International Journal of Electrical and Computer Engineering (IJECE)
Vol. 3, No. 2, April 2013, pp. 230~237
ISSN: 2088-8708

A Method of Steganography – P Message with Q Coefficient (SPMQC)

Zeinab Famili*, Karim Faez, Abbas Fadavi***
* Department of Electrical, Computer and IT Eng., Azad University, Qazvin, Iran
** Department of Electrical Eng., Amirkabir University of Tech, Tehran, Iran
* Department of Mechatronics, Science and Research Branch, Islamic Azad Univercity, Semnan, Iran

Article Info

Article history:

Received Dec 21, 2012
Revised Feb 21, 2013
Accepted Mar 9, 2013

Keyword:

Steganography
Stego image
χ^2 -test

ABSTRACT

In this paper, we are going to propose a method for Steganography- which is based on deceiving χ^2 algorithm. Since the cover image coefficients and stego image coefficients histograms have significant differences for purposes of statistical properties, statistical analysis of χ^2-test reveals the existence of hidden messages inside stego image. We are introducing an idea for hiding messages in the cover image. It causes that DCT (Discrete Cosine Transforms) coefficient histogram not to have remarkable modification before and after embedding message. As a result, identifying the hidden message inside an image is impossible for an eavesdropper through χ^2 -test.
In this paper, we are proposing a better method with developing this algorithm. In fact, the capacity and the security of embedding messages increase extremely.

Corresponding Author:

Zeinab Famili,
Department of Electrical, Computer and IT Eng,
Islamic Azad University, Qazvin, Iran
Email: zeinab.famili@gmail.com

1. INTRODUCTION

Steganography is a hiding communication's knowledge [1], [2]. There are two main branches of steganography and digital watermarking in embedding information of image [3]. Each Steganographic communication system consists of an embedding algorithm and an extraction algorithm. To accommodate a secret message, the original image, also called the cover-image, is slightly modified by the embedding algorithm. As a result, the stego-image is obtained. Steganography goal is to hide message inside a cover image, so that the message is undetectable [4].

The hiding information process in a Steganographic system begins by identifying a cover medium's redundant bits, which can be modified without destroying that medium's integrity [5], [6], and then these redundant bits are replaced withthe data through the hidden messages. A simple method in the hiding system is replacing the bit message with the least significant bit of DCT coefficient. The classification of steganographic algorithms is into three categories: spatial domain, frequency domain and adaptive methods. Adaptive methods can either be applied in the spatial or frequency domains. A spatial domain technique generally uses the leastdirect significant bit (LSB) replacement technique [6]-[8]. The frequency domains based on methods such as discrete cosine transform (DCT), Fourier transforms (FT) and discrete wavelet transforms (DWT). Perceptual masking (PM) or adaptive steganography (AS) is the recent contribution in the domain [9], [10]. In this paper, we apply this method. Modifying the cover medium changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium's statistical properties. The system issecure if the stego images do not contain any detectable artifacts due to message embedding. It means that the stego images should have the same statistical properties as the cover images [11]. There are

different Steganographic algorithms which hide information in JPEG images [12], such as: Jsteg [13], JSteg-Shell [14], JPHide [15], Outguess [16], F5 algorithm [17], [18].

The plan of this paper is given by a brief review of JPEG image format in Section 2. In Section 3, we review statistical analysis. After presentingSteganographic 1 message with 2 coefficients in Section 4, Steganographic 2 message with 3 coefficients in Section 5 are discussed. We present out anew proposed method (Steganographic p message with q coefficients) in Section 6. In Section 7 we summarize theresults.

