ISSN No. 0976-5697

Volume 3, No. 7, Nov-Dec 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Data hiding in image using DCT

Ahmed Saber Sakr*
Department of Mathematics & Computer Science,
Faculty of Science,
Menoufia University, Egypt
a.ssakr@yahoo.com

Hani Mohamed Ibrahem
Department of Mathematics & Computer Science,
Faculty of Science,
Menoufia University, Egypt
hanimir78@yahoo.com

Hatem M. Abdullkader
Department of information System, Faculty of Computers and Information, Menoufia University, Egypt
hatem6803@yahoo.com

Mohamed Amin
Department of mathematics & Computer Science,
Faculty of Science, Menoufia University, Egypt
mohamed_amin110@yahoo.com

Abstract: In this paper, an efficient stegnographic technique based on the discrete cosine transform (DCT) of image is proposed. In this technique, the DCT coefficient is quantized using a predefined mathematical operation then the secret bits is embedded in low and middle frequency component of the quantized DCT coefficient using least significant-bit (LSB) to enable a large message capacity. A comparison between the proposed technique and other existing technique is introduced. The results demonstrated that the performance of the proposed algorithm is satisfied compared to them.

Keywords: Steganography; Data hiding; DCT; LSB.

I. INTRODUCTION

The internet and multimedia are getting widely used in a way which digital data is not secure. The widespread and easy access to multimedia content has motivated development of technologies to secure transmission of data. Various techniques are proposed and already taken into practice like cryptography, watermarking and data hiding each of them has different objectives when serving their purpose. Data Hiding is the process of secretly embedding information inside a data source without changing its perceptual quality. Generally, in Data Hiding, the actual information is embedded in a cover like image, video or audio. This cover is sent through the network to the recipient, where the actual message is extracted it. [1, 2]. In stegnography there are two common methods of embedding data: Spatial embedding in which messages are inserted into the LSBs (least significant bit) of image pixels, and Transform embedding in which a message is embedded by modifying frequency coefficients of the cover image (result is called the stego image).Transform embedding methods are more robust than the Spatial embedding methods which are susceptible to image-processing type of attacks. However with respect to steganography robustness is not a critical property but the perceptibility (i.e., whether the source cover is distorted by embedding information to a visually unacceptable level).There is another important issue of steganography, namely, capacity, i.e., how much information can be embedded relative to its perceptibility [2, 3].

In this paper an efficient steganographic algorithm for data hiding is proposed .Digital images is used as the cover to embed the hidden data. A new stegnographyic method is developed based on Jpeg-Jsteg algorithm to embed a message in a host image.

The rest of this paper is organized as follows. A brief review of related works is given in Section 2

The proposed method is presented in section 3. Simulation and performance analysis are provided in section 4. Finally, the conclusions is in Section 5.

II. RELATED WORK

JPEg-Jsteg algorithm is one of the embedded method of stegnography based on the transform domain which embeds secret message in the LSB of the quantized DCT coefficient.[4].

Mutto and Kumar proposed a Jpeg-Jsteg algorithm based on T-codes for the different images and reported that it is almost the same as original algorithm-Huffman codes based. They reported also that there is no change in the stego-image quality [3]. Westfeld proposed an efficient algorithm F5 that stand up against visual and statistical attack and offers a large steganographic capacity [5].

Zhag et al proposed a classification algorithm that can distinguish between Jsteg and F5 stego images using the difference of image DCT coefficient histogram [6].

Westfeld and Pfitzmann reported that steganographic systems that change LSBs sequentially cause distortions detectable by steganalysis methods. They observed that for a given image, the embedding of high-entropy data (often due to encryption) change the histogram of color frequencies in a predictable way [7].

Chang et al has suggested a new steganographic method to increase the message load in every block of the stego-image

while retaining the stego-image quality. Upon modifying the quantization table, the secret message can be embedded in the middle-frequency part of the quantized DCT coefficients. Moreover, the method is as secure as the original Jpeg-Jsteg [8].

