# Image Hiding Using Magnitude Modulation on the DCT Coefficients

[1]Saad M. A. AL-MOMEN, [2]Loay E. GEORGE
Information Technology Unit, College of Science, University of Baghdad, Iraq
[1]*salmoomen@yahoo.com*, [2]*loayedwar57@yahoo.com*

***Abstract*-In this paper, we introduce a DCT based steganographic method for gray scale images. The embedding approach is designed to reach efficient tradeoff among the three conflicting goals; maximizing the amount of hidden message, minimizing distortion between the cover image and stego-image, and maximizing the robustness of embedding. The main idea of the method is to create a safe embedding area in the middle and high frequency region of the DCT domain using a magnitude modulation technique. The magnitude modulation is applied using uniform quantization with magnitude Adder/Subtractor modules.**

**The conducted test results indicated that the proposed method satisfy high capacity, high preservation of perceptual and statistical properties of the stego-image and also it is robust, to some extents against several levels of JPEG compression.**

***Keywords:* Steganography, Information Hiding, DCT.**

## I. INTRODUCTION

Steganography is the science of *covered writing*. Its purpose is to hide information in a cover medium so that it is "hard" for everyone to detect the existence of the embedded information. A well-written introduction to steganography could be found in [1-4]. Images are the most commonly used carrier to transfer information. Bitmap and JPEG images have been used. Information can be hidden in images using a number of methods. These methods could be categorized into spatial domain embedding and transform domain embedding methods [1,5,6].

By embedding a secret message into a digital image, a stego-image is obtained. It is important that the stego-image does not contain any easily detectable artifacts due to message embedding such that could be detected by an eavesdropper. There are many different steganographic methods that have been overviewed and analyzed by many researchers over the last few years. (e.g., hiding files in the least significant bits of digital images, data hiding in DCT coefficients, and data hiding in DWT coefficients) [1,7]. Some papers introduced the utilization of various embedding techniques in DCT domain [8,9,10,11]. Some of these methods used the strategy of edge block selection, recursive matrix encoding and largest coefficient serving criteria to assign the host coefficient [12]. Other researches suggest the use of LSB to hide data in DCT coefficients [13]. However, one common drawback of all current data embedding methods is the fact that the original image is distorted by small amount of noise due the data embedding itself. This noise could reveal the existence of secret message and hence, weaken the security value of the covert channel.

In this paper, we propose an image steganography system where secret information is embedded in an 8x8 block – DCT coefficients using magnitude modulation method. The proposed algorithm aims to achieve a high capacity, less imperceptibility and good robustness.

## II. PROPOSED STEGANOGRAPHY METHOD BASED ON DCT

The proposed method is used to hide a secrete object (text, image, audio, video…) into a cover image. As shown in figure 1, the method depends on transforming the cover image from spatial to frequency domain, and convert the secrete object into a binary form (bits sequence). The embedding module hides some of the bits sequence in a chosen area in the frequency domain media (i.e., middle and high frequency), after applying a magnitude modulation method on the chosen transformed coefficients in order to get a safe area to hide the secret bits sequence. The magnitude modulation is obtained by applying uniform quantization.

On the other hand, figure 2 shows the extraction part of the method. The magnitude modulation is applied on the transformed stego object; it implies a uniform quantization followed by making a comparison with the original transformed value in order to get the values of embedded hidden bits.

Several techniques could be used to transform an image from spatial to frequency domain representations, such as DCT, DFT and DWT [5,6,12,13]. Each transform has its advantages. Here, the DCT approach is adopted.