2. JPEG IMAGE FORMAT

JPEG is a popular and widely-used image file format and it has a de facto standard for network image transmission [19], [20]. If we apply JPEG (Joint Photographic Experts Group) images for data hiding; the stego-image will draw less attention of suspect rather than the most other formats. The JPEG image format uses a discrete cosine transform (DCT) to transform successive 8×8 pixel blocks of the image into each 64 DCT coefficients [21]. The DCT coefficients $F(u, v)$of an 8×8 block of image pixels $f(x, y)$ are given by Equation (1):

$$F(u,v)=\alpha(u)\alpha(v)\times\sum_{x=0}^{7}\sum_{y=0}^{7}f(x,y)\cos\left[\frac{(2x+1)u\pi}{16}\right]\cos\left[\frac{(2y+1)v\pi}{16}\right] \quad (1)$$

$u, v = 0, 1, 2\ldots N-1$

$$\alpha(u)=\sqrt{\frac{1}{N}}\quad u=0$$

$$\sqrt{\frac{2}{N}}\quad u=1,2\ldots N-1$$

Afterwards, the Equation (2) quantizes the coefficients:

$$F^{Q}(u,v)=round\left[\frac{F(u,v)}{Q(u,v)}\right] \quad (2)$$

The coefficients matrix is divided cell to cell into quantization matrix and their rounds are obtained by Equation (2). $Q(u, v)$, is a 64-element quantization table. (This table is given in reference [22]). The least-significant bits of the quantized DCT coefficients are as redundant bits. If $F^{Q}(u, v) \neq 0, 1$, then hidden message will embed in these bits. For more information about JPEG, refer to [22].

3. STATISTICAL ANALYSIS

At first, we arrange DCT coefficients to (2i, 2i+1) groups in terms of I (see table 1). In study of each group, we will realize that with LSB modification, the members of a group may change their orders and no member of one group conveys to other group.

Table1. Grouping the of two adjacent DCT coefficients according to i.

	Group1	Group2	Group3	Group4	….
2i	2	4	6	8	….
2i+1	3	5	7	9	….

For example, 8 and 9 are at the same group in table (1). With embedding 0 and 1 in the least significant bit, these numbers are converting to each other or itself.

As we are observing in Figure 1, the number eight doesn't change with embedding 0 in it's LSB, But the number nine converts to eight with embedding 0 in it's LSB.

Given uniformly distributed message bits, the probability of zeroand one are equivalent in message's bits. So, the numbers of 8 and 9 coefficients are almost equal after embedding with attention to Figure 1.

Given uniformly distributed message bits, the probability of zeroand one are equivalent in message's bits. So, the numbers of 8 and 9 coefficients are almost equal after embedding with attention to

Figure 1. Then, after embedding the number of coefficient which change from 2i to 2i+1 value is more than 2i+1 to 2i value.

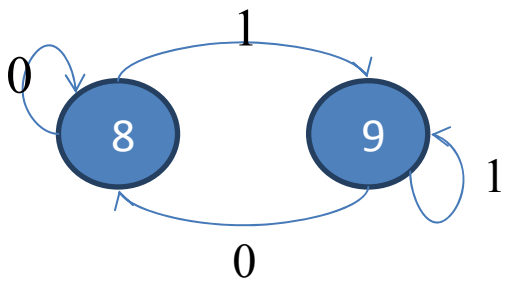

Figure 1. Changeable number of 8 and 9 with embedding 0, 1 in the their LSB

Figure 2 displays the histogram before and after a hidden message that it has been embedded in a JPEG image. Westfield and Pfitzmann observe that the embedding of encrypted data decrease the difference between coefficients histogram in each group inside given image [4], [12].

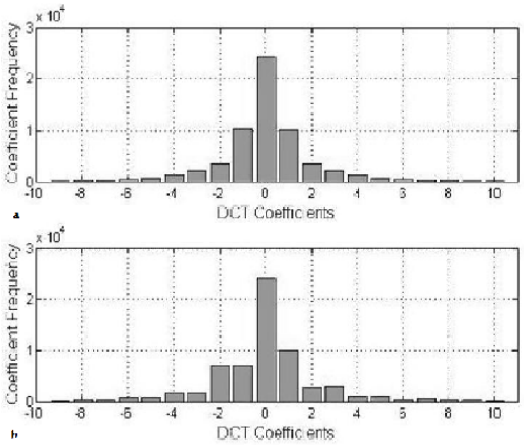

Figure 2. Frequency histograms. Sequential changes to the (a) original and (b) modified image's least-sequential bit of discrete cosine transform coefficients tend to equalize the frequency of adjacent DCT coefficients in the histograms.