Li and Wang presented astegano- graphic method that modifies the quantization table and inserts the hidden bits in the middle frequency coefficients [9].

LENTI J. has shown that the picture visible properties can be modified by embedding a large amount of data into it [1].

III. PROPOSED ALGORITHM

In steganography, the message capacity and the image quality of a stego image are two important criteria. However, the embedding capacity of Jpeg-Jsteg is little small when the quantization table is used [2] . Here, we propose a new Jpeg-Jsteg stegnographyic method that embed a message in a host image without the need to the quantization table. That is a predefined mathematical operations are used to quantize the DCT coefficient .

A. Embedding algorithm:

The proposed embedding method contains two phases. The first phase partition the cover-image (O) into none overlapping i blocks of 8 x 8 pixels, and then the DCT is used to transform each block into DCT coefficients. These coefficients are scaled with some mathematical operation. The second phase we start from the first block and begin embedding the message in the 2LSB (two lest significant bit) of the DCT low and middle coefficient for each block Oi until the end of message. Then we de quantize the coefficient after embedding and return it into spatial Domain using IDCT. Then we return the stego image. The Block diagram of the embedding algorithm is shown in fig(1).

The embedding algorithm can be summarized as follow :

[Algorithm of the embedding procedure]

Input: A cover-image O, message M

Output: A stego-image E, key K.

Begin

Step 1: Input a cover-image O. Suppose its size is N X N pixels. Partition the Cover-image into non-over lapping blocks $\{O_1, O2, O3, \ldots, O_{N/8xN/8}\}$. Each O_i $,i=0,1,\ldots..N/8$ contains 8 x 8 pixels.

Step 2: Use DCT to transform each block Oi into DCT coefficient matrix Fi,
Where $F_i[a,b] = DCT (O_i[a,b])$, where $1 \le a,b \le 8$.

Step3: 3-1 Get the decimal value of every coefficient in F_i assigned to the matrix FLi
3-2 Assign ($F_i - FL_i$). To F_i
3-3 Get the minimum value (min) of the F_i matrix .
3-4 Assign (F_i - min) to F_i

Step 4: Start from O_{1x1}

Step 5: While complete message not embedded do
5.1: Use next coefficient from F_i.
5.2: Get next 2bit from message.
5.3: Replace Fi coefficient 2LSB with message

End {while}

Step 7:
7-1 Assign (F_i + min) to F_i
7-2 Assign (F_i + FL_i) to F_i

Step 8: Use IDCT to transform each block F_i to its original form O_i

Step 9: Return min as a key of stego-image E. and stego image E.

End

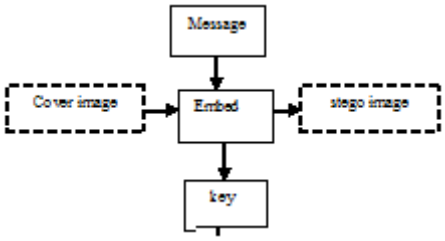


Figure **(1)** Block diagram of the embedding algorithm

B. Extracting algorithm:

The extracting method contains two phases. The first phase partition the cover-image (*O*) into non overlapping *i* blocks of 8 x 8 pixels and a DCT is used to transform each block into DCT coefficients. Then these coefficients are scaled with some mathematical operation using the key. The second phase we begin from block 0 and begin extracting the message from the 2LSB of the DCT coefficient for each block O_i until the end of message . The Block diagram of the embedding algorithm is shown in fig(2) .The extracting algorithm can be summarized as follow :

[Algorithm of the extracting procedure]

Input: A stego-image E., Key K

Output: Message M

Begin

Step 1: Input a stego-image E. Suppose its size is N X N pixels. Partition the Stego-image into non-over lapping blocks $\{E_1,E_2,E_3, \ldots, E_{N/8xN/8}\}$.
Each E_i $i=(1,2,..,n/8)$ Contains 8 x 8 pixels.

