A Steganographic Method Based on DCT and New Quantization Technique

Mohamed Amin[1], Hatem M. Abdullkader[2], Hani M. Ibrahem[1], and Ahmed S. Sakr[1]
(Corresponding author: Ahmed S. Sakr)

Mathematics and Computer Science Department, Faculty of Science, Menofia University, Egypt[1]
Information System Department, Faculty of Computers and Information, Menofia University, Egypt[2]
(Email: a.ssakr@yahoo.com)

(Received Aug. 17, 2012; revised and accepted Mar. 7, 2013)

Abstract

In this paper, an efficient data hiding 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 are embedded in all frequency component of the quantized DCT coefficient using least significant-bit (LSB) to enable a large message capacity. A comparison between the proposed method and other existing methods is introduced. The results demonstrated that the performance of the proposed method is satisfied compared to them.

Keywords: Data hiding, DCT, LSB, steganography

1 Introduction

In the recent decade, new devices and powerful software have made it possible for consumers worldwide to access, create, and manipulate multimedia data. Internet and wireless networks offer ubiquitous channels to deliver and exchange such multimedia information. In order to improve the security features in multimedia data transfers over the internet, two techniques are available to achieve this goal. The first technique is cryptography [3, 6], where the sender uses an encryption key to scramble the message, this scrambled message is transmitted through the insecure public channel, and the reconstruction of the original, unencrypted message is possible only if the receiver has the appropriate decryption key. The second technique is steganography, where the secret message is embedded in another message [3, 4]. 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 [3, 6].

In this paper, an efficient steganographic algorithm for data hiding is proposed .Digital images are used as the cover to embed the hidden data. Steganographic algorithms work on basically three types of images: Raw images (i.e., bmp format), Palette based images (i.e., GIF images) and JPEG images. 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 are in Section 5.

2 A Review of Related Work

Least Significant Bit Method (LSB) is one of spatial domain steganography method it replace the LSB of cover image with secret message bit value [1].

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 [7].

Mutto and Kumar proposed a Jpeg-Jsteg algorithm based on T-codes. T-codes are families of variable-length codes (VLC) that exhibit extraordinarily strong tendency towards self synchronization. The concepts of simple T-codes were given by Titchner [8]. They used it for 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 [6].

Westfeld proposed an efficient algorithm F5 that stand up against visual and statistical attack and offers a large steganographic capacity [11].

Zhag et al. proposed a classification algorithm that can distinguish between Jsteg algorithm and F5 algorithm stego images using the difference of image DCT coefficient histogram [12].

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 [10].

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 [2].

Li and Wang presented astegano-graphic method that modifies the quantization table and inserts the hidden bits in the middle frequency coefficients [5].

Lenti has shown that the picture visible properties can be modified by embedding a large amount of data into it [4].

3 Proposed Method

In steganography, the message capacity and the quality of stego image are two important criteria. However, the embedding capacity of Jpeg-Jsteg is little small when the quantization table is used [3] as it hides data in low frequency only. Also when Chang et al. modified the quantization table to hide data in middle frequency the capacity of his tech was more than Jpeg-Jsteg. Here, we propose a new stegnographyic method that embeds a message in all frequency of quantized DCT coefficient of host image using new quantization technique without the use of ordinary quantization table. That technique is using predefined mathematical operations to quantize the DCT coefficient.

3.1 Embedding Algorithm

The proposed embedding method contains three phases. The first phase partition the cover-image O into none overlapping i blocks of 8 x 8 pixels, and then we use DCT to transform each block into DCT coefficients. Then the DCT coefficients are scaled with some predefined mathematical operation. The second phases we begin from the (i-1) block and begin embedding the message in the 2LSB of the DCT 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. The third phases we hide the message size in the i block of the image in spatial domain then we return the stego image. The block diagram of the embedding algorithm is shown in Figure 1 and embedding algorithm can be summarized in Algorithm 1.

