribution locations after the inclusion of the secret message using the spiral search. The cover image is divided into four equal sized spaces like the first level of Haar technique. Each space (quarter) is divided into equaled sizes blocks. So, to hide a secret message one bit from the random blocks from random quarter are selected to hide the secret message in a spiral manner. The number of selected hosting bits depends on the length of the secret message. Interpolation technique is used to estimate the capacity, robustness, and perceptibility.The experimental results reveal that the proposed technique has achieved good cognitive quality and comparability in other relevant ways.

The rest of the paper is organized as follows: in section 2 the related works are studied, in section 3 the proposed adopted steganography is presented ,in section 4 and 5 the analysis of experimental results are discussed, and finally the conclusions are presented in section 6.

Research Contribution

There are two common ways to hiding data, which can be classified into two categories, namely the spatial domain and the frequency field methods. In the first method, the confidential message is inserted directly into the least significant sign (LSB) of the image pixels (3) (4). In the second method (5), the cover image is first converted from the spatial range to the frequency domain using the conversion methods. This research contributes to the security of hidden data and confidential information transmitted through the media in such a way as to make it difficult for the attacker to penetrate, while maintaining the accuracy and quality of the carrier's medium through using spiral searching.

Related Works

Over the past few decades, the science of steganography has attracted widespread interest in researchers; many related works were proposed in information Hiding and spatial and frequency domains. Many techniques have been proposed to date for embedded confidential information. For example:

In **2011:** Introduced a new approach that provides good protection for confidential data and information, which used LSB method and secret key. The secret key is used to hide highly sensitive information for storing on different LSB bits of the cover image. (5).

In 2014: suggested hiding adaptive information based on LSB replacement. It incorporates a secret message at the edges of the areas in the cover image using the adjustment scheme and the difference between the two pixels adjacent to the cover image. These techniques perform well from LSB-based and Pixel-based techniques, and maintain stego image quality (4).

In 2015: Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture proposed a state-of-the-art approach of binary image steganography. This technique is proposed to minimize the distortion on the texture (6).

In 2017: This paper proposes a new method where no change is made to the cover image, only the pixel position LSB (Least Significant Bit) values that match with the secret message bit values are noted in a separate position file. (1)

In 2017: proposed a novel steganographic method based on the compression standard according to the Joint Photographic Expert Group and an Entropy Thresholding technique. The steganographic algorithm uses one public key and one private key to generate a binary sequence of pseudorandom numbers that indicate where the elements of the binary sequence of a secret message was be inserted. (2)

Proposed adaptive steganography

The proposed technique consists of four stages process: Preprocessing, Hiding process, Searching scanning and Hiding location selection.

Preprocessing

The preprocess procedure implies converting the image color model from RGB components to HSV components, in order to invest one component of the cover image to hide the secret information which is the component (H), because it contains a rich information. This means computing the bands H (Hue), S (Saturation) and V (value) which are computed according to RGB to HSV conversion algorithm as revealed in equations 1 to 4. Where H is in a scaled between 0 to 6 inclusively, and S and V in a scale between 0 to 1. (5) .

$$H = \begin{cases} 0 & if \ \ \Delta = 0 \ \ \ldots\ldots (1) \\ \left(\frac{(H')}{Scale_h} \ mod \ 6\right) + 6 & if \ H' < 0 \ldots\ldots\ldots (2) \\ \left(\frac{(H')}{Scale_h} \ mod \ 6\right) & otherwise \ldots (3) \end{cases}$$

$$H' = H \times scaleh, \quad S = \frac{S'}{Scale_S} \quad ,$$
$$V = \frac{V'}{Scale_V}, \ldots\ldots(4)$$

Then, in receiving side, the values of the channels α, β, γ which are representing the Red, Green, Blue channels are computed according to equations (5, 6, 7).

$$\propto = V \times (1 - S) \ldots (5)$$

$$\beta = \begin{cases} 0 & \Delta = 0 \\ V \times (1 - (\lfloor H \rfloor)) \times S & Otherwise \end{cases} \ldots(6)$$

$$\gamma = \begin{cases} 0 & if\ H = 0 \\ V \times (1 - (1 - (H - \lfloor H \rfloor)) \times S) Otherwise \end{cases} \ldots(7)$$

Now, the computed H value (0-6) can be used to store the message code (secret text) as describes in equation (8)

$$(R, G, B) = \begin{cases} (V; V; V) & \text{if H} = 0 \\ (V; \gamma; \alpha) & \text{if } 0 \leq \text{H} < 1 \\ (\beta; V; \alpha) & \text{if } 1 \leq \text{H} < 2 \\ (\alpha; V; \gamma) & \text{if } 2 \leq \text{H} < 3 \\ (\alpha; \beta; V) & \text{if } 3 \leq \text{H} < 4 \\ (\gamma; \alpha; V) & \text{if } 4 \leq \text{H} < 5 \\ (\gamma; \alpha; V) & \text{if } 5 \leq \text{H} < 6 \end{cases} \ldots\ldots(8)$$

