Ibn Al Haitham Journal for Pure and Applied Science
Journal homepage: http://jih.uobaghdad.edu.iq/index.php/j/index

Image Steganography Based on Wavelet Transform and Histogram Modification

Enas Muzaffer Jamel

Department of Computer Science, College of
Education for Women, University of
Baghdad Department

enasm.altai@gmail.com

Article history: Received 13 June 2019, Accepted 24 July 2019, Publish January 2020.

Doi: 10.30526/33.1.2365

Abstarct

Recently, digital communication has become a critical necessity and so the Internet has become the most used medium and most efficient for digital communication. At the same time, data transmitted through the Internet are becoming more vulnerable. Therefore, the issue of maintaining secrecy of data is very important, especially if the data is personal or confidential. Steganography has provided a reliable method for solving such problems. Steganography is an effective technique in secret communication in digital worlds where data sharing and transfer is increasing through the Internet, emails and other ways. The main challenges of steganography methods are the undetectability and the imperceptibility of confidential data. This paper presents a steganography method in frequency domain. Haar Wavelet Transform is applied for decomposition of gray level cover image into four sub-bands. The secret image is hidden in the high frequency HH sub-band after applying the histogram modification followed by scrambling process. A Histogram modification is adopted, to scale the secret image to normalize its values, that manipulates the secret image from bright image to dark. Thus the secret image becomes invisible so it can be hidden in the high frequency sub-band. Scrambling the positions can be for rows then columns, which will give strong security of the hiding process. The experimental results demonstrate the proposed method has achieved superior performance in terms of quantifiable measurement (PSNR and correlation) and in terms of visual quality. The proposed method propositions good imperceptible results and good response for against the various image attacks.

Keyword: Data Hiding, Haar Wavelet Transform, Histogram Modification, Scrambling, Correlation.

1. Introduction

The open environment in digital world has brought a new prospect for achieves the secret

Communication [1]. Information hiding has attracted lots of attention due to the proliferating use and exchange of digital media over the internet. Information hiding is a science of embedding information through digitally covered media and transmitted it's without leaving any notable trace, which leads to attention of eavesdroppers. The steganography via a digital cover of multimedia data is a good manner to provide protection of data [2]. The major requirements of Steganography system are perceptual imperceptibility, capacity and robustness [3].

Steganography methods can be categorized to spatial domain and frequency domain. The spatial field hides the confidential information through altering the LSBs for pixels in the cover image. The pixels can be take randomly or sequentially. The benefits of spatial field methods are simple implementation, high capacity but fail to prevent attacks and are easily detected. On the other hand, alternatively methods involve steganography in frequency domain. Different transforms such as DFT, DCT and DWT have been used for vary data hiding techniques. The transforms found numerous applications in image processing. This type of technique is more robust [4]. Additionally, this manner enhanced the problem which due to sensitivity and imperceptibility compared to the spatial domain [5].

Wavelet transform has the capability of converting images from spatial field into frequency field. Compared with DCT and DFT, the Wavelet transform has less intensive resource, so that arises less distortion in the image. There are varying filters that are available, but the Haar-DWT and the Daubechies-DWT are widely used [5]. Haar wavelet transform is precisely reversible without the edge effects problem that are acted in other wavelet transforms [6]. It analyzes the signal to different scales and frequency bands and decomposes the image into different images of the sub - band low-low (LL), low-high (LH), high-low (HL) and high-high (HH) [7]. The low frequency part has information of image close to the original image. The high frequency parts have information about edge components. This allows the steganography systems to use the high frequency sub-bands for embedding the secret data. Since the human eye is less sensitive, when changes in edges. These changes being unobserved by the human eye, the image becomes durable to penetrate compared to other methods [8].

In the paper [6]. Image steganography adopts different orthogonal and biorthogonal wavelet families. Using modified LSB method to embedded the secret message. The results showed that Haar wavelet is the better choice for image steganography based on modified LSB method. The proposed method is shown to be non-robust to Gaussian and Salt-n-Pepper noise. In [7]. Haar wavelet transform is used to decompose of the cover image. Data hiding is applied as text, encrypted the data by Advanced Encryption Standard (AES) algorithm before hiding it. The text can constitute the key from alphabetic words taking the length of 8 characters. In LL sub-band wavelet decomposed image, the Least Significant Bit (LSB) method of wavelet coefficients is changed with the encrypted text. The researcher in [9]. Using the Least Significant Bit (LSB) to hide secret message in image. Where the secret message was converted into binary and the image was divided to the original colors Red, Green and Blue (RGB). The blue sector was converted into binary, and then the hide process is implemented by means of hide two bits of secret message in two bits of least significant bits in the blue sector of the cover image. In [10]. Encoded the secret image by Huffman coding before hiding it. The cover image is decomposed by applying Haar wavelet transform. Huffman code is divided into 3-bits blocks that led to constitute a decimal value ranging from 0 to 7. Using Least Significant Bit (LSB) method, 3 bits of Huffman encoded bit stream is embedded into the 3 least significant bits for wavelet coefficients in the high frequency sub-bands. While in [11]. Huffman codding was applied to the secret data to provide a kind of security in addition to high capacity, which gives the possibility to compress the information before hidden in the cover. The pixels in the cover image were represented using Fibonacci decomposition that increased the system's durability.