The most common 2D DCT definition is given by [6]:

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

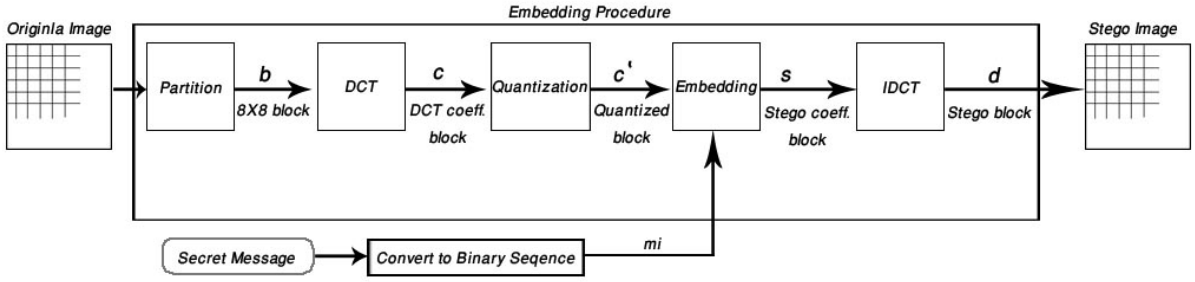


Figure 1. Message Embedding Block Diagram

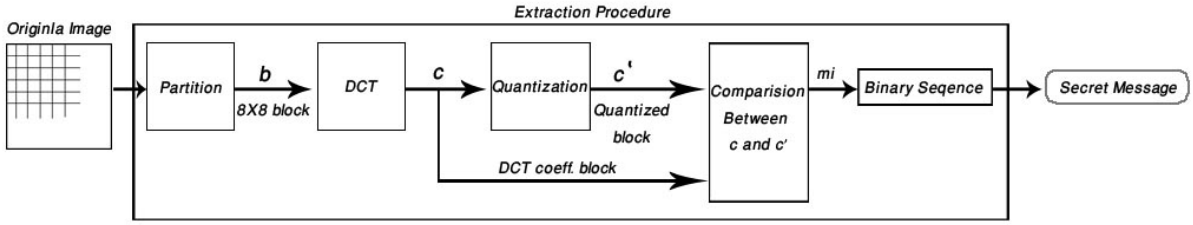


Figure 2. Message Extracting Block Diagram

Where

$$\alpha(k) = \begin{cases} \sqrt{\frac{1}{N}} & \text{for } k = 0 \\ \sqrt{\frac{2}{N}} & \text{for } k = 1,2,...,N-1 \end{cases}$$

where N is the image size.

To get the matrix form of equation (1), we will use the following equation

$$T_{i,j} = \begin{cases} \sqrt{\frac{1}{N}} & \text{for } i = 0 \\ \sqrt{\frac{2}{N}} \cos\left[\frac{(2j+1)i\pi}{2N}\right] & \text{for } i \neq 0 \end{cases} \quad (2)$$

According on the equation 2, the DCT could accomplish by matrix multiplication

$$C = T\, I\, T' \quad (3)$$

while the inverse transform equation is

$$I = T'\, C\, T \quad (4)$$

As mentioned before, the DCT transforms an image from spatial domain to frequency domain. It decomposes the image signal into spectral sub-bands, each having different importance with respect to the image's visual quality. As a rough view, as shown in figure 3, DCT decomposes the image signal into low, middle, and high frequency components [5,6,7,12,13].

### *Message Embeding Module*

The introduced system can embed a hidden message (text, image, audio) in its binary form within a cover image of suitable size. The proposed embedding method consists of four stages: Transformation, Quantization, Embedding, and Inverse Transformation (see figure 1).

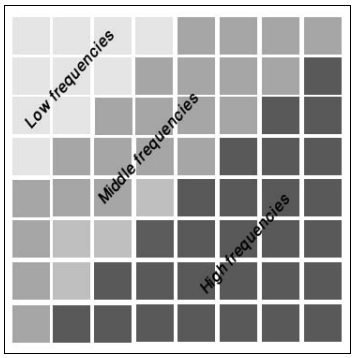


Figure 3. Low, Middle, and High frequency distribution in a DCT block.