After converting the RGB image into the components (H, S, V.) the H image is divided into four quarters as shown in Fig. 2, then each quarter is divided into equal size blocks as shown in Fig. 3 and 4 represents a selection of the host blocks through the spiral search method and using geometric function (transforms image I (cover image) to new image I' (stegno-image) by modifying coordinates of image pixels) as implemented in equation (9).

$$I(X, Y) \xrightarrow{Spirally} I'(X', Y') \ldots\ldots\ldots(9)$$

The selection of searching method starts from the image center and spreads away in all directions, one block is selected from each quarter of the four quadrants in each spiral searching cycle, this randomization manner of selection leads to increasing the complexity of the hiding process. Then only one pixel is obtained at a time from each symmetry selected blocks, choosing the LSB bits of selected pixels to hide one bit from secret message in those selected hosting bits as shown in Fig. 5 the hiding process is illustrated in algorithm 1.

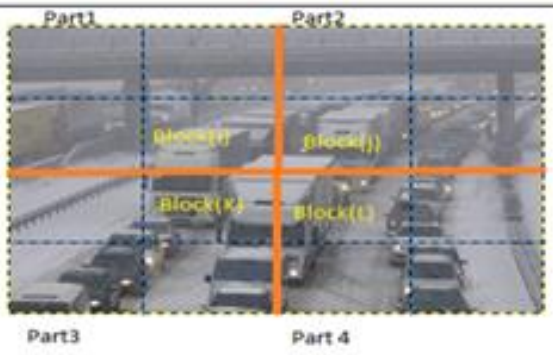

Figure 2. Divide band tofour parts and blocks hsv

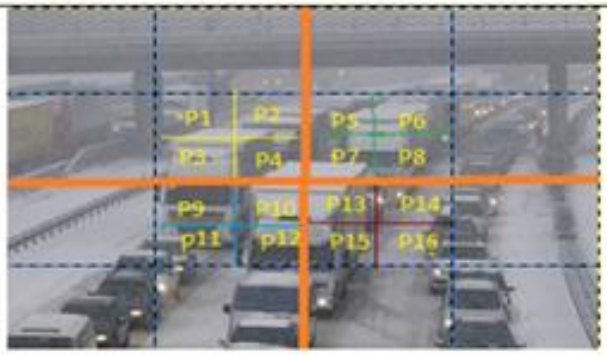

Figure 3. Divide each block to(n ×n) pixcels

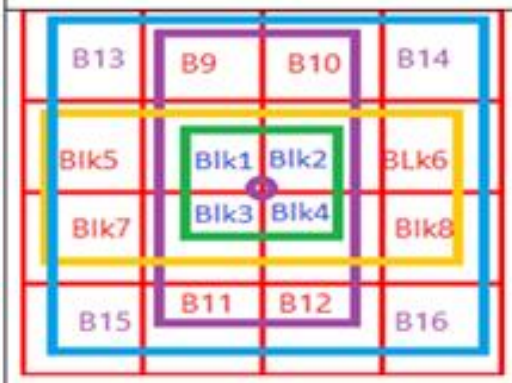

Figure 4. Move in Spiral Manner

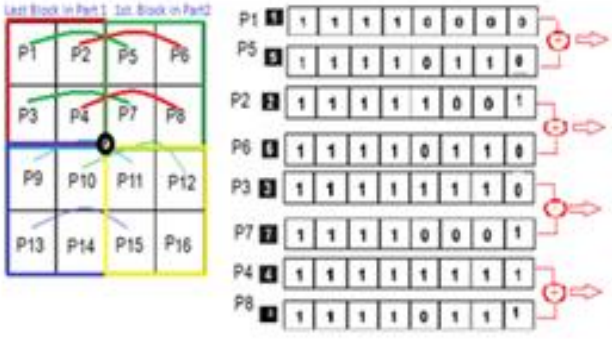

Figure 5. Get Pixels Symmetry

Spiral Scanning and Selecting Hosting Blocks

Spiral search scanning can begin either at the center of the cover image (outward spiral) or a corner of the cover image (inward spiral). Like linear or Cantor-diagonal scanning, Spiral scanning is continuous in any one plane, but continuity in the image of two dimensions can only be maintained by reversing the inward/outward direction (4) (5).

Algorithm (1) is used *to* preparing and determining hosting bits positions in hosting image based spiral technique starting from image center and moving clockwise through all the hosting image blocks.

