PAPER • **OPEN ACCESS**

Image Steganography using Dynamic Threshold based on Discrete Cosine Transform

To cite this article: Namar A Taha *et al* 2021 *J. Phys.: Conf. Ser.* **1879** 022087

View the article online for updates and enhancements.

You may also like

- Comparison of Least Significant Bit, Pixel Value Differencing, and Modulus Function on Steganography to Measure Image Quality, Storage Capacity, and Robustness
D Darwis, N B Pamungkas and Wamiliana
- Improvement of Image Steganography Scheme Based on LSB Value with Two Control Random Parameters and Multi-level Encryption
Mohammed Hashim Mahdi, Ali Abdulwahhab Abdulrazzaq, Mohd Shafry Mohd Rahim et al.
- Based on IoT Healthcare Application for Medical Data Authentication: Towards A New Secure Framework Using Steganography
Mohammed Mahdi Hashim, Suhad Hasan Rhaif, Ali A. Abdulrazzaq et al.

244th Electrochemical Society Meeting
October 8 – 12, 2023 • Gothenburg, Sweden
50 symposia in electrochemistry & solid state science
Deadline Extended!
Last chance to submit!
New deadline: April 21
submit your abstract!

This content was downloaded from IP address 37.238.109.21 on 19/04/2023 at 12:16

Image Steganography using Dynamic Threshold based on Discrete Cosine Transform

Namar A Taha, Amna Al Saffar, Alaa A Abdullatif and Firas A Abdullatif

University of Baghdad, College of Education for Pure Science-Ibn Al-Haitham, Computer Science Department

E-mail: namar.t@ihcoedu.uobaghdad.edu.iq

Abstract. The art of preventing the detection of hidden information messages is the way that steganography work. Several algorithms have been proposed for steganographic techniques. A major portion of these algorithms is specified for image steganography because the image has a high level of redundancy. This paper proposed an image steganography technique using a dynamic threshold produced by the discrete cosine coefficient. After dividing the green and blue channel of the cover image into 1*3-pixel blocks, check if any bits of green channel block less or equal to threshold then start to store the secret bits in blue channel block, and to increase the security not all bits in the chosen block used to store the secret bits. Firstly, store in the center of the block and then store another bit in the write or left bit depended on differences between them.
The proposed method was applied to many color images and many measurement terms used to show the efficiency of it. The experiment result showed good result that the PSNR = 53.76, MSE = 0.273, SSIM= 0.999, with embedding rates 0.55

Key Words: Steganography, DCT, and Least Significant Bit (LSB)

1. Introduction

Steganography is the technique of covered writing [1] it tends to hide the digital message with the digital data of different carriers' media, the carrier's media may be audio, image, movie, etc. [2,3]. For hiding secret information inside an image, several algorithms have been proposed. The main important element used in image steganography is carrier image also known as cover-image; it is the media to hide the secret information by using some embedding algorithms. Embedding algorithm: it is combining the cover image with the secret information. Stego -image: it is the image obtained after embedding the secret message that is the goal of the image steganography technique. The two images (the stego -image and cover image) must have the same quality and without distorting the quality of the cover image [4].

Steganography techniques can be done into two types of domains: spatial and frequency domain. In the spatial domain technique, the secret information is embedded directly in pixels of the image. Where in the frequency domain also known as the transform domain, the image is transformed, and then the secret information is embedded in it [5].

The most common and simplest steganography method is the Least Significant Bit. It is a spatial domain substitution process where the secret message is hidden in the least significant bit pixels of the

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

cover image [6]. Various algorithms for steganography hide a large number of secret information in the first least significant bits of the cover-image pixels. Because the sensitivity of the human visual system is very weak, the Presence of the hidden secret information unable to be noticed [7]. If the message is simply hidden in the least significant bits of the Sequential pixels, it can be easily destroyed by filtering, compression, or a less than size transmutation to get the original hidden message. So, this technique must be modified and combined with another transform to resist any stego-analysis methods [8] transformation technique based on the covert the cover image from the spatial domain into frequency coefficients by manipulation of the orthogonal transform of the image through using different transformation techniques like Discrete Cosine Transformation DCT [9].

