IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 1, Ver. I (Jan.- Feb. 2018), PP 47-52
www.iosrjournals.org

Comparison study between LSB and DCT Based Steganography

AlaaAbdulhusseinDaleh Al-magsoosi
College of Education,Wasit University, wasit, Iraq.
Corresponding Author: adleah@uowasit.edu.iq

Abstract : *Information security is one of the most interested topic in computer science filed.is art of hiding data in cover media like audio, image ,etc . In this paper I will focus on two different methods hiding based on least significant bit and discrete cosine transform and compare between the result based on some measurement that calculated MSE , PSNR and SSIM. And based on those factors the result of hiding based on DCT achieve result better than LSB as shown MSE of LSB =16.1722 when hide 3 bits, PSNR of LSB =36.0771 and SSIM of LSB=0.9872 compare with Discrete Cosine transform MSE of DCT =7.981when hide 3 bits, PSNR of DCT =41.001and SSIM of DCT =0.901 as shown above the result of` hiding based on DCT is better than LSB.*
Keyword-*DCT, LSB,security, steganography and hiding*

I. Introduction

Information security is one of the most important topic in Computer Science and Network communication. And Because of the growing of modern communication in last years that need a special means of security especially in computer network and cloud services, the network security is becoming more important as the number of data being exchanged of data and information through Internet increases [1]. Therefore, the confidentiality and data integrity are required to protect data against unauthorized access. one of the ways that used to secure data is a steganography is an art of hiding secret message or information into cover-media or another message without letting anyone know about presence of secret message except the intended receiver. Data privacy issues can appear from a wide range of sources such as companies' records, criminal justice investigations and proceedings, bank system and transactions, military information. Information security or information privacy has become increasingly important as more systems are connected to the Internet. There are information privacy laws that cover the protection of data or information on private individuals from intentional or unintentional disclosure or misuse. Thus, steganography system used to hide data in a kind of form such as within videos or an image is vital in order to make sure that security or privacy of the important Data or information is protected [2]. This research concentrates on using two algorithms to hide the data inside images using steganography technique and compare between them. In this paper will used optimal LSB and DCT to hide a secret image into cover image. And analysis the two techniques.

II. MethodsOf Hiding Data In Digital Image

There are many techniques that used to hide data into image or any other multimedia, and the most popular is a LSB based Steganography.in this section optimal LSB and DCT have been consider as steganography techniques.

a. Optimal LSB

Least Significant bit based hiding (steganography) is one of stenographic technique used to insert secret data into Least Significant bit of cover data [3], when images used as a cover data, the secret information can be hide into LSB of each pixel of cover image. Hiding in LSB location can be detected easily for example can be reset all LSB location and destroy the message or secret data so the biggest challenge is to find the optimal LSB place to be used for hiding and how to protect it from the hackers. Assume 250 is a secret data and want to hide it into image,250 equal to: 11111010 in binary digit form, so it's need eight locations to insert each binary digit with LSB of cover data.

b. Discrete Cosine Transform DCT

The Discrete Cosine Transform (DCT) is a way to transform the image from spatial to frequency domain [2]. It split the image into sub-bands with 8*8 sub-block with respect to its visual quality, i.e. high, middle and low frequency components. In DCT based techniques, DCT coefficients are obtained for the given input image [2]. The secret information is inserted in the image of DCT coefficients in the place of block that value's is lower than the threshold value. To avoid visual detection and distortion.

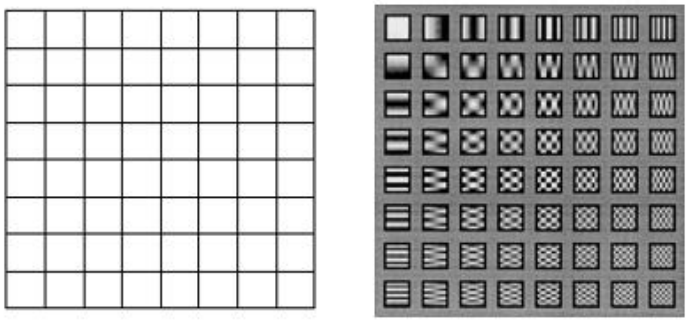

Figure1 Discrete Cosine Transform of an Image

The general equation for a 2D (*N* by *M* image) DCT is defined by the following equation:

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad \ldots.1$$

for u,v = 0, 1, 2, . . . , N-1 Here, the input image is of size N X M. c(i, j) is the intensity of the picture element in row i and column j; C(u,v) is the Discreet Cosine Transform coefficient in row u and column v of the DCT matrix. Signal energy lies at low frequency in image; it appears in the upper left corner of the DCT [2]. Compression can be achieved since the lower right values represent higher frequencies, and generally small enough to be neglected with little visible distortion. DCT is used in steganography as- Image is split into 8×8 blocks of pixels. Working from left to right, top to bottom, the DCT is applied to each block. Each block is compressed through standard quantization table as show in table number 1 to scale the DCT coefficients and message is inserted in DCT coefficients as a secret message.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Table1standard quantization table

2- Proposal Algorithms

In this paper will discuss two methods or algorithm of steganography: Least Significant bit and Discrete Cosine transform based on hiding technique.