Algorithm 1: Embedding algorithm

```
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 $O_{i,j}$ where $1\leq i , j \leq N/8$
Each $O_{i,j}$ contains $8 x 8$ pixels.
Step 2: Use DCT to transform each block $O_{i,j}$ into DCT coefficient matrix $\mathrm{F}_{i,j}$ , Where $F_{i,j}$ [a,b] = DCT ($O_{i,j}$ [a,b]), where 1≤a,b≤8 .
Step3:
3-1 Get the decimal value of every coefficient in $\mathrm{F}_{i,j}$ assigned to the matrix $FL_{i,j}$
3-2 Assign ($F_{i,j} - FL_{i,j}$ ). To $C_{i,j}$
3-3 Get the minimum value (min) of the $C_{i,j}$ matrix.
3-4 Assign ($C_{i,j}$ - min ) to $C_{i,j}$
Step 4: Start from $\mathrm{C}_{(N/8)-1,(N/8)-1}$
Step 5: While complete message not embedded do
        5.1: Use next coefficient from $\mathrm{C}_{i,j}$ .
        5.2: Get next 2bit from message.
        5.3: Replace $\mathrm{C}_{i,j}$ coefficient 2LSB with message
End {while}
Step 7: 7-1 Assign ($C_{i,j}$ + min ) to $C_{i,j}$
        7-2 Assign ($\mathrm{C}_{i,j}$ + $\mathrm{FL}_{i,j}$ ) to $\mathrm{F}_{i,j}$
Step 8: Use IDCT to transform each block $\mathrm{F}_{i,j}$ to its original form $\mathrm{O}_{i,j}$
Step 9: Calculate the message size .
Step 10: Replace the ($\mathrm{O}_{(N/8)x(N/8)}$) block LSB with the message size bit .
Step 11: Return min as a key of stego-image $E$.
End
```

3.2 Extracting Algorithm

The extracting method contains two phases. The first phase partition the cover-image (O) into none overlapping i blocks of 8 x 8 pixels, retrieve the message size from i block 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 phases we begin from the (i-1) block and begin extracting the message from the 2LSB of the DCT coefficient for each block Oi until the end of message. The block diagram is shown in Figure 2 and The extracting algorithm can be summarized in Algorithm (2).