This paper proposed a method that combines the Least Significant Bit (LSB) and Discrete Cosine Transform (DCT). This is done by separate the color image into RGB channels and then applying DCT transform on the green channel to find the dynamic threshold by using the DCT coefficient. The dynamic threshold used to select the block to hide text data in the blue channel based on the absolute differences between the value on the pixels in the block, The pixels in the block of cover image satisfying the threshold condition are not in Sequential locations makes this proposed method stronger and secured. The rest of the research is ordered as follows; Section 2 illustrated the discrete cosine transform with its general equation. Section 3 described the proposed algorithm with its block diagram, performance measurement explained in Section 4 and the corresponding simulations and discussions are done in section5. Finally, the conclusion of the paper was given in section 6.

2. Discrete Cosine Transform (DCT)

For image and signal processing DCT is orthogonally transformed with many advantages such as little in bit error rate and high compression ratio with good in both synthetic effects of calculation complexity and information integration ability. It broke the image into three frequency bands the low, high, and mid as in Fig1 [8,9].

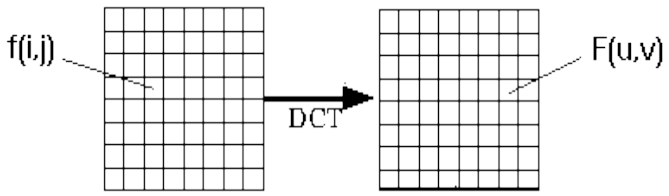


Fig 1. The DCT transform of An Image

The one-dimension DCT equation (k data items) is:

$$F(u)=\alpha(u)\sum_{x=0}^{k-1} f(x)cos\left[\frac{(2x+1)u\pi}{2k}\right] \qquad (1)$$

for u = 0, 1, 2, . . . , K-1.

The two-dimension DCT equation (k by L image) is [10]:

$$F(u,v)=\alpha(u)a(v)\sum_{x=0}^{k-1}\sum_{y=0}^{K-1} f(x,y)\cos\left[\frac{(2x+1)u\pi}{2K}\right]cos\left[\frac{(2y+1)u\pi}{2K}\right] \qquad (2)$$

for u,v = 0, 1, 2, . . . , K-1 Here, the input image is of size K × L. The pixel intensity is f(i, j); and DCT coefficient is F(u,v).

Broken the image into 8 by 8 blocks pixels and applying DCT to each block Through working left to right, top to bottom is how to used DCT in steganography [11].

3. Proposed algorithm

The proposed algorithm used the discrete cosine transform on the cover image. The DCT transform was applied on the green of the color cover image, calculate the threshold for each row, divide the blue channel and green channel into non overlapping block 1*3 and then check if any bits of green channel block less or equal to threshold then store one of the secret bits in center of blue channel block and the other in right or left according to the differences between the pixels. This way is ensuring secret bits is non embedding in consecutive pixels, which increase the security. Final step in the proposed method applied inverse DCT transform on green channel and combined it with blue channel after embedding and red channel to get the stego- image as shown in Fig 2 and explain the hiding for two bit of secret text in example as shown in Fig 3.