In this paper, applied steganography system and study of the effectiveness of the Haar Wavelet Transform and histogram modification which were used in the hiding process. Histogram modification is used as a threshold for the secret image that manipulates the secret image from bright image to dark. Shrink histogram is used to achieve low contrast to secret image, then the low contrast values are shifted by slide histogram to the low end of the range which leads to provide a dark image. Thus the secret image becomes invisible.

This paper is ordered as follows: Section 2 defines Haar-wavelet Transform. Section 3 gives description of Histogram Modification. Section 4 describes the proposed method in detail. The experimental results are presented in section 5. Section 6 shows the conclusions.

2. Haar Wavlet Transform

The Wavelet transform is a mathematical method, has the capability to convert images from spatial domain into frequency domain. The low and high frequencies are extracted by passing the image through the high and low pass filters, respectively. Wavelet transforms analysis treaties with the signal and divides in to detail category and the category of approximations. It analyzes the signal to different scales and frequency bands. DWT applies two groups of function: scaling and wavelet that relate with high and low pass filters. The decomposition work by dividing time separation. In other word, in a signal only half of the samples are enough to be the whole signal that makes doubling the frequency separation [12].

In Haar Wavelet Transform, the low frequency wavelet coefficient is produced through compute the averaging of the two pixel values and high frequency coefficients are produced through taking half of the difference for the same two pixels. For two deamination images, WT decomposes the image into different sub – bands as resolution approximation band or low-low (LL) in addition to horizontal high-low (HL), vertical low-high (LH) and diagonal high-high (HH), detail components as shown in **Figure 1.** The important information of the spatial domain image (smooth parts) is existent in the low frequency wavelet coefficients (approximation band) and the edge and texture details typically be existent in the high frequency sub bands, such as LH, HL, and HH [10]. Haar wavelet transform is identical to its inverse, that is consider one important feature of it [12].

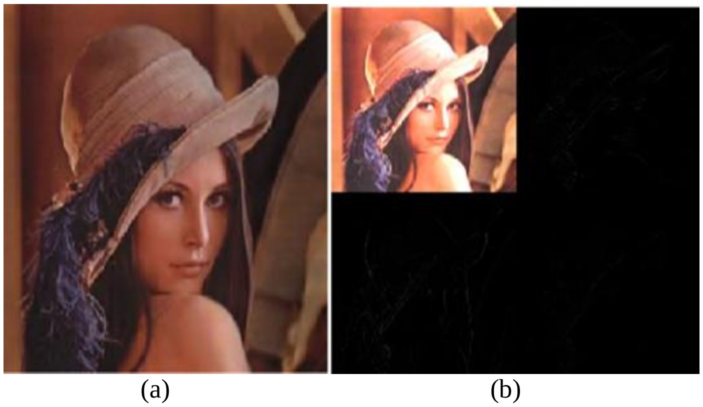


Figure 1. Shows a: the original image, b: the Lena image after one Level Decomposition of Haar wavelet.

3. Histogram Modification

Many image processing applications are concerned of Histogram techniques. The histogram has tool which is effective and useful not just to about quality of the image but considered also to modify the contrast and brightness of image [13].

It appears as an intensity distribution or probability density function. A histogram of the image can be modified as a result of mapping functions. The gray-scale modification is including two methods are histogram shrink and histogram stretch, sometimes denoted as histogram scaling.

The histogram shrink is used to decrease the contrast for image by compressing the gray levels. While the histogram stretch is a obverse of histogram shrink, which spread the histogram across the whole gray level range. That has the effect of increasing the contrast of a low contrast image. The mapping functions for a histogram shrink and histogram stretching can be represented as:

$$Shrink\big(I(r,c)\big) = \left[\frac{Shrink_{max} - Shrink_{min}}{I(r,c)_{max} - I(r,c)_{min}}\right]\left[I(r,c) - I(r,c)_{min}\right] + Shrink_{min} \qquad (1)$$

$$Streach\big(I(r,c)\big) = \left[\frac{(I(r,c) - I(r,c)_{min}}{I(r,c)_{max} - I(r,c)_{min}}\right]\ [MAX - MIN] + MIN \qquad (2)$$

Where Shrink $_{max}$ and Shrink $_{min}$ represent the maximum and minimum are chosen in the compressed histogram. Image has reduced contrast as result of this process.