A. Least Significant bit

The first algorithm that has been used in this paper is LSB to embedded secret data (image) into cover image.
Step 1: Read the cover image and secret image which is to be hidden in the cover image.
Step2: Select the lowest entropy layer (Red, Green and Blue) of the cover image to be used as a cover data.
Step 2: Convert secret image into stream of binary digit.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: Replace the first two location from LSB of cover image within each two bits of secret image one by one.
Step 5: Write stego image.
And to retrieve the secret image from the stego image used the following Algorithm steps:
Step 1: Read the stego image and collocate the length of bits stream of secret image from the first locations of the lowest entropy band of the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert each 8 bit into pixel value.

Step 4: re-write the secret image.

B. Discrete Cosine transform

DCT based steganography is the second technique that has been used in this paper to embedded secret image into cover image and the following steps show the algorithm of hiding:

Step 1: Read cover image.

Step 2: Read secret image and convert it to stream of binary.

Step 3: The cover image is split into 8×8 block of pixels and apply two dimension DCT to each block.

Step 6: from left to right, top to button of cover image, each block is compressed through standard quantization table.

Step 7: select the optimal location of DCT's coefficient to hide the secret data "in the result section will show the optimal position".

Step 8: apply inverse DCT to each block and collect together as one image.

Step 9: Write stego image.

Algorithm to retrieve the secret image:-

Step 1: Read stego image.

Step 2: Stego image is broken into 8×8 block of pixels and applied DCT to each block.

Step 5: Each block is compressed through standard quantization table.

Step 6: extract the value of a secret image from known location of DCT's coefficient

Step 7: Retrieve and convert each 8 bit into one pixel of a secret image.

And all work from left to right from top to button.

3- Image quality Assessment

There are many techniques and ways that used for check the quality of the image and in this work paper selected Mean Square Error, PSNR and SSIM for Assessment the quality of the reconstructed image after hiding process.

4-1 MSE (Mean Square Error)

The mean squared error (MSE) of an estimator is one of many ways to quantify the difference between values implied by an estimator and the true values of the quantity being estimated. MSE measures the average of the squares of the "errors [3][4]." The error is the amount by which the value implied by the estimator differs from the quantity to be estimated. The difference occurs because of randomness or because the estimator doesn't account for information that could produce a more accurate estimate.

$$\text{MSE} = \frac{1}{\text{M}*\text{N}} \sum_{\text{i}=1}^{\text{M}} \sum_{\text{j}=1}^{\text{N}} [\text{x}(\text{i},\text{j}) - \text{y}(\text{i},\text{j})]^2 \quad \text{…. Equation 1}$$

Where

M, N: size of the image

X(i ,j):original image

Y(i,j):result image

4-2 PSNR (Peak Signal in Noise Ratio)

Peak signal-to-noise ratio is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale [4][5].The PSNR is most commonly used as a measure of quality of reconstruction image. The signal in this case is the original data, and the noise is the error introduced by any modification on image like steganography or compression. When comparing cover images data before and after hiding it is used as an approximation to human perception of reconstruction quality, therefore in some cases one reconstruction may appear to be closer to the original than another, even though it has a lower PSNR (a higher PSNR would normally indicate that the reconstruction is of higher quality)[6]. One has to be extremely careful with the range of validity of this metric; it is only exclusively valid when it is used to compare results from the same codec (or codec type) and same content.

$$\text{PSNR} = 10 * \log_{10}(\frac{255^2}{\text{MSE}}) \quad \text{…. Equation 2}$$

4-3 The structural similarity (SSIM)

The Structural Similarity (SSIM) index is a method for measuring the similarity between two images. The SSIM index can be viewed as a quality measure of one of the images being compared, provided the other image is regarded as of perfect quality. And because there are many limitation of MSE as an image quality assessment like different image quality but have same MSE value, Wang et al proposed a more intelligent solution to the problem of image quality assessment the SSIM index has been shown to outperform MSE and the related PSNR in measuring the quality of natural images across a wide variety of distortions. The Structural Similarity (SSIM) Index quality assessment index is based on the computation of three terms, namely the luminance term, the contrast term and the structural term. The overall index is a multiplicative combination of the three terms.