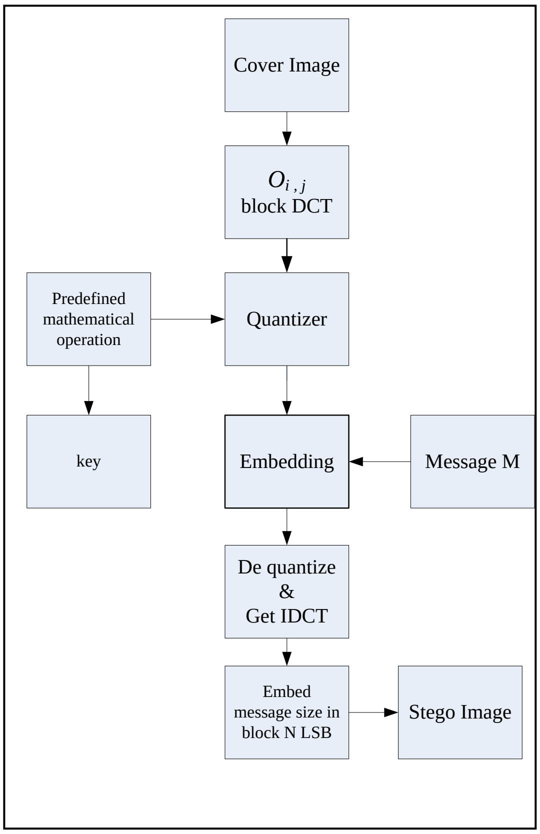


Figure 1: Block diagram of the embedding algorithm

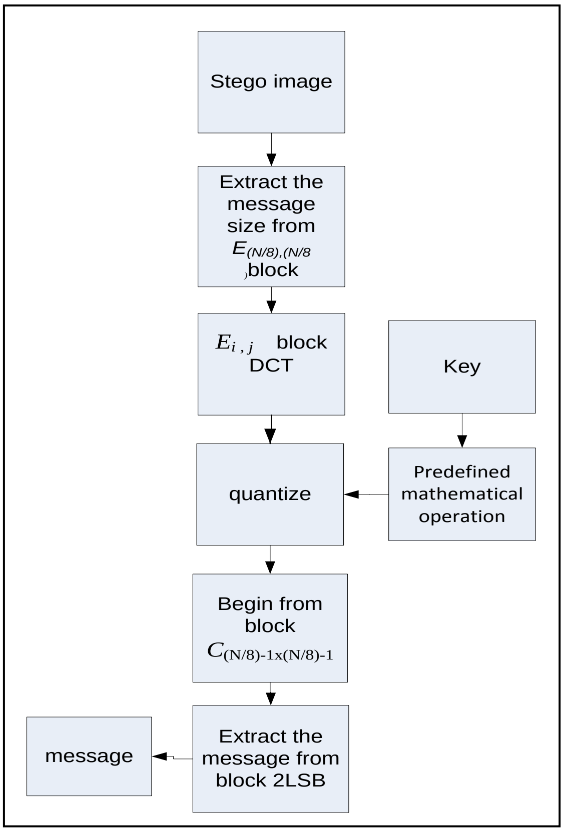

Stego image
Extract the message size from $E_{(N/8),(N/8)}$,block
$E_{i,j}$ block DCT
Key
quantize
Predefined mathematical operation
Begin from block $C_{(N/8)-1x(N/8)-1}$
message
Extract the message from block 2LSB

Figure 2: The extracting algorithm block diagram

Algorithm 2: Extracting algorithm

```
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 $E_{i,j}$ where $1 \le i , j \le N/8$
Each Ei , j contains 8 x 8 pixels.
Step 2 : Get the message size from the ($E_{(N/8),(N/8)}$) block LSB.
Step 3: Use DCT to transform each block $E_{i,j}$ into DCT coefficient matrix $F_{i,j}$ , Where $F_{i,j}$ [a,b] = DCT ($E_{i,j}$ [ a , b ]), where $1 \le a,b \le 8$ .

Step4:
      4-1 Get the decimal value of every coefficient in $F_{i,j}$ in the matrix $FL_{i,j}$
      4-2 Assign ($F_{i,j}$ – $FL_{i,j}$ ) to $C_{i,j}$
      4-3 Assign ($C_{i,j}$ - key) to $C_{i,j}$
Step 4: start from $C_{(N/8)-1x(N/8)-1}$
Step 5: while complete message not extracted do
        5.1: get next coefficient from $C_{i,j}$
        5.2: concatenate $C_{i,j}$ coefficient 2 LSB to secret message.
         End {while}
End
```

4 Simulation and Performance Analysis

This section presents the experimental results of the proposed method implemented on image. In addition a comparison between the proposed methods, Jpeg–Jsteg method and Chang et al.'s method are included in this section. All the methods were implemented on a personal computer (PC) Pentium core 2 duo with 4GB of RAM under the Window 7 professional operating system. Matlab 2009 was used to implement the proposed methods, Jpeg–Jsteg method and Chang et al.'s method.

The stego-image quality and message capacity are the two most important criteria in evaluating a steganographic method. Thus, our experiments of comparison focus on these two criteria. We use four standard gray-level images Lena, Baboon, Pepper and Girl [9], with 256 x 256 pixels.

In the Jpeg–Jsteg method, however, the message capacity can be inferred from the number of the quantized DCT coefficients whose values are not (0, 1, or - 1). Because the DCT coefficients after the quantization are almost all zeros, the message capacity of Jpeg–Jsteg is very much limited.

In Chang et al. method the maximum capacity is 52 secret bits in (8 x 8) block after the modification of quantization table is applied .in addition 53248 secret bits are embedded in image with 256 x 256 pixels.

In the proposed method 128 secret bits are embedded in (8 x 8) block. Thus 131008 secret bits are embedded in image with (256 X 256) pixel.

The peak signal to noise rate (PSNR) metrics is the most common and widely used full reference metrics for objective image quality evaluation. In particular, PSNR is used in many image processing applications and considered as a reference model to evaluate the efficiency of other objective image quality evaluation methods. PSNR as a metric computes the peak signal-to-noise ratio, in decibels, between two images. It is used in steganography to measure the peak signal-to-noise ratio between the original image and the stego-image after embedding the hidden data.