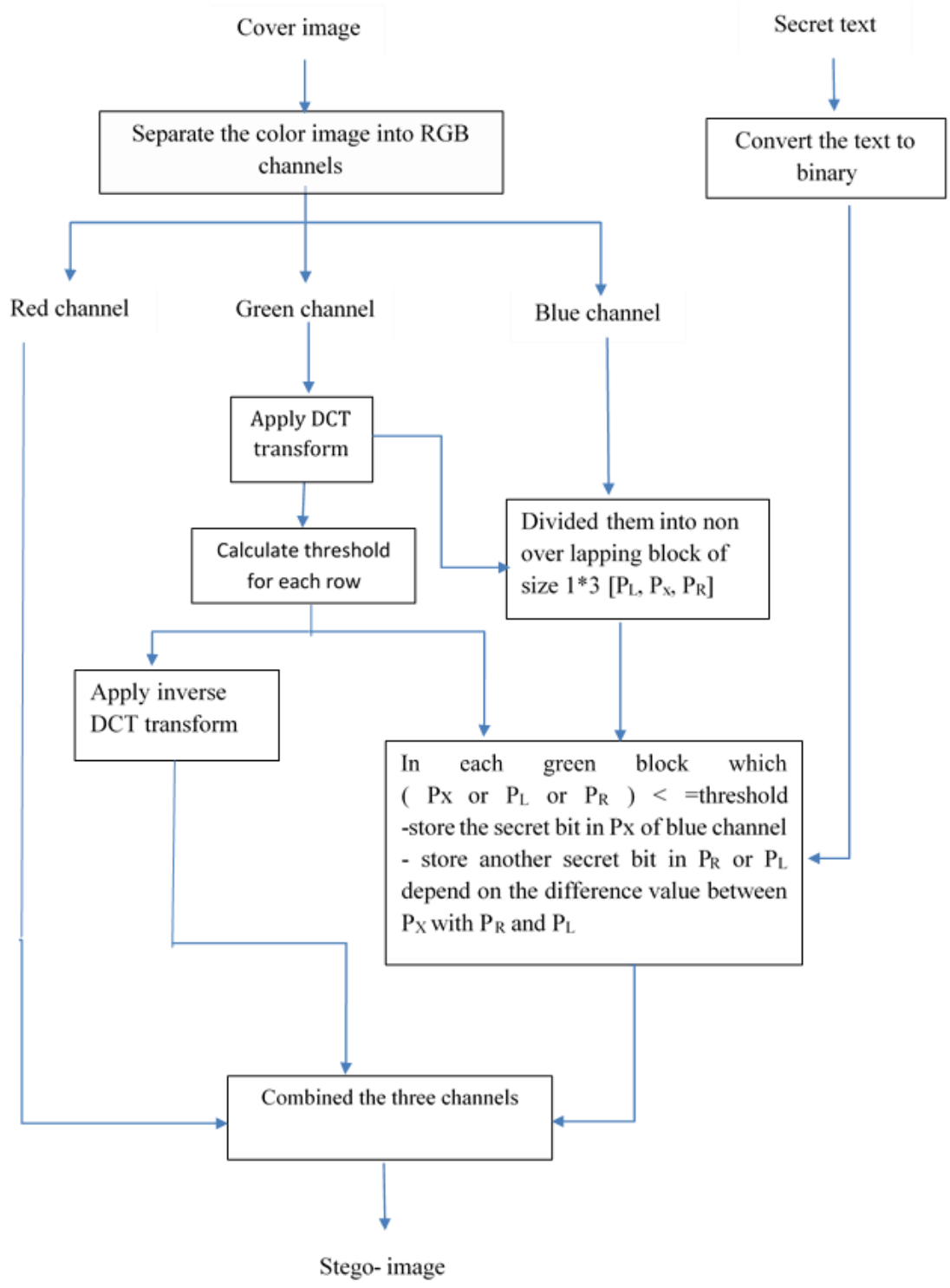


Fig 2. The main block diagram of the proposed method

An embedded and extracts algorithm are shown in 3.1 & 3.2

3.1. Embedded data process

The embedding algorithm

Input: color image with the size [M x N], secret text.

Output: stego_image.

Begin

Step 1: Read the color image and separate it into three channels R, G, and B.
Step 2: Apply DCT transform on G channel.
Step3: Calculate the dynamic threshold by the following equation (3) $\mathrm{Ti} = 1/(N-1)\sum_{j=1}^{N-1} |(\mathrm{Ci,j} - \mathrm{Ci,j+1})|$, i= 1 to M (3)
Where
$C_{i,j}$ is the DCT coefficient in i row, j column
Step 4: Apply inverse DCT on G channel
Step 5: Divide B and G channels into non overlapping blocks of size 1 x 3, P_L, P_X, and P_R.
Step 6: Convert the secret text into binary bits.
Step 7: i=1, L=1
While (i≤ M and L≤ length of secret bits) do
j=1 // the counter of blocks in each row
While (j≤ N/3 and L≤ length of secret bits) do
If (P_L, P_X, and P_R) in block [i, j] in G channel ≤ Ti then
- Store secret bit in LSB of P_X in block [i, j] in B channel
- If $|(P_X - P_L)| \geq |(P_X - P_R)|$ of B channel
- store another secret bit in LSB of P_R
Else
- store another secret bit in LSB of P_L
L= L+2;
End //
- j= j+1
End // end of j
i=i+1
End // end of i
Step 8: Reconstruct the stego-image by combination the three-color channels of the image to produce stego-image
End.