Algorithm (1): preparing *hosting bits positions* based Spiral search technique //*scanning and selecting hosting bits positions.*
Input: cover image, secret text ***Output****: information embedding*
1. Divide the cover image into four equal size parts. 2. Divide each part into equal sized blocks. 3. Start from the center of the cover image; move in a spiral way clockwise. 4. Passing through the corresponding blocks located in each of the four quarters. 5. Get the pixels values in each symmetry blocks. a. According to the peer pixel locations in each block. Perform the following actions: If the value of bit taken from the text equal to 1 , apply the following steps : • If the values of bits taken from pixels of both parts equal to 1, nothing is done. • If the values of bits taken from pixels of the first part equal 0 and the second equal 1, changes the first one to 1. • If the values of bits taken from pixels of the first part equal 1 and the second equal 0, changes the second one to 1. • If the values of bits taken from pixels of both parts equal to 0's then both bits changes to 1's. b. If the value of bit taken from the text equal to 0 ,the following steps applied: • If the values of bits taken from pixels of both parts equal to 0 we there is no action. • If the values of bits taken from pixels of the first part equal 0 and the second equal 1, the second one changed to 0. • If the values of bits taken from pixels of the first part equal 1 and the second equal 0, the first one bit changed to 0. • If the values of bits taken from pixels of both parts equal to 1, both bits changed to 0. Step6: If the values of bits taken from pixels of image parts equal to 0 go to step 9 Step7: if binary bit from text reach to end go to end Step8: go to step 5 Step 9: end

Hiding Algorithm

The process of hiding secrete massage in cover image is described in the Algorithm (2).

Algorithm (2) **Proposed Hiding Algorithm**// *perform hiding process*
Input: Secret text ***Output: embedding information***
Step1: Convert text file to binary secret bits Step2: Read the cover image in RGB and then convert it to HSV according to equations 1-4 Step3: Divide the HSV image into 4 quarters. Step4: Get Pixel values of each selected blocks through spirally technique. Step5: Selecting 4 pixels from selected blocks according to geometric function and these pixels are symmetric in positions Step6: Select the first bit (LSB) from each selected pixels Step7: Check the binary bit from text and do the following Step8: If binary bit from text equal 0 then go to step 13 Step9: If the values of bits taken from pixels of image parts equal to 0 then changes both bits to 1 and go to step 17. Step10: If the values of bits taken from pixels of image parts, the first one equal 0 and the second equal 1, change the first one to 1 and go to step17. Step11: If the values of bits taken from pixels of image parts first one equal 1 and the second equal 0, changes the second one to 1 and go to step 17. Step12: If the values of bits taken from pixels of image parts equal to 1 go to step 17. Step13: If the values of bits taken from pixels of image parts first one equal 0 and the second equal 1, change the second one to 0 and go to step 17. Step14: If the values of bits taken from pixels of image parts first one equal 1 and the second equal 0, change the first one to 0 and go to step 17. Step15: If the values of bits taken from pixels of image parts equal to 1, changes both bits to 0 and go to step 17. Step16: If the values of bits taken from pixels of image parts equal to 0 then go to step 17. Step17: if binary bit from text reach to end go to step 19 Step18: go to step 7 Step19: End

Proposed Embedding Procedure

Embedding process consists of the performs frequency transformation of the target image, selection of the feature subblocks, start embedding process, perform extraction embedded message, frequency domain conversion of the images can lead to better enhancement. It represent the rate of change of spatial pixels and hence gives an advantage when the problem dealing with relates to the rate of change of pixels, which is very important in image processing. On the other hand, high frequency in the frequency domain represents rapidly or sharply changing pixels such as boundaries or edges in an image. A high pass filter can be extremely helpful in identifying or removing these edges easily but the same problem is much more difficult in the spatial domain (x-y domain). Similarly, a simple low pass filter can be used to get a smoother image.

First, frequency transformation of the image is performed on each image channel (R, G, B, ranging from 0-255). Second, the image is divided into four parts and convert the text into the binary form. Third starting the embedding process as explained in Algorithm II, Fourth, save the hosting image (geometric functions) generated from the retrieved image that is used in the system. Then save the image in HSV and send the image to the destination**.**

Extraction Procedure for the Proposed System

The first procedure is an equivalent process as the first procedure in the embedding process. Extractor must receive the coordinate from the embedded user. Only knowing the proper coordinates of feature sub-blocks will lead the user to the proper input values. Second, the user uses the equivalent method that was used in embedding process to generate the same locations used before (geometric functions). After selecting the pixels, we compare the first bits and extract the binary hiding data, after that combine this binary data together to construct text. Third, convert the HSV image to RGB image and display it on the screen. Algorithm (3) explains the main idea.