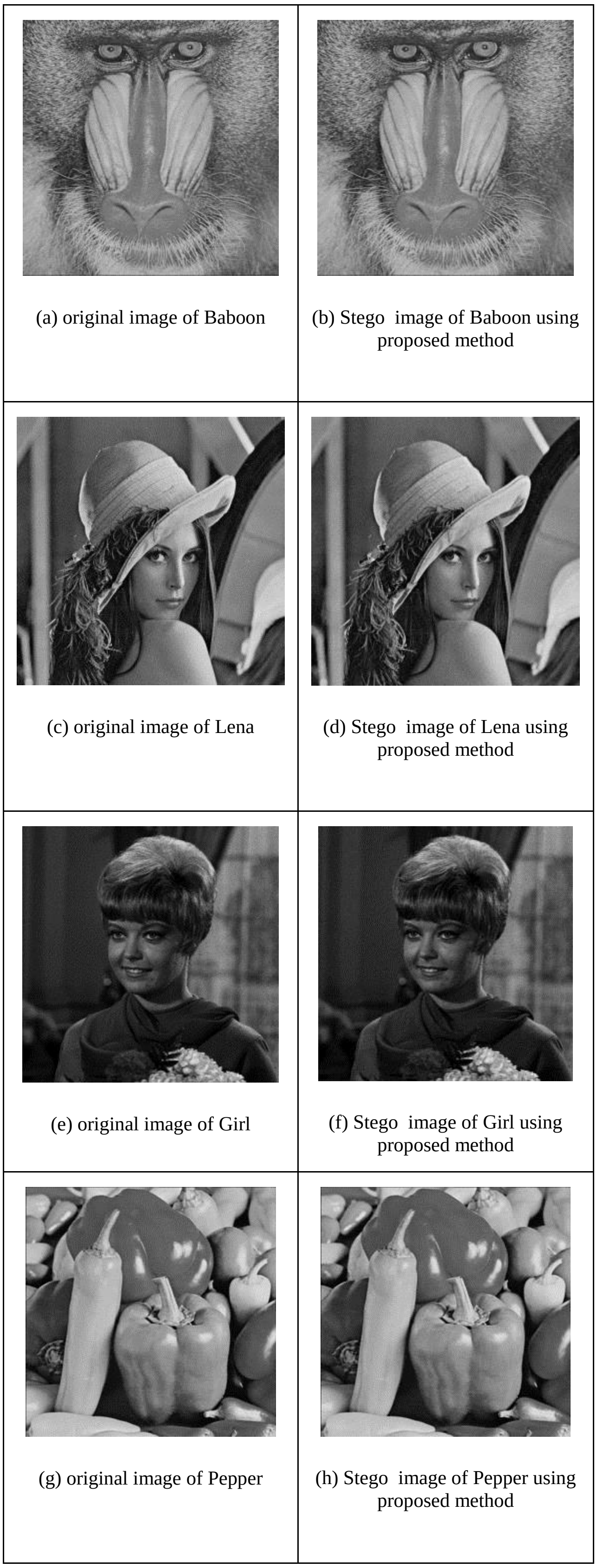
The correlation coefficient is a measure of the strength of the straight-line or linear relationship between two variables. The correlation coefficient takes on values ranging between +1 and -1. It is used to measure the correlation between the stego-image and the original image.

In our experiment PSNR, image size, image capacity and correlation coefficient are used to evaluate the image quality and the performance of the proposed algorithm.

The numerical comparison between Jpeg–Jsteg, Chang and the proposed algorithm is presented in Table 1. These results demonstrated that the proposed method gives better results than other techniques. Figure 3 shows the images before and after embedded the secret bit. In addition, Figure 4 shows the histogram of images before and after embedded the secret bits.