SSIM(x,y)=[l(x,y)]α· [c(x,y)]β· [s(x,y)]γ …Equation 3

Wherel(x,y)=2μxμy+C1μ2x+μ2y+C1,c(x,y)=2σxσy+C2σ2x+σ2y+C2,s(x,y)=σxy+C3σxσy+C3
Where, μy, σx,σy, and σxy are the local means, standard deviations, and cross-covariance for images x, y. If α = β = γ = 1 (the default for Exponents), and C3 = C2/2 (default selection of C3) the index simplifies to:

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y+c1)(2\sigma_{xy}+c2)}{(\mu_x^2+\mu_y^2+c1)(\sigma_x^2+\sigma_y^2+c2)} \ldots \text{Equation 4}$$

4- Experiment result

The experiment result of this work will classified into two part, first one concentrate on the Least Significant bit, and second experiment will discuss steganography based on DCT.

5-1 LSB

Least Significant bit is one of steganography technique that has been used in this paper to embedded secret image into cover image. And each pixel value contain eight position as shown below

MSB LSB

8th	7th	6th	5th	4th	3rd	2nd	1st

In our experiment we used first three position of each pixel value to use as a cover position and replace the new value of secret image instead of an original data. The image has been used for all the experiment as a secret image is a gray image "Lena.jpg" with 128×128 dimension, the total bits of a secret image is 16384 byte or 131072 bits. And the cover images that have been used in all experiment as shown below in table 2:

Cover image	Dimension	Available Space		
		1 bit	2bits	3bits
Lena.jpg	512 × 512	262144	524288	786432
Pepper.jpg	512 × 512	262144	524288	786432
Babylon.jpg	512 × 512	262144	524288	786432

Table2: available Space of Cover images

The space that available for hiding or capacity of cover image calculate depend on the hiding system used only one layer. And figure 2 show gray level test image that have been used in this work. And figure 3 shows the original cover image and image after masked one bit per pixel and steganography image after reconstruction. And in this work used MSE, PSNR and SSIM to check the quality of the cover image after hiding, and table 2, 3 and 4 show the result of each test image when hide one bit ,two bits and three bits.

a) Lena.jpg b)pepper.jpg c) babylon .jpg

Figure 2 three 512×512 gray level test image

Figure 3 result of one bit hiding per pixel

Cover image	Secret image	MSE		
		1 bit/ pixel	2bits/ pixel	3bits/ pixel
Lena 512×512	Lena 128×128	0.4995	3.2204	16.2108
Peppers 512×512	Lena 128×128	0.5059	3.2328	15.9632
Babylon 512×512	Lena 128×128	0.4989	3.2178	16.1722

Table 2 MSE of steganography image after embedding 1, 2 and 3 bits per pixel

Cover image	Secret image	PSNR		
		1 bit/ pixel	2bits/ pixel	3bits/ pixel
Lena 512×512	Lena 128×128	51.1794	43.0857	36.0668
Peppers 512×512	Lena 128×128	51.1246	43.0689	36.1336
Babylon 512×512	Lena 128×128	51.1849	43.0892	36.0771

Table 3 PSNR of steganography image after embedding 1, 2 and 3 bits per pixel

Cover image	Secret image	SSIM		
		1 bit/ pixel	2bits/ pixel	3bits/ pixel
Lena 512×512	Lena 128×128	0.9972	0.9882	0.9557
Peppers 512×512	Lena 128×128	0.9947	0.9774	0.9210
Babylon 512×512	Lena 128×128	0.9992	0.9966	0.9872

Table 4 SSIM of steganography image after embedding 1, 2 and 3 bits per pixel

Figure 4 shows the histogram of the original image and images after embedding data within cover image for one ,two and three bit per pixel.