Algorithm (3)* Proposed Extracting Algorithm // *Perform* Extracting *Process
Input: Hosting image ***Output: Get Plain Text***
Step1: a: Compute length of secret message in bits //(No. Bytes * 8) **Step1: b:** Read the hosted Image and, Divide the HSV band image into 4 parts. **Step2:** Divide each part into (n× n) equal size blocks. **Step3:** Selecting 4 pixels from symmetry (around image center), these pixels are symmetric in four quarters positions and blocks positions. **Step4:** Select the LSB (Least Significant Bit) from each selected pixels. **Step5:** If the values of bits taken from pixels of image parts equal to 1 generate 1 binary bit for text character. **Step6:** If the values of bits taken from pixels of image parts equal to 0 generate 0 binary bit for text character. **Step8:** if reached to length of text go to end **Step9:** go to step 2 **Step9:** end

Analysis of Experimental Results

In this section the results are presented and discussed, many images in different size and resolution are tested which are 256×256, 512×512 and 1024 × 1024 and different blocks size (2×2,4×4,8×8) pixels are tested as described in Fig. 6,7 and 8 and Table 1.

Figure 6. Lina with image size (256 × 256)

Figure 7. Fruits with image size (1024 × 1024)

Figure 8. Parrot with image size (512 × 512)

Table 1. Different images and block Size are used to hiding information

Image Name	Image Size W×H	Block Length/pixels (n)	Step Size	Block Size (pixels/Block) S=n × n	# hosting Blocks B=W/S×H/S	# hosting Bits/ Block (L)	Total hosting Bits T=B×L
Icon finder	128×128	2	2	4	1024	4	4096
		4	4	16	64	16	1024
		8	8	64	4	64	512
Lena	256×256	2	2	4	4096	4	16384
		4	4	16	256	16	4096
		8	8	64	16	64	1024
Parrot	512×512	2	2	4	16384	4	65536
		4	4	16	1024	16	16384
		8	8	64	64	64	4096
Fruits	1024*1024	2	2	4	16256	4	65024
		4	4	16	1024	16	16384
		8	8	64	64	64	4096

Different blocks sizes are studied and tested as shown in Fig. 9,10,11,12. The effect of blocks sizes on cover images can explain as follow:

When dividing the host image into blocks, the size of the block plays an important role. If the size of the block is small (2 × 2, 4 × 4), the number of hosted blocks will be more and therefore the capacity of hidden information will be more and the quality of the host image will not be affected and vice versa. If the block size is large (8 ×8, 16×16), the capacity of the hidden information will be less and there will be an impact on the quality of the host image. Using the spiral method to identify the host blocks, a random manner was found in selecting the host blocks (gradually moving away from the center of the image and spread in different directions). This reduced the deformation of the host image, maintained its quality, and chose the cover image that contains rich information as shown in Fig. 7 which makes the human eye be unaffected by the process of hiding. This will lead to less suspicion by analysts of the embedded method and leads to the difficulty of retrieving hidden information in the host image, and increasing the degree of complexity.

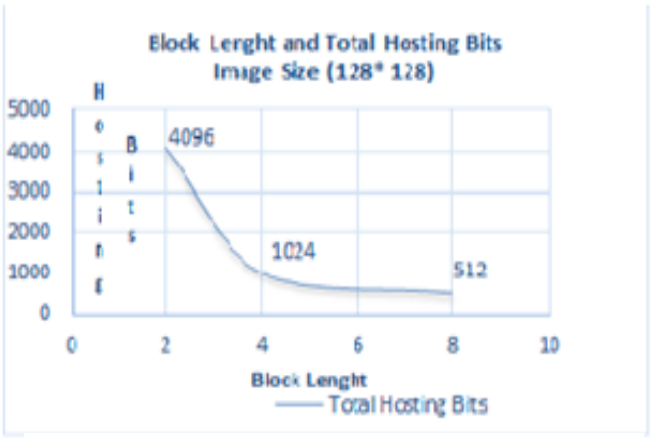

Figure 9. Effect of block length image size(128×128)

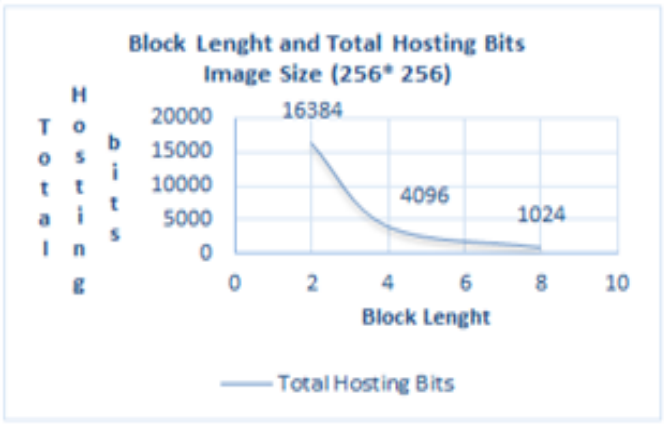

Figure 10. Effect of block length image size(256×256)