$I(r,c)_{max}$ and $I(r,c)_{min}$ represent the largest and the smallest gray level value in the image respectively. The Max and MIN denote to maximum and minimum gray level values, probable (these are 0 and 255 for an 8-bit image).

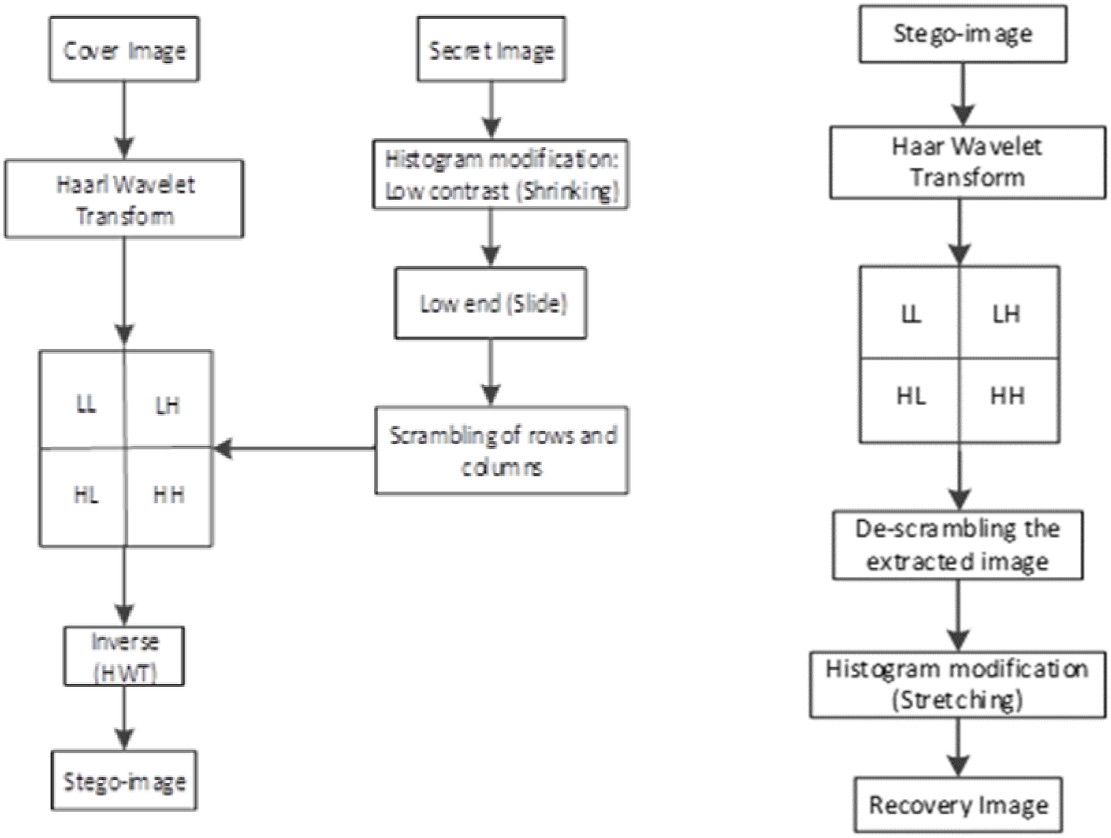
In histogram sliding techniques, the complete histogram of the image can be shifted to become either darker or lighter. Due to shifting of histogram to rightwards or leftwards, a clear change will be seen in the image. This can be done by addition or subtraction a fixed value for entirely the gray-level values. In this paper, the subtraction process was applied as follows:

$$Sd(r,c) = I(r,c) - offset \qquad (3)$$

Where *OFFSET* denote a fixed value to slide the histogram. In this calculation will create a darker image [14].

4. Proposed Image Steganography Algorithm

In this section, the proposed technique for steganography is presented.



(a): Embedding image

(b) : Extracting image

Figure 2. Illustrates the hiding and extracting steps of the Proposed method.