Table 1: numerical comparison between Jpeg–Jsteg, Chang and the proposed algorithm

Baboon				
Algorithm	Size (Kbytes)	Capacity(bytes)	PSNR(db)	Correlation
Jsteg	16.8	13773	29.1777	0.9681
Cahng	14.9	53248	29.2715	0.9668
Proposed	14.7	130911	44.7670	0.9990
Lena				
Jsteg	10.1	10333	32.6824	0.9936
Cahng	10.5	53248	31.4143	0.9914
Proposed	11.3	130911	44.2082	0.9995
Girl				
Jsteg	7.35	7747	35.6348	0.9943
Cahng	7.72	53248	33.4638	0.9906
Proposed	8.55	130911	43.3132	0.9990
Pepper				
Jsteg	11.1	10615	34.8292	0.9963
Cahng	10.0	53248	32.5549	0.9937
Proposed	10.2	130911	42.6457	0.994



(a) original image of Baboon

(b) Stego image of Baboon using proposed method

(c) original image of Lena

(d) Stego image of Lena using proposed method

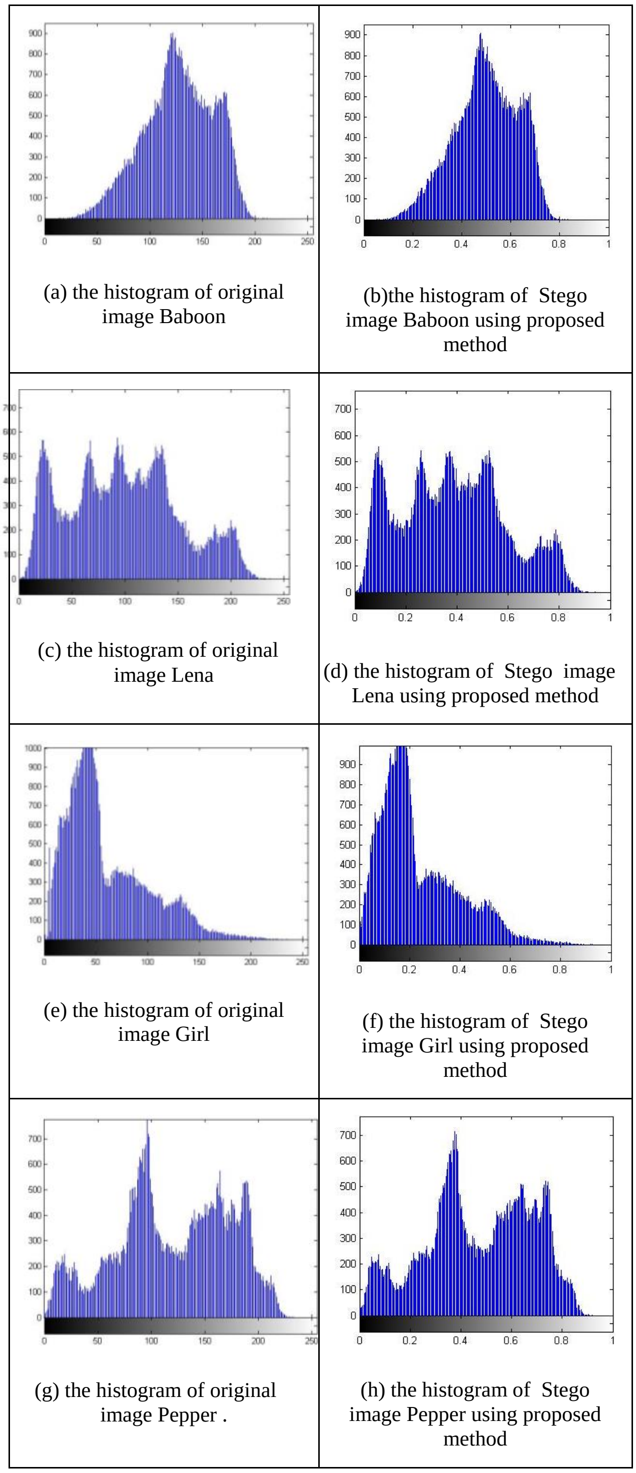
(e) original image of Girl

(f) Stego image of Girl using proposed method

(g) original image of Pepper

(h) Stego image of Pepper using proposed method

Figure 3: The images before and after embedded the secret bit



(a) the histogram of original image Baboon

(b)the histogram of Stego image Baboon using proposed method

(c) the histogram of original image Lena

(d) the histogram of Stego image Lena using proposed method

(e) the histogram of original image Girl

(f) the histogram of Stego image Girl using proposed method

(g) the histogram of original image Pepper .