3.2. Extraction Secret text process, the extracting algorithm

Input: stego_image
Output: secret text
Begin
Step 1: Read the color image and separate it into three channels R, G, and B.
Step 2: Apply DCT transform on G channel.
Step3: Calculate the dynamic threshold by using eq. (3)
Step 4: Divide G and B channel into non overlapping block of size 1 x 3, P_L, P_X, and P_R.
Step 5: i=1, L=1
While (I ≤ M) do
j=1 // the counter of blocks in each row
While (j ≤ N/3) do
If (P_L, P_X, and P_R) in block [i, j] of G channel ≤ Ti then
- extract secret bit from LSB of P_X in block [i, j] of B channel
- If $|(P_X - P_L)| \geq |(P_X - P_R)|$ of B channel
- extract another secret bit in LSB of P_R
Else
- extract another secret bit in LSB of P_L
End //
j= j+1
End // end of j
i=i+1
End // end of i

Step 6: Convert the extracted bits to Ascii then to text
End

An Implementation example for the proposed algorithm is as follows:
After applying DCT on the green channel and calculate the dynamic threshold for each row, divide the blue and green channel into non overlapping blocks of size 1 x 3, (P_L, P_X, and P_R).
Suppose the threshold of row **i** in green channel = 151
If any pixel (P_L or P_X or P_R) in the block (i, j) of green channel < =151

Store secret bit in LSB of P_X in the block (i, j) of blue channel

Calculate the difference between the center pixel and the right, left pixels in block (i, j) of blue channel

$|Px-P_L|= |165-170| =5$

$| Px-P_R|=|165-162|= 3$

$$| (P_X - P_L) | \geq | (P_X - P_R) | \qquad (4)$$

Store another secret bit in LSB of P_R of blue channel.

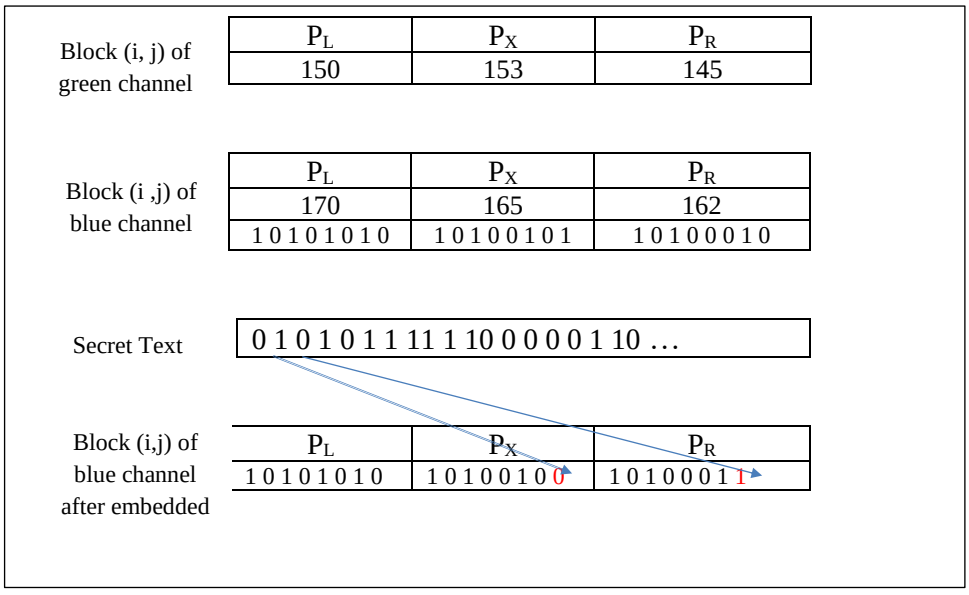


Fig 3. shows the blocks of the green and blue channel of the implemented example.