**Stage One (Transformation Stage):**

The cover image B is partitioned into 8x8 blocks, each block is denoted by $b_i$. Then DCT is applied to each one, denoted by $c_i$.

$$c_i = T\, b_i\, T' \tag{5}$$

where T is the transformation matrix (see Equation 1).
As shown in figure 3, the upper-left corner of $c_i$ contains the low frequency coefficients, and as we proceed down along the main diagonal we will pass through the middle and reach to the high frequency coefficients. The secret message is to be hidden in the middle and high frequency regions, leaving the low frequency part as it is. It is not wise to embed the secret message bits in the low frequency components of the DCT blocks, because human vision system is more sensible to modifications may occur in the lower frequency subband.

**Stage Two (Quantization Stage):**

Figure 4 illustrates the magnitude modulation method, it is simply based on creating a slacked space (due to quantization) within the values of DCT coefficients, and then, this space is utilized to host a secret bit value.

The middle and high frequency coefficients in $c_i$, which are used as host coefficients, are quantized using the following equation:

$$c'_i(u,v) = \text{round}\left(\frac{c_i(u,v)}{Q_{Step}(u,v)}\right)\cdot Q_{Step}(u,v) \tag{6}$$

where

$$Q_{Step}(u,v) = Q_0 + \alpha(u+v) \tag{7}$$

$Q_0$ and $\alpha$ are chosen constants. The values of $(u, v) \in \{0, 1, 2, \ldots, N-1\}$, where N is the block size.

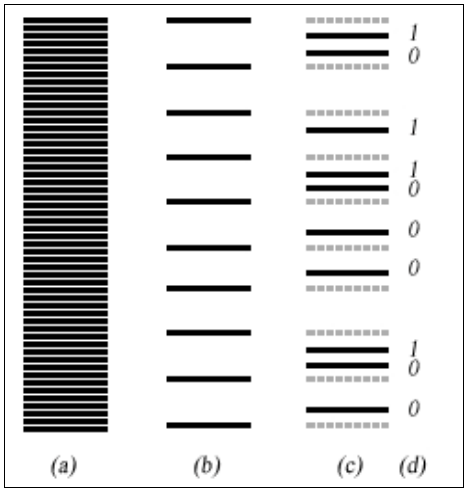


Figure 4 Quantization and Embedding stages.

(a) Original DCT coefficient values.
(b) Quantized DCT coefficient values.
(c) New quantized DCT coefficient values.
(d) The values of the binary secrete bits.

**Stage Three (Embedding Stage):**

The secret message (text, image, audio,…) that we wish to embed within the cover image should be converted into a binary sequence mi , or more specifically, into bits sequence. This binary sequence is embedded in the middle and high frequency coefficients area of $c'_i$ to get a stego-block $s_i$. The embedding process is based on applying magnitude modulation to the quantized values of the host DCT coefficients, such that:

$$s_i(u,v) = \begin{cases} c'_i(u,v) + \dfrac{Q_{Step}(u,v)}{3} & \text{if } m_i = 0 \\ c'_i(u,v) - \dfrac{Q_{Step}(u,v)}{3} & \text{if } m_i = 1 \end{cases} \tag{8}$$

**Stage Four (Inverse Transformation Stage):**

For each stego-block $s_i$, the inverse DCT will be taken to get the output blocks $d_i$

$$d_i = T' s_i T \tag{9}$$

Finally, $d_i$ blocks will be put together to establish stego-image D.

***Message extraction module***

As shown in Figure 2, to extract the hidden message from the stego-image the following three stages are applied:

**Stage One (Transformation Stage):**

This stage is exactly like the transformation stage of the embedding process. It is applied to get the DCT coefficients block c.

**Stage Two (Quantization Stage):**

This stage is, also, same like quantization stage of the embedding process. It is applied to get the quantized block c'.

**Stage Three (Extraction Stage):**

In this stage each entry in the middle and high frequency area in c is compared with the corresponding entry in c' , to get the hidden binary bits using the following criteria:

$$m_i = \begin{cases} 0 & \text{for } c_i(u,v) > c'_i(u,v) \\ 1 & \text{for } c_i(u,v) < c'_i(u,v) \end{cases} \tag{10}$$

## III. Experimental Results

In this work, a set of tests were conducted to examine the performance of the proposed method to hide a binary payload within a test image and, then to investigate the effect of the compression on the extracted message. In this section, some samples of test results are presented to illustrate the system performance. The popular image Lena of size 256X256 was used as a cover image, while a random sequence of bits is used as a secret message.