We consider that $n_i$and $n_i^*$are the value of the histogram DCT coefficient in i before and after the embedding, respectively. As a result, $n_{2i}$and $n_{2i}^*$are the number of the histogram DCT coefficient in 2i before and after the message embedding, respectively. So n_{2i+1} is the number of n_{2i} adjacent coefficient and n_{2i+1}^* is the number of n_{2i}^* adjacent coefficient.
Given uniformly distribution of zero and one in message,The following relation is confirmed [4].

$$\left|n_{2i} - n_{2i+1}\right| \geq \left|n_{2i}^* - n_{2i+1}^*\right| \tag{3}$$

A χ^2- test used to determine whether the observed frequency distribution y_i in the image matches a distribution which shows distortion from embedding hidden data [12], [23]. Although we do not know the cover image, we know that the sum of adjacent DCT coefficients remain invariant, which lets us compute the expected distribution y_i^* from the stego image. Then we take the arithmetic concept,

$$y_i^* = \frac{n_{2i} + n_{2i+1}}{2} \tag{4}$$

To determine the expected distribution by equal (5) and compare with the observed distribution [4].

$$y_i = n_{2i} . \quad (5)$$

The χ^2 value for the difference between the distributions is given as:

$$\chi^2 = \sum \frac{(y_i - y_i^*)^2}{y_i^*} \quad (6)$$

Figure 3 displays the χ^2value during the hidden message in the LSB's coefficients of the image. As the χ^2value is decreasing with hidden message in LSB's coefficients, and then with study of χ2value, we realize that the message was hidden in the image.

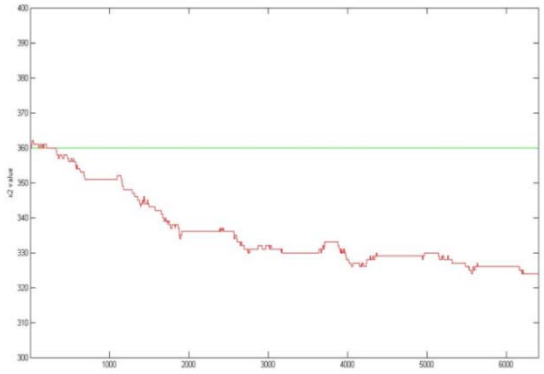

Figure 3. The grin line is χ^2 value for cove image and red line is χ^2 value during the hidden message.

4. STEGANOGRAPHY 1 MESSAGE WITH 2 COEFFICIENTS (S1M2C)

We proposed a new method in [24]. In this approach two sequential DCT coefficients only hide one message bit. First of all, we choose two sequential DCT coefficients that they are in the same group in Table 1.

Indeed, after applying the Steganography inside an image, χ^2 algorithm is operated on the basis of sensible modification which will increase the difference between Δn, and Δn*. In the next step, we calculate the following relation according to last description:

$$\Delta n = n_{2i} - n_{2i+1} \quad (7)$$

$$\Delta n^* = n_{2i}^* - n_{2i+1}^* \quad (8)$$

$$d = \Delta n - \Delta n^* \quad (9)$$

The goal of this approach is to minimize the d value by replacing two new DCT coefficients, according to the value of the sequential coefficients, and the hidden message and d value. For this approach we use of Table 2.

Table 2. This table indicate the new coefficient replacement according to the message bit to be 0 or 1.