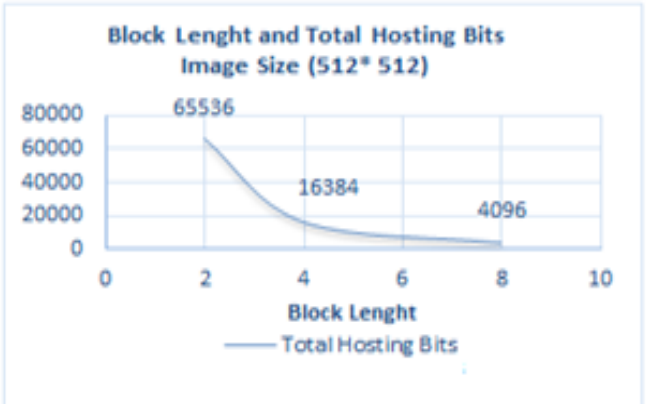

Figure 11. Effect of block length image size(512×512)

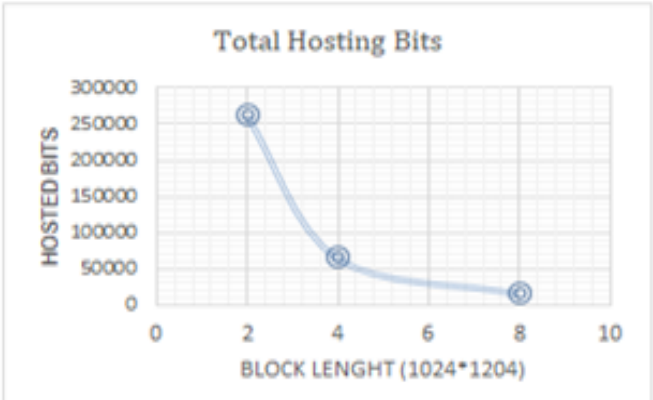

Figure 12. Effect of block length image size(1024×1024)

Experiments showed that using the spiral-searching manner and randomly selected hosting blocks have effects on quality of the hosting image. Fig. 13 and 14 shows the impact of the block size on the quality of the hosting image. When the block size is small (2 ×2) the quality of the host image is high. The larger the block size (8×8), the less the quality of the hosting image. In other words, the block size is inversely proportional to the quality of the hosting image.

In this research, many metrics are used to verify the quality of results, such as Peak Signal to Noise Ratio (PSNR) is expressed in decibels (dB), MSE ,and Structural Similarity Index Metrics (SSIM) such measures are used to study the quality of a stego image, the PSNR is defined as equation (10,11,12,13,14,15,16) (7) (8),.

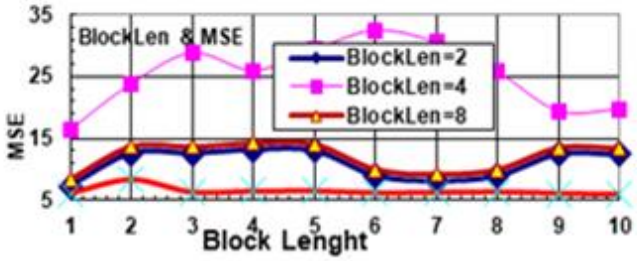

Figure 13. Block length with MSE

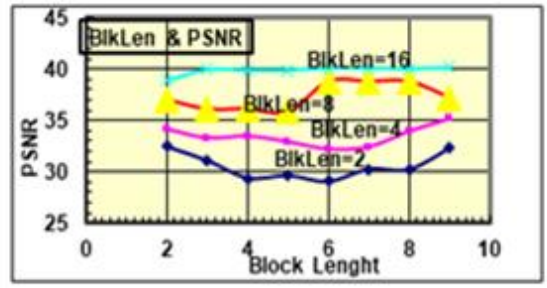

Figure 14. Block length with PSNR

MSE is the average of the square of the errors (pixel differences) of the two images.

$$\text{MSE} = \frac{1}{N}\sum_{k=1}^{n}(p_{x,y} - \overline{P_{x,y}})^2 \quad \ldots. (10)$$

Mean Square Error (MSE) between the two images (8):

Where $P_{x,y}$the original is image and $\bar{P}_{x,y}$ is the StegoImage.

$$\text{PSNR} = 10 \times log10 \frac{(Max)^2}{\sqrt{MSE}} \ldots (11)$$

Where Max is the maximum gray value of pixels.