Step 2: Use DCT to transform each block E_i into DCT coefficient matrix Fi, Where $F_i[a,b] = DCT (E_i[a , b])$, where $1 \le a,b \le 8$.

Step3:
4-1 Get the decimal value of every coefficient in F_i in the matrix FL_i
4-2 Assign ($F_i - FL_i$) to F_i
4-4 Assign (F_i - key) to F_i

Step 4: start from E_{1x1}

Step 5: while complete message not extracted do
5.1: get next coefficient from F_i.
5.2: concatenate F_i coefficient 2 LSB to secret message.
End {while}

End

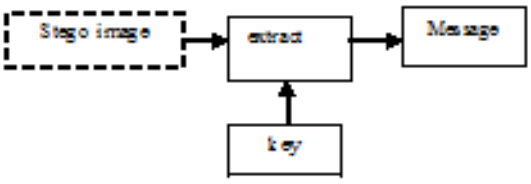


Figure (2) Block diagram of the extracting algorithm

IV. SIMULATION AND PERFORMANCE ANALYSIS

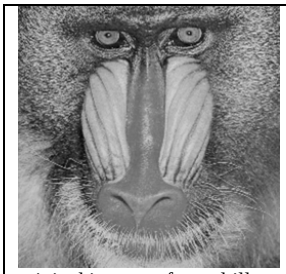
This section presents the experimental results of the proposed method. We also compare the proposed method with chang et.al method under the same circumstances. All these programs were coded in Matlab2009 and run on a personal computer (PC) Pentium core with 4GB RAM under the Window XP operation system.

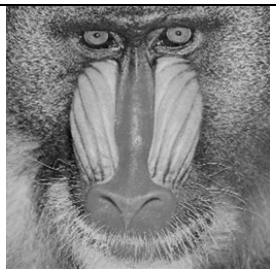
In chang et.al [8] the maximum capacity is 52 secret bits in (8x8) block after the modification of quantization table is applied .in addition 53248 secret bits are embedded in image with 256x256 pixels.

In the proposed method 72 secret bits are embedded in (8x8) block. Thus 73728 secret bits are embedded in image with (256X256) pixel. The proposed algorithm is implemented on four standard gray-level images Lena, mandrill, woman and Pirate, with 256 x 256 pixels. These images are used as the cover-images .The peak signal to noise rate (PSNR), image capacity and correlation coefficient are used to evaluate the image quality and the performance of the proposed algorithm. The numerical comparison between Chang and the proposed algorithm is presented in Table 1. These results demonstrated that the proposed method gives better results than other techniques. Fig. 4 shows the images before and after embedded the secret bit. In addition, Fig. 5 shows the histogram of images before and after embedded the secret bits.

Table 1: numerical comparison between Chang and the proposed algorithm

Mandrill			
Algorithm	**Capacity**	**PSNR**	**Correlation**
Cahng	53248	28.9636	0.9718
Proposed	73728	47.1326	0.9996
Lena			
Cahng	53248	32.3366	0.9916
Proposed	73728	47.2633	0.9997
Woman			
Cahng	53248	31.8775	0.9876
Proposed	73728	47.2466	0.9996
Pirate			
Cahng	53248	31.1721	0.9887
Proposed	73728	47.1039	0.9997