A-The Hiding Algorithm

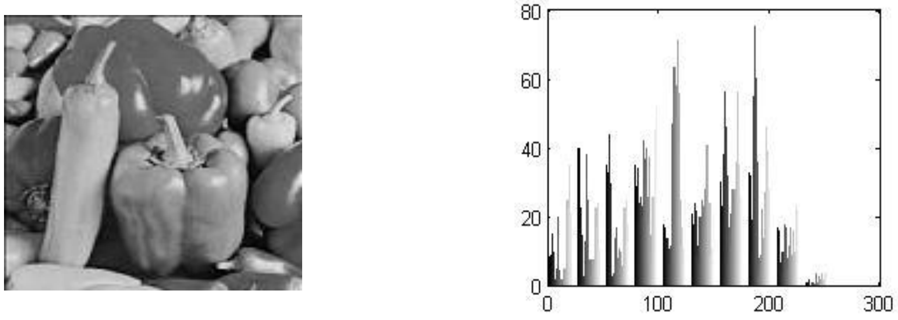
The steps of the hiding algorithm:

Input: Cover Image, Secret Image.
Output: Stego-image.
Step 1: Apply Haar Wavelet Transform to the cover image to get the decomposition sub-bands (LL, LH, HL, HH).
Step 2: Manipulate the secret image by histogram modification to scale the secret image and normalize its values, using mapping function of a histogram shrink via using various range of histogram such as (80-130), (90-120), (100-110). The next step is to apply histogram slide to shift the histogram range to low end region, where offset= shrink$_{min}$ to ensure the histogram doesn't extent low end (zero value), as in **Figure 3, 4.**
Step 3: Scrambling of rows positions then columns positions for the image obtained from step 2, as in **Figure 5.**
Step 4: Embed the Secret image in HH sub-band.
Step 5: Calculate inverse Haar wavelet transform for image obtained in step 4.

B- Extracting Algorithm

The algorithm involves from four steps as follows:

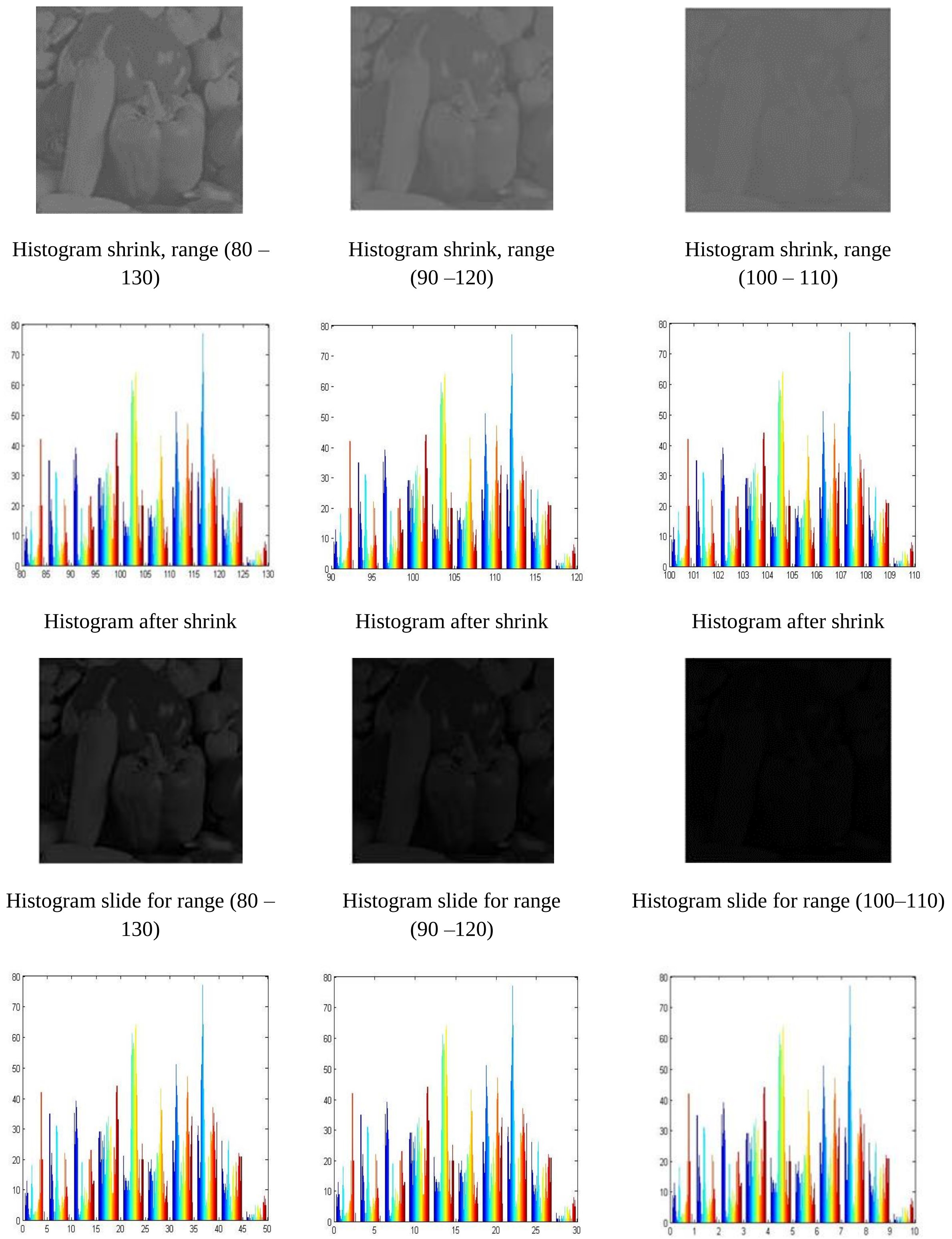
Input: Stego-Image.
Output: Recover Secret Image.
Step 1. Apply HWT for the stego-image to get the sub-bands (LL, LH, HL, HH).
Step 2. Extract secret image is hidden, which represent the scrambled secret image. Extract secret image from HH.
Step 3. De-scrambling the extracted image.
Step 4. Apply histogram stretch for the image of step3 to recover the secret image.