The *Root Mean Square error* (RMSE) is defined as the square root of the MSE. (9)

$$RMSE = \sqrt{\frac{1}{N}\sum_i \sum_{j(E_{ij} - O_{ij})} 2} \ldots\ldots\ldots\ldots\ldots (12)$$

Where N is the size of the image, E is the processed image, and O is the original image.

$$SSIM = \frac{(2\times\bar{x}\times\bar{y}+C1)(2\times\sigma_{xy}+C2)}{(\sigma_x^2+\sigma_y^2+C2)\times((\bar{x})^2+(\bar{y})^2+C1)} \ldots\ldots\ldots\ldots..(13)$$

Where c1 and c2 are constants, $\bar{x}, \bar{y}, \sigma_x^2, \sigma_y^2$, and σ_{xy} are given as:

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i, \quad , \qquad \bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i \ldots\ldots.(14)$$

$$\sigma_y^2 = \frac{1}{N-1}\sum_{i=1}^{N}(y_i - \bar{y}) \ldots\ldots\ldots\ldots\ldots\ldots\ldots.(15)$$

$$\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y}) \ldots\ldots\ldots\ldots.(16)$$

In hiding stage, different blocks are taken for image Parrot (10) , and compare to the same image before converting to HSV format, while the hiding text has been stored in the band (H) wich contains the rich information.

The extracting stage (received side) extracts the hidden text bits form H, converting them back to RGB format, as shown in Figs. 15, 16, 17, a's and b's . Figures 15 and 16 shows the average PSNR (58.4) as in Table 2, it is a well PSNR for size block (2×2) and (4×4). Sequentially, the human eyes can't detect any changes in the resulted hosted image and that achieves information hiding objectives. This leads to get well perceptibility. Figure 17 a and b shows less PSNR (41.126667) for size block (8×8). The proposed method resists changes (robustness) like translation, scaling and rotation.

MSE measure is used to confirm and analyze the results (**0.445491667**) which has been indicated in the equations (10). MSE is a measure of the differences between cover image and hosting image. The experimental results show when the block length is selected as (2×2) the differences is between (2- 4), while block length is selected as (16×16) then the value of MSE is between (37-40) as shown in Fig. 14. This indicates that the mean squared error (MSE) is inverse proportional to the length of the block

Comparison of results

The proposed system results have been compared with P. U. Deshmuk et al. (4) and Karim et al. method (10) on Table 1 and 2. They hide the bits of secret text directly in the image using bit insertion on the same image which is called hammer and same text for hiding the results (7). The comparison results are described in Table 2 .The

PSNR of the proposed system is between (38-41) as shown in Fig. 14 a and b, and the traditional method (bit insertion) got 44.5, so the result of the proposed system is in the acceptable range of PSNR standard (between 38- 55) while the other method is out of the range.

Figure 15.a Before hosting block size(2 ×2)

Figure 16.a Before hosting block size(4 ×4)

Figure 17.a Before hosting block size(8 ×8)

Figure 15.b After hosting block size(2 ×2)

Figure 16.b After hosting block size(4×4)

Figure 17.b After hosting block size(8×8)

The experimental results explained the various image quality assessment metrics for performance evaluation (PSNR, MSE, RMSE, and SSIM). The proposed technique is also compared with the Karim et al. method (10) and the proposed method implemented by utilizing MS.VB version 6 and MS. SSPS V. 14.

Multiple experiments are done to evaluate the results from different perspectives and different standard color images of differing dimensions.

Results Discussion:

The proposed algorithm experimental results and the Karim et al. (10) algorithm shown in Table 2 contain the PSNR values, MSE values, and RMSE values of (Karim, Proposed) algorithms**.** The hosting image having PSNR values less than 54 (dB) are assumed to be of higher quality. Nevertheless, PSNR values less than 32 dB represent a less variety of hosting image and then makes noticeable deformation in cover image that are readily detectable. Similarly, the MSE values for the proposed algorithm are less as compared to the Karim et al. (10) method. Furthermore, the RMSE scores of the proposed technique are less than the Karim et al. (10)method. This means that the proposed algorithm provides promising results regarding PSNR values, confirming its better performance and quality.