### *Results Without Jpeg Compression Attack*

Generally, the image steganography system must embed the content of a hidden message in the image such that the visual quality of the image is not perceptibly changed. Thus to study the embedding perceptual effect, we have used the peak signal to noise ratio (PSNR) which is defined as [6,12]:

$$\mathrm{PSNR} = 10\log_{10}\frac{(L-1)^2}{\mathrm{RMS}} \tag{11}$$

where

$$\mathrm{RMS} = \frac{1}{m\cdot n}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(x_{i,j}-x'_{i,j}\right)^2 \tag{12}$$

and L is the number of gray levels, X is the cover image, X' is the stego-image, m is the image width, and n is the image height.

On the other hand, a Rate of Wrong Retrieved Bits (RWRB) where defined as:

$$\mathrm{RWRB} = \frac{n_r}{n}\times 100\% \tag{13}$$

where, $n_r$ is the number of wrong retrieved bits (WRB), and n is the total number of hidden bits. This metric was used to calculate the accuracy of the extraction process. As long as RWRB goes to zero, better extraction results where obtain.

Table 1 shows the results of different choices of $Q_0$ and α. In most cases the extracted message has no errors.

TABLE 1 PSNR AND RATE OF WRONG RETRIEVED BITS FOR DIFFERENT CHOICES OF $Q_0$ AND α

| α | $Q_0$ | PSNR | RWRB* |
|---|---|---|---|
| 0.1 | 5 | 41.4 | 0.04% |
| | 6 | 40.8 | 0.004% |
| | 7 | 38.9 | 0% |
| | 8 | 38 | 0% |
| | 9 | 37.1 | 0% |
| | 10 | 36.4 | 0% |
| | 11 | 35.7 | 0% |
| | 12 | 35.1 | 0% |
| 0.5 | 5 | 37.6 | 0% |
| | 6 | 36.8 | 0% |
| | 7 | 36.1 | 0% |
| | 8 | 35.4 | 0% |
| | 9 | 34.7 | 0% |
| | 10 | 34.3 | 0% |
| | 11 | 33.7 | 0% |
| | 12 | 33.3 | 0% |
| 1 | 5 | 34.6 | 0% |
| | 6 | 34.1 | 0% |
| | 7 | 33.6 | 0% |
| | 8 | 33.1 | 0% |
| | 9 | 32.7 | 0% |
| | 10 | 32.2 | 0% |
| | 11 | 31.8 | 0% |
| | 12 | 31.4 | 0% |
| 1.5 | 5 | 32.4 | 0% |
| | 6 | 32 | 0% |
| | 7 | 31.7 | 0% |
| | 8 | 31.3 | 0% |
| | 9 | 30.9 | 0% |
| | 10 | 30.6 | 0% |
| | 11 | 30.2 | 0% |
| | 12 | 29.9 | 0% |

* Rate of Wrong Retrieved Bits.

Figure 5 shows the original image with its histogram, in addition to two samples of stego images with their histograms. The first stego sample is produced using $Q_0$ =8 and α=1.5, while the values of these two parameters for the second sample are $Q_0$ = 9 and α = 1.