Original secret image

Histogram of original image

Figure 3. Shows the original secret image and histogram of it



Histogram shrink, range (80 – 130)

Histogram shrink, range (90 –120)

Histogram shrink, range (100 – 110)

Histogram after shrink

Histogram after shrink

Histogram after shrink

Histogram slide for range (80 – 130)

Histogram slide for range (90 –120)

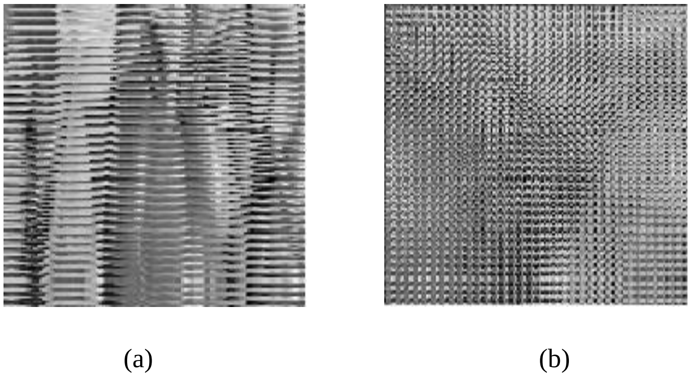
Histogram slide for range (100–110)

Histogram after slide Offset=80

Histogram after slide Offset=90

Histogram after slide Offset=100

Figure 4. Shows the steps of the histogram shrink and histogram slide for the secret image with different ranges.



(a) (b)

Figure 5. (a) Scrambling the rows of secret image, (b) Scrambling the columns of secret image.

4. Experimental Results

The proposed system is designed using Matlab 7.0 for programming. Three different images are used as secret image of size 128x128, Lena is employed as the cover-images of size 512x512, 8-bit gray-level images as shown in **Figure 6.** In this section, demonstrates the results and evaluate the efficiency of the hiding algorithm, PSNR and Correlation criteria are used to test images. PSNR is measured as:

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

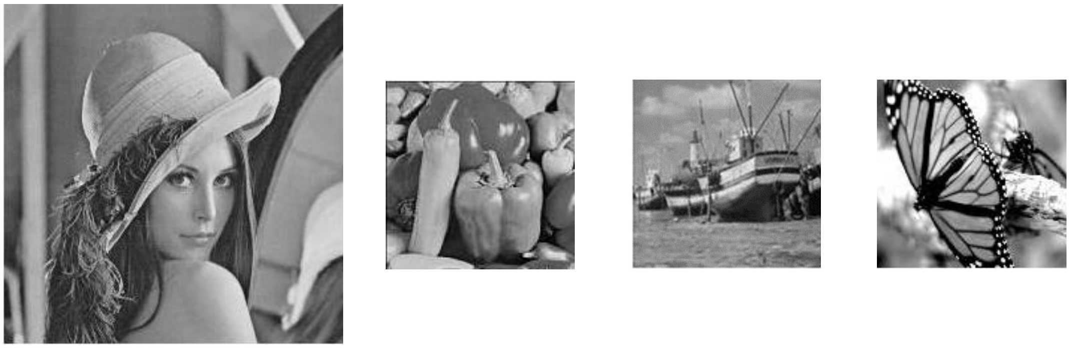
$$MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (L(x,y) - L'(x,y))^2 \quad (5)$$

Where M represents the number of rows and N is the number of columns. L (x, y) and L’(x, y) are the pixel values that denote for the cover and stego-image, respectively [15].