Table 2. Methods using PSNR and MSE with different images comparison

S_No.	Image Name	Karim et al. [10] method	Proposed method	Karim et al. [10] method	Proposed method	Karim et al. [10] method	Proposed method
		PSNR	PSNR	MSE	MSE	RMSE	RMSE
1	**Lena**	55.6551	58.0362	0.4682	0.449	0.6842	0.67
2	**Parrot**	41.9414	59.3242	0.6212	0.4392	0.7881	0.6627
3	**House**	50.949	58.1054	0.5114	0.4484	0.7151	0.6696
4	**Peppers**	17.3893	58.0362	1.4984	0.449	1.224	0.67
5	**Building**	55.1595	59.3242	0.4724	0.4392	0.6873	0.6627
6	**Army**	55.6788	60.3252	0.468	0.4319	0.6841	0.6571
7	**Building1**	28.7007	58.0116	0.9078	0.4491	0.9527	0.67014
8	**Office**	45.3351	58.3514	0.5747	0.4465	0.758	0.6682
9	**Trees1**	38.7399	58.1752	0.6726	0.4479	0.8201	0.6692
10	**Trees2**	24.0736	58.0284	1.0823	0.449	1.0403	0.67
11	**Baboon**	50.8811	58.0648	0.5121	0.4487	0.7156	0.6698
12	**Girl**	28.3517	58.1558	0.919	0.448	0.9586	0.6693
Average		**41.07126667**	**58.49488333**	**0.725675**	**0.445491667**	**0.835675**	**0.667395**

Table 3 highlights the proposed technique which gives more PSNR values if compared to the A. P. U. Deshmuk (4). The proposed algorithm shows its better results regarding PSNR which validate the effectiveness.

Table 3. The methods using PSNR values with variable image dimensions, Comparison

Image name / Dimensions	Hidden (bits)	Block Length / Block size	P. U. Deshmuk (4)**Method**	Proposed Method
			PSNR dB)	**PSNR(dB)**
Baboon 128×128	1926	2×2 = 4 bits	52.89	53.17
	3240	4×4 = 16 bit	50.01	50.34
	6480	8×8= 64 bit	48.92	48.51
	12960	16×16=256 bit	47.63	47.47
Building 256×256	166782	2×2 = 4 bits	53.12	53.18
	175208	4×4 = 16 bits	50.17	50.87
	187564	8×8= 64 bits	48.82	48.39
	186416	16×16 =256 bits	47.73	47.93
Girl 512×512	166780	2×2 = 4 bits	53.46	53.87
	209873	4×4 =16 bits	50.13	51.43
	214584	8×8= 64 bits	48.15	48.79
	225490	16×16=256 bits	47.63	47.45

The most common methods for measuring the quality of enhanced images are Mean Square Error (MSE), Peak Signal-to-Noise-Ratio (PSNR). Those measures have been recognized as inadequate because they do not evaluate the result in the way that the human vision system does. So, more quantitative performance estimation of the security requirements of the secret message estimated are based on the evaluation of stego-image enhancement of quality.

The evaluation stego-Image quality was performed by computation Peak to Signal Noise Ratio (PSNR), Signal to Noise Ratio (SNR) Root Mean Square Error (RMSE), and Structural Similarity Index metrics (SSIM) of index level of 0, between cover image and the stego image and using SNR and SSIM which is used to assessments the enhancement of retrieved cover image . The results of the evaluation of the stego-Image quality using PSNR, SNR, RMSE, and SSIM between the stego-image and cover image are explained in Table 4 .It is obvious that the increase in enhancement of the retrieved cover image is inversely proportional to evaluate cover image size, according to values of SNR and PSNR increasing with a decrease in the pixel value of a cover image. This comparison is viewed from the theoretical perspective where the high value of PSNR is referred to a higher quality of the image (11).

Table 4. Different comparison of quality enhancement measurements

	Cover-Image				Stego-Image			
Image Size	SNR/ dB	PSNR /dB	RMSE /dB	SSIM Lvl-0	SNR / dB	PSNR / dB	RMSE /dB	SSIM Lvl-0
House.jpg 512*512	50.118	46.015	89.136	0.5700	50.118	56.456	89.136	0.7698
Peppers.jpg 256*256	51.909	47.840	83.109	0.7191	51.909	55.921	83.109	0.8011
Girl.jpg 128*128	55.569	51.566	72.030	0.8075	55.569	54.967	72.030	0.9056
average	52.532	48.478	81.425	0.6988	52.532	55.761	81.425	0.8255

Table 5 the higher embedding capacity is achieved by introducing 1bit with the least degradation in the cover image.

Table 5. Quality evaluation of proposed system using randomly selected images.