4. Performance measurement

The digital quality of an image can be calculated by using many parameters to measure the performance of the proposing method:

4.1. *Peak Signal to Noise Ratio (PSNR)*

The peak signal-to-noise ratio between two images is computed using PSNR the ratio is used to measure the quality between the cover-image and a stego- image. When PSNR is high, good quality of stego-image is obtained. (MSE) mean square error represents the differences between the pixels of two images (cover image (CI) and stego-image (SI)). The PSNR equation is [13,14].

$$\text{PSNR}= 10\ \text{Log10}\ \frac{\text{RI}^2}{\text{MSE}} \qquad (5)$$

$$\text{MSE} = \frac{1}{\text{mn}}\sum_{\text{k=1}}^{\text{m}}\sum_{\text{l=1}}^{\text{n}}[\text{CI(k,l)} - \text{SI(k,l)}]2 \qquad (6)$$

Where *m* and *n* are representing the image size, RI is the maximum value of the image's pixels.

4.2. *Structural Similarity Index Measure (SSIM)*

SSIM is an improvement method of the classical PSNR & MSE methods which is used to determine the resemblance between two images. [0,1] is the range value of the SSIM index. If the index is high then it means more similarity of two images (cover image (CI), and stego-image (SI)), and it's calculated as the follows:

$$SSIM\ (x_1,y_1)=\frac{(2\mu_{x1}\mu_{y1}+c_1)(2\sigma_{x1y1}+c_2)}{(\mu_{x1}^2+\mu_{y1}^2+c_1)(\sigma_{x1}^2+\sigma_{y1}^2+c_2)} \qquad (7)$$

Where x_1 and y_1 are two windows of common size, μ_{x1} is the average of $x1$, μ_{y1} is the average of y_1, $\sigma x_1{}^2$ is the variance of x_1, $\sigma y_1{}^2$ is the variance of y_1 and $\sigma x_1 y_1$ is the covariance of x_1 and y_1 [15].

4.3. *Image histogram*

One of the important criteria of security analysis is histogram. The security for the encrypt message is more guaranteed as the histogram of the image being is more uniform [16]. The x axis and y axis of the histogram graph explains the pixel difference between each pair and the number of occurrences, respectively. Comparing the histogram of cover and the stego-image to monitor unusual shapes as a result of an embedding algorithm or to identify pixels distribution, it is considered as one of the effective experiments of a stego-image identify the pixels distribution [17, 18].

5. Results and Discussion

The proposed algorithm was implemented and tested on several standard images. The cover images with the size (256 × 256) color – scale are used such as (a) Lena, (b) Baboon, (c) pepper, (d) monarch, (e) sails and (f) tulips as shown in Fig. 4. Fig 5 shows the stego image after embedding 36000 secret bits with embedded rate ER =0.55.

Many metrics are used to measure the performance of proposed method such as PSNR, MSE and SSIM and the result shown in table -1, High value of PSNR indicates good perceptual quality of stego-image and the high value of SSIM indicate that have more similarity between cover image and stego-image

(a) (b) (c)

(d) (e) (f)

Figure 4. The cover image (a) Lena, (b) Baboon, (c)pepper, (d) monarch, (e) sails and (f) tulips

(a) (b) (c)

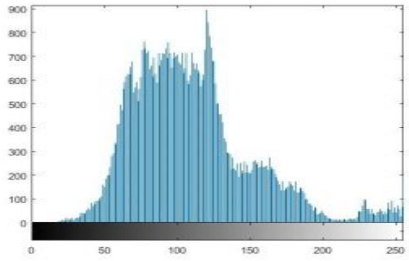
(d) (e) (f)

Figure 5. the stego-images (a) Lena, (b) Baboon, (c)pepper, (d) monarch, (e) sails and (f) tulips

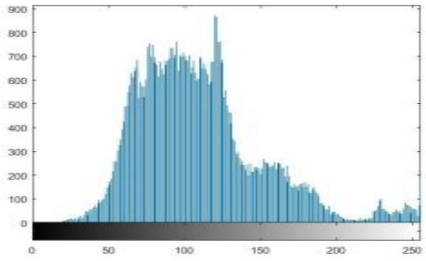
Table 1. PSNR, MSE and SSIM values for different cover images