The correlation measures the extent of similarity between the original secret image and the recovered image and can be considered using the following equation:

$$Corr = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}} \quad (6)$$

Where x , y represents the secret image and recovered respectively. Correlation of about 0.7 or above is counted passable [16]. The maximum value of Correlation is 1 [17].



Cover image

Secret image: (a) Peppers, (b) Boat and (c) Butterfly

Figure 6. Show the cover image and secret images.

In this work, the efficiency of Haar Wavelet Transform in hiding process is studied. This algorithm devotes the HH sub-bands in the hiding process. The histogram modification is used as scale for secret image, the scale controls the quality of stego-image. That can be done through transform secret image from high contrast to low contrast as a result of shrink histogram, then the low contrast image is shifted to low end of range as a result of slide histogram. Finally, the secret image becomes invisible (dark image). The experimental results, including the secret image under different values ranges of histogram scaling (shrinking) which are (80 -130), (90 - 120) and (100 -110).

From the **Table 1.** It can be noted that the smaller range of histogram scaling (shrinking) for secret image can produce high visual quality of the stego-image. Since the changes made in the cover image is small. While the large range of histogram scaling (shrinking) that lead to more changes occur in cover image which lead to more distortion and the visual quality are reduced.

Table 1. Show the PSNR and Corr. with different ranges of histogram shrinking.

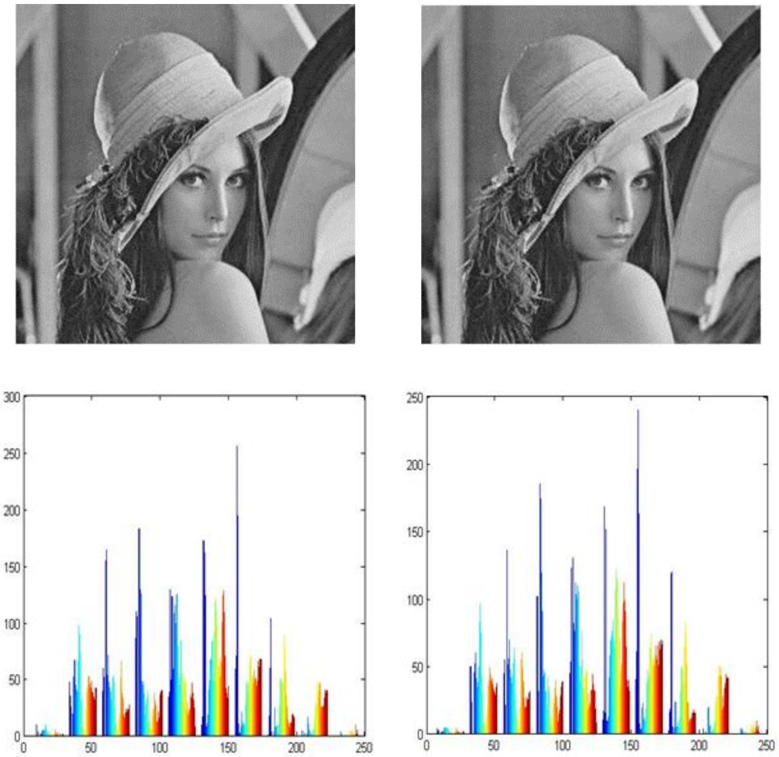
Histogram range (80 – 130)	Histogram range (90 –120)	Histogram range (100 –110)	secret image Recovery
PSNR= 25.0139 dB	PSNR= 28.9949 dB	PSNR= 35.0258 dB	Corr= 1
PSNR=25.1068 dB	PSNR= 29.0843 dB	PSNR=35.0781 dB	Corr= 1

PSNR= 24.3719 dB	PSNR= 28.4125 dB	PSNR= 34.7559 dB	Corr= 1

Histogram scaling provides less image distortion and detectability of stego-image. From the results, one can notice that best results are obtained from hiding secret image which has smaller range of histogram scaling. So that the stego-image has highest PSNR value that indicate good perceptibly. The PSNR of the stego-images for hiding process and Correlation of the recovered images shown in **Table 1.**

The haar wavelet transform at different range of histogram scaling (shrinking) was performed well, and can be noted that the results of PSNR has accepted values. Typically, the assortment of PSNR values between 20 - 40 to good quality image [18]. The average PSNR of this method for (100-110) range are found to be 34.9533 dB. On the other hand, the extracted image has correlation of 1 in comparison with the original secret image. That indicted the proposed algorithm is sufficiently secure.