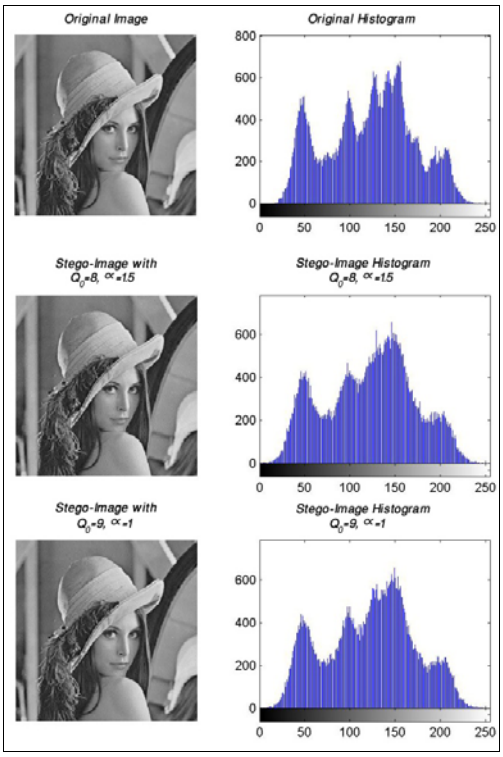


Figure 5. Two stego-samples produced by the proposed method.

***Results with jpeg compression attack***

Digital images with hidden information (i.e., stego images) may be compressed using one of the lossy compression schemes. In such case the contents of these images may change and consequently this will cause degradation in the integrity of extracted hidden message.

To access to level of compression effectiveness, another set of tests were conducted. In this set the stego image is passes through JPEG compression before its secret message is extracted. During the test various degrees of compression rates were applied. The over all test results indicated the proposed method can achieve good hiding results for certain values of $Q_0$ and $\alpha$, and the corresponding fidelity measure values around 32dB.

Figure 6 shows the performance parameters of the proposed method under JPEG compression attack at different quality factors.

In both considered cases (i.e., without and with the JPEG compression attack), the hiding capacity was 9.18% of the cover size. The hiding capacity (HC) is computed using the following equation:

$$HC = \frac{L_s}{L_c} \times 100\% \qquad (14)$$

where, $L_s$ is the size of secrete message and $L_c$ is the size of cover image.

The results of the conducted tests show that the proposed method have good hiding capacity (HC) compared with the other known methods, and doesn't change perceptual and statistical properties. Also, the extracted hidden information almost survived if no JPEG attack is done, and it has an acceptable RWRB when low compression rate is imposed.

## IV. CONCLUSIONS

The test results illustrated that the proposed method can preserve image quality and provide good hiding capacity of hidden message, which it reaches to 9.18%.

When no JPEG attack is applied, the extraction process is fully successful. While, when applying a low compression ratio the hiding method work with acceptable rate of wrong extracted bits. Of course, a good choice of the parameters $Q_0$ and $\alpha$, plays a significant role in the success of the whole process. Experiments showed that good tradeoff results can be obtained when the values of $Q_0$ and $\alpha$ that lead to PSNR values lay around 32dB.

Many variations could be introduced to improve the performance of the introduced hiding system. In the embedding stage we can restrict the embedding area to the middle frequency subbands only.