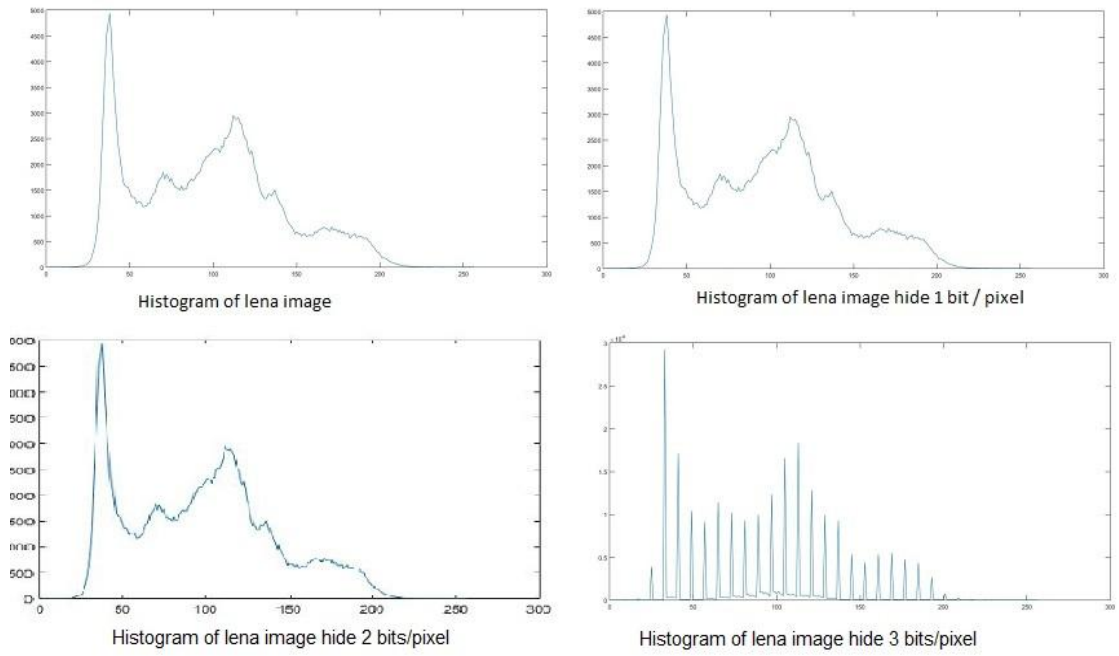

Figure 4 Histogram of Lena image and after hiding 1,2 and 3 bits per pixel

5-2 DCT Experiment result

Image hiding based on DCT concept in fourth part of the coefficient block show good result than the pervious on specially in reconstructed and figure number 5 shows original image and image after hiding.

Figure 5 experiment result of DCT

Cover image	Secret image	MSE
Lena 512×512	Lena 128×128	7.214
Peppers 512×512	Lena 128×128	6.87
Babylon 512×512	Lena 128×128	7.981

Table 5 MSE of DCT

Cover image	Secret image	PSNR
Lena 512×512	Lena 128×128	40.12
Peppers 512×512	Lena 128×128	40.058
Babylon 512×512	Lena 128×128	41.001

Table 6 PSNR of DCT

Cover image	Secret image	SSIM
Lena 512×512	Lena 128×128	0.97
Peppers 512×512	Lena 128×128	0.901
Babylon 512×512	Lena 128×128	0.981

Table 7 SSIM of DCT

III. Conclusion

In this paper I give interview on image steganography based on two different methods DCT and LSB. Steganography technique is an art of hiding data in cover media in this paper I have used hide image into cover image. Both of method achieve good result but hiding based on DCT based the result of MSE, PSNR and SSIM show the good result than LSB.

References

[1]. El Abbadi, N., Hassan, A. M., & AL-Nwany, M. M. (2013). Blind Fake Image detection. International Journal of Computer Science Issues, 10(4), 180-186.

[2]. Hussein, M. A. A. H. (2014). Video Data Steganography Based on Discrete Cosine Transform Method (Doctoral dissertation, University of Baghdad).

[3]. Singla, D., &Syal, R. (2012). Data security using LSB & DCT steganography in images. International Journal Of Computational Engineering Research, 2(2), 359-364.

[4]. Awad, W. S. (2013). Information Hiding Using Ant Colony Optimization Algorithm. Technology Diffusion and Adoption: Global Complexity, Global Innovation: Global Complexity, Global Innovation, 289.

[5]. Shamsudin, R., Taujuddin, M., &Afifi, N. S. (2010). Text hiding using Discrete Cosine Transformation (DCT).

[6]. Fardad, K., Nouri, M., &Medadian, M. (2013). Steganography on Multimedia Products by ACO. International Journal of Engineering Science and Innovative Technology, 2(2).

[7]. Fardad, K., Nouri, M., &Medadian, M. (2013). Steganography on Multimedia Products by ACO. International Journal of Engineering Science and Innovative Technology, 2(2).

[8]. Khan, S., Yousaf, M. H., &Akram, J. (2011). Implementation of Variable Least Significant Bits Stegnography using DDDB Algorithm. International Journal of Computer Science Issues (IJCSI), 8(6).

[9]. Chen, P. Y., & Lin, H. J. (2006). A DWT based approach for image steganography. International Journal of Applied Science and Engineering, 4(3), 275-290.

[10]. Al-Momen, S. M. A., & George, L. E. (2010). Image hiding using magnitude modulation on the DCT coefficients. Journal of Applied Computer Science & Mathematics, 4(8), 9-14.

AlaaAbdulhusseinDaleh Al-magsoosi "Comparison study between LSB and DCT Based Steganography." IOSR Journal of Computer Engineering (IOSR-JCE) 20.1 (2018): 47-52.