Figure 7. Presents the histogram of stego-image and considered the image Peppers as secret image, and (100-110) as range of histogram scaling (shrinking), which provides the secret image in low contrast. It can be seen from **Figure 7 a,b.** the stego-image histogram is still having the same shape as the original one, so the stego-image quality still good even after the data embedding.



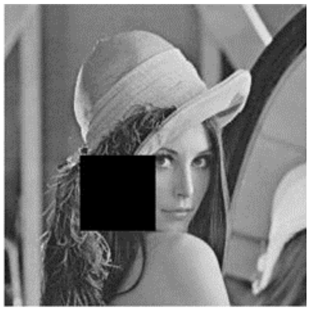
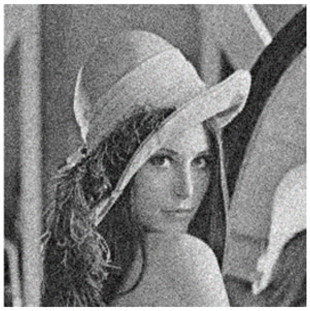
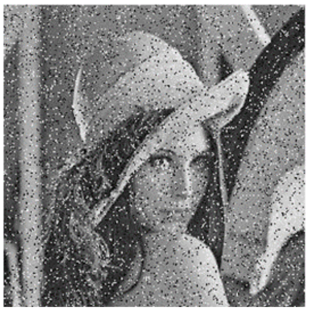
Histogram of the cover image

Histogram of the stego-image at range (100-110)

Figure 7. Show histogram for original Lena image and for stego-image at range (100-110).

Robustness of the steganography system is its ability to resist various attacks, such as geometrical distortion (cropping), JPEG compression, Gaussian noise [19]. And Salt & Pepper noise [20]. **Table 2.** Illustrations the results of attacks for the proposed method test.

Table 2. Show the PSNR and Corr. of the various attacks.

Crop 1/16 of image
PSNR=19.7725 dB
	JPEG compression,
	compression rate (50%)
	PSNR= 30.8742 dB
		PSNR=22.7959 dB,
		Gaussian noise Mean=0,
		variance =0.005
			PSNR= 15.5178 dB
			Salt & Pepper noise(0.1)

Corr=1

Corr=1

Corr=1

Corr=1

Crop 2/16 of image
PSNR=15.8465 dB

JPEG compression,
compression rate (40%)
PSNR= 29.8201 dB

PSNR=30.9097 dB,
Gaussian noise
Mean=0,variance=0.0005

PSNR= 22.2012 dB
Salt & Pepper noise(0.02)

Corr=1

Corr=1

Corr=1

Corr=1

Crop 3/16 of image
PSNR=13.7744 dB

JPEG compression,
compression rate (30%)
PSNR= 28.2021dB

PSNR=28.7628 dB,
Gaussian noise Mean=0,
variance =0.001

PSNR=30.9920 dB
Salt & Pepper noise(0.002)

Corr=1

Corr=1

Corr=1

Corr=1

When tested with various attack, the extracted image has correlation of 1. From results, the proposed method is found strong against various attacks.

Table 3. Illustrations the capacity, PSNR and Corr. of the proposed method in hiding at HH sub-band for Haar wavelet, for Lena test image as host with different capacity of secret images. The experimental results presented that the proposed method gives a good performance with a large amount of data hiding capacity in terms of PSNR.

Table 3. Show the capacity, PSNR, correlation from Lena stego-image.

Capacity of secret image in KB	PSNR	Corr.
3584	35.4219	1
3850.24	35.0781	1
4157.44	35.0258	1
5324.8	34.7559	1

5. Conclusions

This paper, proposed a new steganography algorithm which uses a threshold-based on histogram modification methods for data hiding. Histogram modification has been successfully implemented in Haar wavelet transform domain [19]. The histogram modification can be achieved to control the quality of steganography images when manipulated the secret image by transform the high contrast to low contrast, then low contrast is shifted to the low end. So that the secret image becomes invisible. Before hiding the secret image in the cover, scrambling process is applied to the positions of the rows and then columns which would give strength to the hiding process. So the secret image is difficult identify for someone he wants to attack. According to the experimental results, the PSNR is still an acceptable value even with high capacity of hidden secret image, it has been shown that in the stego-image is good quality and there is no any suspicion from existence of hidden secret data when compared with cover image. In addition, the obtained values for the correlation of the secret images were verified that the method of hiding the information obtained by the proposed method was sufficiently secure. From the results, it was confirmed the proposed method is highly strong for against the various attacks.