(h) the histogram of Stego image Pepper using proposed method

Figure 4: The histogram of images before and after embedded the secret bit

5 Conclusion

The goal of data hiding is to make the secret messages hidden in the cover-images. In Jpeg–Jsteg, the message capacity that can be embedded in the cover-image is little small. 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 all part of the quantized DCT coefficients except the last block it is used to hide the message size. 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 as Jpeg–Jsteg. Overall, the proposed method matches the requirement of steganography with a larger message capacity than that of Jpeg–Jsteg.

References

[1] C. K. Chan, L. M. Cheng, “Hiding data in images by simple LSB substitution,” *Pattern Recognition*, vol. 37, pp. 469-474, 2004.

[2] C. C. Chang, T. S. Chen, and L. Z. Chung, “A steganographic method based upon JPEG and quantization table modification,” *Information Sciences*, vol. 141, pp. 123-138. 2002.

[3] A. Cheddad, J. Condell, K. Curran, and P. McKevitt “Digital image steganography: Survey and analysis of current methods,” *Signal Processing*, vol. 90 pp. 727-752, 2010.

[4] J. Lenti, “Steganographic methods,” *Periodica Polytechnica*, vol. 44, pp . 249-258, 2000.

[5] X. Li and J. Wang “A steganographic method based upon JPEG and particle swarm optimization algorithm,” *Information Sciences*, vol. 177, no. 15, pp. 3099-3109, 2007.

[6] S. K. Muttoo and Sushil Kumar “Data hiding in JPEG images,” *International Journal of Information Technology*, vol. 1, no.1, pp. 13-16, 2008 .

[7] N. Provos and P. Honeyman “Hide and seek: An introduction to steganography,” *IEEE Security and Privacy*, vol. 1, no. 3, pp. 32-43, 2003.

[8] M. Titchener, “Technical note: Digital encoding by way of new T-codes,” *IEE Proceedings - Computers and Digital Techniques*, vol. 131, no. 4, pp. 151-153, 1984.

[9] USC-SIPI image database, 2012. http://sipi.usc.edu/database/" accessed 2-2012

[10] A. Westfeld and A. Pfitzmann, “Attacks on steganogrphic systems,” in *3rd International Workshop on Information Hiding*, pp. 61-76, 1999.

[11] A. Westfeld, “F5-A steganographic algorithm: high capacity despite better steganalysis,” in *Proceedings of Fourth International Work- shop on Information Hiding*, LNCS 2137, pp. 289-302, Springer-Verlag, 2001.

[12] Q. Zhang, Y. Liu, Y. Nan, T. Zhao, and F. Liu “Classification algorithm of jsteg and F5 stego-images based on histogram difference,” *Energy Procedia*, vol. 13, pp. 8759-8766, 2011.

Mohammed Amin was graduated in mathematics in1983 at Menoufia University. He studied computer science from 1986 to 1989 at Ain Shams University in Cairo and received the M.Sc. degree in 1990 and the Ph.D degree in computer science in 1997 at the University of Gdansk, Poland. He is associate professor of computer science at the faculty of science, Menoufia University, and research visitor to the faculty of Philosophy and sciences of the Silesian University, Opava, Czech Republic. His research area in formal languages and their application in compiler design. Cooperating/distributed systems, web information retrieval, Petri nets and its applications, and finite automata and cryptograph.

Hatem Abdul-Kader obtained his BS and MSC, both in electrical engineering from the Alexandria University, Faculty of Engineering, Egypt, 1990 and 1995, respectively. He obtained his PhD degree in electrical engineering also from Alexandria University, Faculty of Engineering, Egypt in 2001. His areas of interest are data security and computer vision, and he is specialized in neural networks. He is currently an assistant professor in the Information Systems Department, Faculty of Computers and Information, Menofia University, Egypt, since 2004

Hani M. Ibrahem received the M.S. and Ph.D degrees in Computer Science at the University of Menoufyia, Egypt in 2004 and 2008, respectively. His research interests lies in the areas of image processing. Currently he is a lecture of Computer Science in the Faculty of Science, at the University of Menoufyia, Egypt.

Ahmed S. Sakr received his B.Sc degrees in Computer Science from Menoufia University, Egypt in 2008. His research interests lies in the areas of datahiding and cloud computing Currently he is a demonstrator of Computer Science in the Faculty of Science, at the University of Menoufyia, Egypt.