Image	Max. Capacity	Payload	PSNR	MSE	SSIM
Army	195416	52428	54.11	0.252	0.9996
Office	227490	52428	54.04	0.256	0.9997
Trees1	198564	52428	53.98	0.259	0.9995
Trees2	185108	52428	54.06	0.253	0.9994

Conclusions:

This paper proposes a steganography method based on searching spiral method to determine hosted blocks and identify the hosted bits on each block of the whole cover image to insert secret information in colored images without significant change to the cover image. The proposed method effectively specifies the positions of hosting blocks in a complex manner due to the spirally selection of hidden blocks, which are utilized to embed secret information bits. The cover image is retained after inserting the confidential message so that the data accurately can be retrieved on the receiver side. Experimental results reveal that the proposed method achieves better quality of hosted images compared to other methods of the same inclusion capacity rates as computed in equation (12).

Conflicts of Interest: None.

References:

1. Mamaheswari GU, Sumathi CP. A New Information Hiding Technique Matching Secret Message And Cover Image Binary Value. International Journal of Computer Science and Information Security (IJCSIS). 2017; January 15(1).
2. Soria-Lorente A, Berres S. A Secure Steganographic Algorithm Based on Frequency Domain for the Transmission of Hidden Information". Hindawi, Security and Communication Networks. 2017; Volume 2017(3): p. 14 pages.
3. Prashanti G, Sandhyaran K. A New Approach for Data Hiding with LSB Steganography. Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI. Springer 2015; 3: p. 423-430.
4. Pattewar P. A Novel Approach for Edge Adaptive Steganography on LSB Insertion echnique. In ; Feb. 2014. p. 1-5.
5. Debnath D, Deb S, Nar N. Encryption Using Hill Cipher and RGB Image Steganography. IEEE International Conference on Computational Intelligence and Networks (CINE). Jan. , 2015.;: p. 178-183.
6. Parvin BD, Pradfi SB. Image Steganography Using LSB Algorithm. International Journal of Advanced Research in Electrical. August 2016; 5(8).
7. Modi MR, Gupta , Islam S. Edge Based Steganography on Colored Images. 9th International Conference on Intelligent Computing (ICIC). July 2013;: p. 593- 600.
8. ALDmour H, AlAni A. A steganography embedding method based on edge identification and XOR coding. Expert systems with Applications. 2016. p. 293-306.
9. Diaa M, Khalifa OO. Robust and Secure Image Steganography Based on Elliptic Curve Cryptography. In ICCCE; 2014; Kuala Lumpur, Malaysia. p. 288-291.
10. Karim MA. New Approach for LSB Based Image Steganography Using Secret Key. In ICCIT; 2011; Bangladesh. p. 286-291.
11. Muhammad K, Ahmad J, Sajjad M. Secure image steganography using cryptography and image. NED University Journal of Research. June 2015.
12. Goel S, Gupta, S, Kaushik N. Image Steganography – Least Significant Bit with Multiple Progressions". In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA). 2014-2015. p. 105.

تقنية إخفاء المعلومات المتناظرة باستخدام طريقة البحث الحلزوني للصور الملونة HSV

رحيم عبد الصاحب عكلة

قسم علوم الحاسوب، الجامعة التكنولوجية، بغداد، العراق.

الخلاصة:

إخفاء المعلومات يعني أخفاء المعلومات السرية في بعض الوسائط المختارة الأخرى دون ترك أي دليل واضح على تغيير ميزات الوسط الناقل. تخفي معظم طرق الاختباء التقليدية الرسالة مباشرةً في الوسائط الناقلة مثل (النص والصورة والصوت والفيديو). يترك بعض الاخفاء تأثيرًا سلبيًا على صورة الغلاف الناقلة، هذا التأثير السلبي يُمكن من اكتشاف التغير في والوسط الناقل من خلال الإنسان والآلة. الغرض من طريقة إخفاء المعلومات المقترحة هو ان جعل هذا التغيير غير قابل للكشف، يركز البحث الحالي على استخدام طريقة معقدة لمنع الكشف عن إخفاء المعلومات بواسطة الإنسان والآلة باعتماد على طريقة البحث اللولبي، تم استخدام مقاييس مؤشر التشابه الهيكلي للقياس للحصول على دقة وجودة الصورة المستردة وتم تحسين جودتها المدركة.

تم حساب قيم مقاييس المعلومات من خلال التجارب العملية (الإدراك، المتانة، السعة) باستخدام تقنية الاستيفاء ومقاييس التشابه الهيكلي. تظهر النتائج التجريبية أن استخدام هذه المقاييس (PSNR و MSE و SSIM) قد حسن جودة الصورة بنسبة 87٪ وأنتج قيم PSNR (38-41 ديسيبل) و MSE = 0.6537 و SSIM = 0.8255. توضح النتائج أيضًا تقدمًا ملحوظًا في مجال إخفاء المعلومات وتزايد صعوبة اكتشافها من قِبل البشر والآلات.

الكلمات المفتاحية: إخفاء المعلومات، البحث اللولبي، التحلل الهرمي، تقنيات الأمن، معالجة الصور،