Image	PSNR	MSE	SSIM
Lena	53.750	0.274	0.998
Pepper	53.764	0.273	0.998
Baboon	53.730	0.275	0.999
Monarch	53.720	0.276	0.997
Sails	53.770	0.272	0.999
Tulips	53.731	0.275	0.999

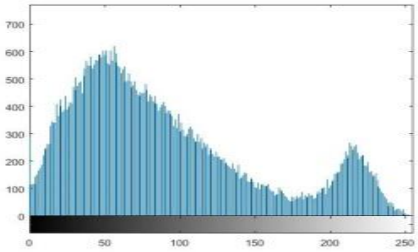
The histogram for the blue channel to the cover images and the stego images are shown in Fig. 6. It can be seen the high correlation between cover and stego- images.



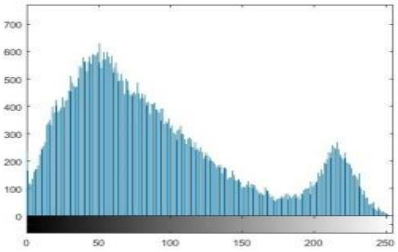
(a)



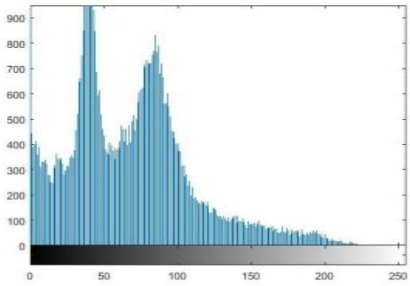
(b)



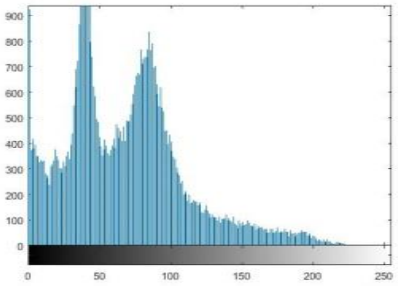
(c)



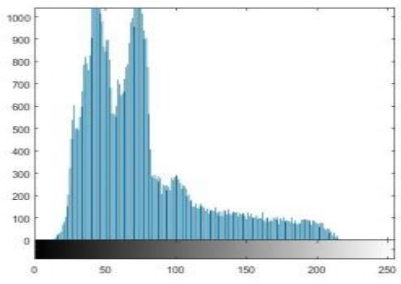
(d)



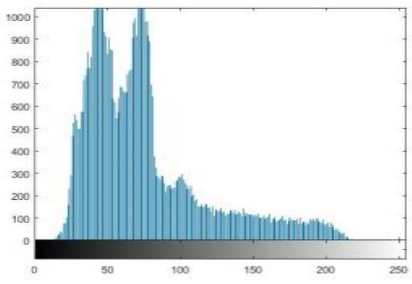
(e)



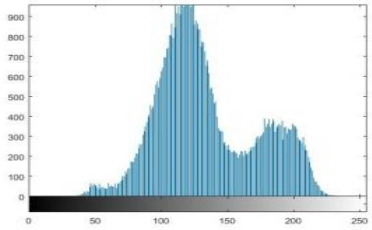
(f)



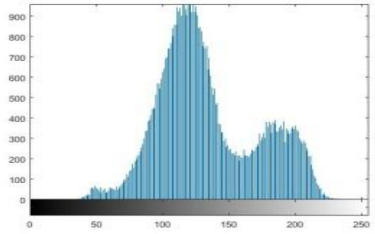
(g)



(h)



(i)



(j)

(k) (l)

Figure 6. histogram for cover and stego images: (a) Cover Lena image, (b) Stego -Lena image, (c) Cover Baboon image, (d) Stego -Baboon image , (e) cover pepper image (f) stego- pepper image, (g) cover monarch image (h) stego -monarch image , (i) cover sails image (j) stego -sails image (k) cover tulips image, and (l) stego -tulips image