References

1. Rabie, T. Digital image steganography: An fft approach. In *International Conference on Networked Digital Technologies*.**2012,** 217-230.
2. Fouad, M.M. Enhancing the Imperceptibility of Image Steganography for Information Hiding. IEEE: CFP1785N-ART c, PTI, Proceedings of the *Federated Conference on Computer Science and Information Systems*, **2017**, *11*, 545–548, doi: 10.15439/2017F10.
3. Kasana, G.; Singh, K.; Bhatia, S. Data Hiding Algorithm for Images Using Discrete Wavelet Transform and Arnold Transform. KIPS, *Journal of Information Processing Systems*. **2017**, *13*, *5*, 1331-1344,
4. Cheddad, A.; Condell, J.; Curran, K.; Kevitt, P. M. Enhancing Steganography in Digital Images. *Canadian Conference on Computer and Robot Vision, IEEE*.**2008**, 326-332, doi: 10.1109/CRV.2008.54.
5. Atawneh, S.; Putra, S. An Overview of Frequency-based Digital Image Steganography. International *Journal of Cryptology Research*.**2015**, *5*, *2*, 15-27.
6. Azad, S. K.; Muttoo, S. Image Steganography Based on Wavelet Families. *Journal of Computer Engineering & Information Technology*, SciTechnol.**2013**, *2*, *2*, *2*.
7. Reddy, M.I.S.; Kumar, A.P.S. Secured Data Transmission Using Wavelet Based Steganography and Cryptography by Using AES Algorithm. Elsevier, International Conference on Computational Modeling and Security (CMS), *Procedia Computer Science*. **2016**, *85*, 62 – 69, doi: 10.1016/j.procs.2016.05.177.

8. Jiansheng, M.; Sukang, L.; Xiaomei, T. A Digital Watermarking Algorithm Based On DCT and DWT. Proceedings of *the 2009 International Symposium on Web Information Systems and Applications (WISA'2009)* Nanchang, P. R. China. **2009**, 104-107, Academy Publisher AP-PROC-CS-09CN001.
9. Hussein, L.H. Hiding Data in Color Image Using Least Significant Bits of Blue Sector. *Ibn Al-Haitham J. for Pure & Appl. Sci*. **2018**, *31*, *2*, 193-198, doi:10.30526/31.2.1948.
10. Nag, A.; Biswas, S.; Sarkar D.; Sarkar, P. A Novel Technique for Image Steganography Based on DWT and Huffman Encoding. International *Journal of Computer Science and Security (IJCSS)*. **2011**, *4*, *6*, 561-570.
11. Abu-Almash, F.S. New Steganography System Based on Huffman Coding and Fibonacci Decomposition. *Ibn Al-Haitham J. for Pure & Appl. Sci*.**2018**, *31*, *1*, 231-243.
12. Houssein , E.H.; Ali, M.A.S.; Hassanien, A.E. An Image Steganography Algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System. IEEE Proceedings of the *Federated Conference on Computer Science and Information Systems*. **016**, *8*, 641–644, doi: 10.15439/2016F521.
13. Sridhar, S. Digital Image Processing; Oxford University Press, **2011**.
14. Umbaugh, S.E. Computer Vision and Image Processing; Prentice hall, **1998**.
15. Juneja, M.; Sandhu, P. S. A New Approach for Information Security using an Improved Steganography Technique. KIPS, *J Inf Process Syst (JIPS)*. **2013**, *9*, *3*, 405 – 424.
16. Pan, J.S.; Huang, H.C.; Jain, L.C. *Intelligent Watermarking Techniques*. World Scientific Publishing Co. Pte. Ltd, **2004**.
17. Swain, G.; Lenka, S. K. Classification of Image Steganography Techniques in Spatial Domain: A Study. International *Journal of Computer Science & Engineering Technology (IJCSET)*. **2014**, *5*, *03*, 219 – 232, ISSN: 2229-3345.
18. Salomon, D. Data Compression. The complete reference, Fourth Edition; Springer- Verlag London Limited, **2007**.
19. Tawfiq, L.N.M.; Hussein, A.A.T. Design feed forward neural network to solve singular boundary value problems. *ISRN Applied Mathematics*. **2013**, *2013*, 1-8.
20. Tawfiq, L.N.M. Using collocation neural network to solve Eigenvalue problems. *MJ Journal on Applied Mathematics*.**2016**, *1*, *1*, 1-8.