original images of mandrill


stego images of mandrill


original images of Lena


stego images of Lena

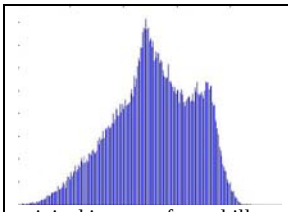

original images of woman

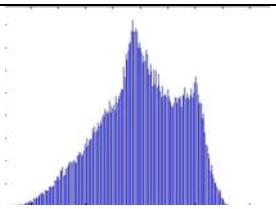

stego images of woman

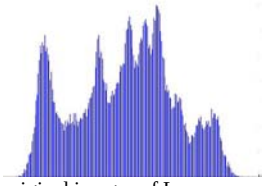

original images of pirate

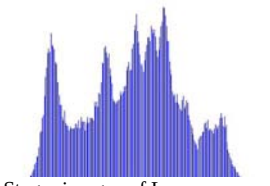

original images of pirate

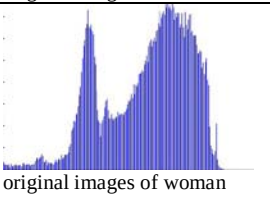
Figure. 4 the images before and after embedded the secret bit

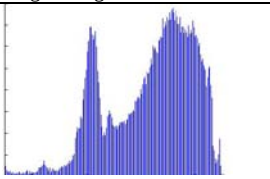

original images of mandrill

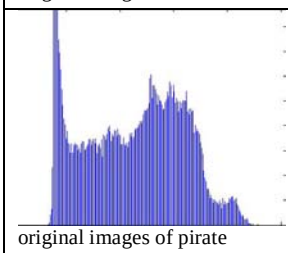

Stego images of mandrill


original images of Lena


Stego images of Lena


original images of woman


Stego images of woman


original images of pirate

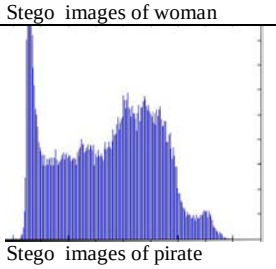

Stego images of pirate

Figure. 5: Histogram of images before and after embedded the secret bits.

V. CONCLUSION

The goal of data hiding is to make the secret messages hidden in the cover-images. In chang et al, the message capacity that can be embedded in the cover-image is little small as he embed in middle frequency of quantized DCT coefficient . To improve the capacity of hidden message, we propose a new steganographic method to increase the message capacity in every block of the stego-image while keeping the stego-image quality acceptable. In our method, the secret message is embedded in low and middle frequancy of the quantized DCT coefficients. Our experimental results show that the proposed method provides acceptable image quality and a large message capacity. Moreover, based on our security analysis, we observe that the proposed method has the same camouflage and thus has the same security level aschang et al . Overall, the proposed method matches the requirement of steganography with a larger message capacity than that of chang et al .

VI. REFERENCES

[1]. József lenti (2000): Steganographic methods, Periodica Polytechnica, 44, (3-4): 249–258.

[2]. Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKevitt (2010): Digital image steganography: Survey and analysis of current methods, Signal Processing 90: 727–752.

[3]. S. K. Muttoo, Sushil Kumar (2008): Data Hiding in JPEG Images. International Journal of Information Technology. Vol.1 No.1 : 13-16

[4]. Niels Provos and Honeyman (2003): "Hide and Seek: an Introduction to Steganography", IEEE Security and Privacy, May/June 32-43.

[5]. A.Westfeld (2001): F5-A steganographic algorithm: high capacity despite better steganalysis, in: Proceedings of Fourth International Work- shop on Information Hiding, Lecture Notes in Computer Science, vol. 2137: 289–302.

[6]. Qian Zhang, Yuan Liu, Yu Nan, Tao Zhao, Fenlin Liu (2011): Classification Algorithm of Jsteg and F5 Stego-images Based on Histogram Difference. Energy Procedia 13:8759-8766.

[7]. A.Westfeld and A. Pfitzmann (1999): "Attacks on steganogrphic systems", 3rd International Workshop on Information Hiding.

[8]. Chin-Chen Chang, Tung-Shou, and Lou-Zo Chung (2002): A steganographic method based upon JPEG and quantization table modification", Information Sciences 141, 123-138.

[9]. X. Li, J. Wang (2007): A steganographic method based upon JPEG and particle swarm optimization algorithm. Information Sciences 177 (15):3099–31091.