6. Conclusion

To increase the security in the steganography methods, the process of hiding the secret bits must not in a consecutive manner. In this proposed method the dynamic threshold was produced based on DCT coefficient in the green channel of the cover. The blue channel was divided into blocks of size 1*3. The block is selected to hide the secret data depend on the dynamic threshold. Two pixels only in each selected block were used to hide the secret bit to increase the security, these two pixels are the center pixel in the block and the right or left pixel of the center. The proposed method maintained good result depend on the high value of PSNR and SSIM

Reference

[1] B. Della T. Jitha A. Gisny G. Elsa R. Neenu 2015 A Novel DWT based Image Securing Method using Steganography *Procedia Computer Science* **Vol.46** pp. 612 – 618
[2] H. Nagham Y. Abid R. Ahmad M. Osamah 2012 Image Steganography Techniques: An Overview *(IJCSS)* **Vol.6** : Issue (3) pp. 168-187
[3] A. Firas, A. Alaa, A. Amna 2018 Hiding Techniques for Dynamic Encryption Text based on Corner Point *Journal of Physics* **Conf. Series 1003**
[4] M. Mohammed S. Mohd A. Fadil S. Mustafa S. Hassan 2018 Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats *International Journal of Engineering & Technology* **Vol.7** (4) pp. 3505-3514
[5] Parul Manju R. Harish 2014 Optimized Image Steganography using Discrete Wavelet Transform (DWT) *IJRDET* **Vol.2** Issue 2
[6] M. Oudah A. Abed R. Khudhair S. Kaleefah 2020 Improvement Of Image Steganography Using Discrete Wavelet Transform *Engineering and Technology Journal* **Vol.38** Part A No.1 pp. 83-87
[7] A. Khalid K. Ahlam, F. Iyad 2017 A New Steganographic Algorithm Based on Multi Directional PVD and Modified LSB *ITC*, **Vol.46** (1) pp. 16-36
[8] D. Ajit A. Preethi 2010 Randomized Embedding Scheme Based on DCT Coefficients for Image Steganography *IJCA* Special Issue on **RTIPPR (2)** pp.97-103
[9] K. Manal N. Aqeela S. Rula M. Saad 2020 Improvement of Image Steganography using Discrete Wavelet Transform *Engineering and Technology Journal* **Vol. 38** Part A No. 1 pp. 83-87

[10] W. Ekta J. Payal Navdeep 2010 An Analysis of LSB & DCT based Steganography *Global Journal of Computer Science and Technology* **Vol. 10** Issue 1 (Ver 1.0) pp.4-8
[11] B. Kaur A. Kaur , J. Singh 2011 Steganographic Approach For Hiding Image In DCT Domain *IJAET* **Vol.1** Issue 3 pp.72-78
[12] A. Amna, 2011 Proposed Steganography Method Based on DCT Coefficients *IHJPAS* **Vol.24**
[13] A. Firas A. Alaa A. Namar 2020 Data Hiding Using Integer Lifting Wavelet Transform And DNA Computing *Periodicals of Engineering and Natural Sciences* **Vol.8** No.1 pp.58-66
[14] S. Ali M. Ali L. Abd Z. Qudr S. Ali 2019 PDA : A Private Domains Approach for Improved msb Steganography Image *Period. Eng. Nat. Sci.* **vol.7** no. 3 pp. 1405–1411
[15] A. Bovik Z. Wang H. Sheikh 2005 Structural Similarity Based Image Quality Assessment. Digital Video Image Quality and Perceptual Coding *Series in Signal Processing and Communications* chap. 7
[16] M. Melika B.Reza 2014 CVC: Chaotic Visual Cryptography to Enhance Steganography *DOI: 10.1109* **ISCISC.2014.6994020** pp.44-48
[17] M. Mohammed S. Mohd A. Fadil S. Mustafa S. Hassan 2018 Performance Evaluation Measurement Of Image Steganography Techniques With Analysis Of LSB Based on Variation Image Formats *International Journal of Engineering & Technolog* **Vol.7** pp.3505-3514.
[18] T. A. Al-asadi and A. J. Obaid, "Object detection and recognition by using enhanced speeded up robust feature," International Journal of Computer Science and Network Security (IJCSNS), vol. 16, no. 4, pp. 66-71, 2016.