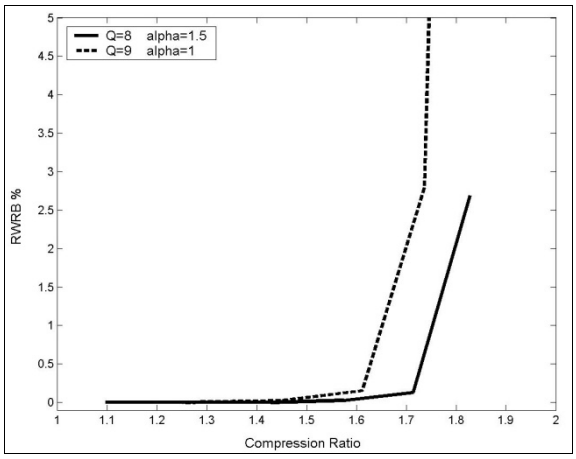


Figure 6. Rate of Wrong Retrieved Bits w.r.t. Compression Ratio

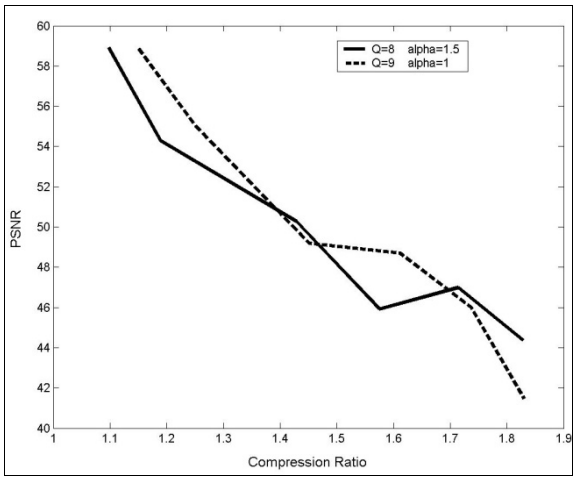


Figure 7. PSNR w.r.t. Compression Ratio

This will decrease the effect of the JPEG compression on the extracted message and better successful bits retrieval rates could be attained.

## REFERENCES

[1] N. F. Johnson and S. Katzenbeisser, .A survey of steganographic techniques., in S. Katzenbeisser and F. Peticolas (Eds.): "*Information Hiding*", pp.43-78. Artech House, Norwood, MA, 2000.

[2] N.F. Johnson and S. Jajodia: "Exploring Steganography: Seeing the Unseen" Computer, vol. 31, no. 2, 1998, pp. 26–34.

[3] N.F. Johnson, Z. Duric and S. Jajodia: "Information Hiding: Steganography and Watermarking – Attacks and Countermeasures". Kluwer Academic, Dordrecht, The Netherlands, 2001.

[4] R. Anderson, S. Goldenstein: "Steganography and Steganalysis in Digital Multimedia: Hype or Hallelujah?", RITA, Volume XV, Número 1, pp. 83-110, 2008.

[5] R. C. Gonzalez and R. E. Woods: "Digital Image Processing". Prentice-Hall, Boston, MA, USA, second edition, 2002.
[6] E. Scott, Umbaugh: "Computer Vision and Image Processing", Prentice Hall PTR,1998.
[7] T. Morkel, J. Eloff and M. Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005 (Published electronically).
[8] K. WONG and K. TANAKA , "StegErmelc: A Novel DCT-Based Steganographic Method Using Three Strategies", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 2008 E91-A(10):2897-2908.
[9] K.B. Raja, C.R. Chowdary, K.R. Venugopal, L.M. Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", ICISIP 2005 Third International Conference on Intelligent Sensing and Information Processing 2005, p.p. 170- 176.
[10] L. Chih-Yang, C. Chin-Chen, W. Yu-Zheng, "Reversible Steganographic Method with High Payload for JPEG Images", IEICE Transactions on Information and Systems 2008 E91-D(3):836-84.
[11] K. Wong, X. Qi, K. Tanaka, "A DCT-based Mod4 steganographic method", Signal Processing 87 ,2007, p.p. 1251–1263.
[12] D. Salomon, "Data Compression: The Complete Reference", Springer, forth edition, 2007.
[13] I. M. Pu, "Fundamental Data Compression", Butterworth-Heinemann, 2006.

**Saad M.A. AL-MOMEN** received the B.Sc. degree in Applied Mathematics (1993) from School of Applied Science, University of Technology, M.Sc. in Mathematics and Computer Applications (1996) from Department of Mathematics, College of Science, Al-Nahrin University, Baghdad, Iraq.
In 1996, he joined the High Institute for Teachers in Musrata, Lybia as a member of the teaching staff. In 2000 he transformed to Al-Mansour University College in Baghdad to be a lecturer there. Since 2008, he is a lecturer in the IT Unit in College of Science, University of Baghdad. His current research interest includes images processing, data security, and web development.

**Loay E. GEORGE** received the B.Sc. degree in Physics (1979), M.Sc. in Theoretical Physics (1982), and Ph.D degree in Digital Image Processing (1997) from Physics Department, College of Science, Baghdad University, Iraq.
In 1984, he joined the Iraqi Research Council and worked as research scientist. Since 2005 he transformed to Baghdad University to be a lecturer. Currently, he is head of IT Unit in College of Science. His current research interest includes images processing, transform coding, biometrics, and video coding.