Message bit	New Coefficient
0	(2i,2i) or (2i+1,2i)
1	(2i,2i+1) or (2i+1,2i+1)

For example, we assume *i* is equal to 4 (i= 4), and two sequential coefficients equal to (9, 8). For the purpose of a hiding message bit with zero value, we can replace (8, 8) or (9, 8) according to Table 2. There are three cases in choosing (8, 8) or (9, 8) in the example.

1- If d > 0, it means that the number of eights is less than its number in the cover image. So that, it should be converted one 9 to one 8. Therefore, we use (8, 8). As a result, one occurrence of the nines is decreased and it is increased to 8. So, d is decreased.

2 - If d = 0, it means that we don't need to change the number of eights and nines, then new coefficients are same (9, 8).

3 - If d < 0, it means that the number of eights is more than its frequency in the cover image. Thus, it should convert one 8 to one 9, because in transmitting this message, there isn'tany (9, 9) then we use (9, 8) until d doesn't become worst.

General convert method (approach) is in [24]. The Steganography 1 message with 2 coefficients approach had been explained that χ^2 value of stego image is nearly equal to χ^2 value of cover image, but the capacity of embedding message decreases to 50%.

5. PROPOSEDMETHODFORSTEGAANOGRAPHY 2 MESSAGE WITH 3 COEFFICIENTS (S2M3C)

As we considered the consequences last section, we can hide one message with two coefficients. To avoid of decreasing capacity in hidden information, we propose another method. In this approach two message are hidden with three coefficients.

First of all, we choose three sequential DCT coefficients that they can convert to each other after the embedding message bit.

According to the value of three coefficients and the hiding message bits, dthree coefficients are replaced by three new coefficients. With due attention to two message bits to be 0, or 1, we create the Table 3 for new coefficients. These three coefficients are chosen optional for hiding messages.

Table 3. This table indicate the new coefficient replacement according to two message bits to be 0 or 1.

Message bit1	Message bit2	New Coefficients
0	0	(2i,2i,2i) or (2i,2i,2i+1)
0	1	(2i,2i+1,2i) or (2i,2i+1,2i+1)
1	0	(2i+1,2i,2i) or (2i+1,2i,2i+1)
1	1	(2i+1,2i+1,2i) or (2i+1,2i+1,2i+1)

We show general convert method of steganography 2 message with 3 coefficients in Table 4. For example, in second row of Table 4; three old sequential coefficients are (2i, 2i, 2i) respectively, and two message bits that we want to embed are (0, 0) and d value is equal to 0. It means that Δn hasn't changed after the embedding. So, the number of 2i and 2i+1coefficients are fit and they don't need to change. Thus, the new coefficients will be (2i, 2i, 2i) according to Table 4.

Another example, in third row of Table 4: three old sequential coefficients are (2i, 2i, 2i) consecutively, and the message bits that we want to embed are (0, 0) and d value is less than zero (d<0). It means that the Δn has been increased after the embedding. There for, we should decrease difference between Δn, and Δn^*. With attention to Table 3, we are replacing (2i, 2i, 2i+1) of new coefficients that it increase the number of 2i+1 coefficients.

In another example, we consider fourth row in Table 4: three old sequential coefficients are (2i, 2i, 2i) consecutively, and the message bits that we want to embed are (0, 1) and d value is more than zero (d>0). It means that the Δn has been decreased after the embedding. Therefore, we should increase difference between Δn, and Δn^*. Because in transmitting this messages, there isn't any choice for increasing the number of 2i coefficients. Thus, we are replacing (2i, 2i, 2i) coefficients.

As we considered in three previous example, in some rows d value is inclined to zero (the difference between Δn, and Δn^* are decreasing). But in some rows, d value couldn't incline to zero. In addition, some rows have special situation, like 91 row of Table 4, to decrease d value we should increase 2i value in this row. We put (2i+1, 2i, 2i+1) coefficients in table (4) but if the d value is more than one (d>1), we can't follow the Table 4 and with attention to Table 3 we replace (2i+1, 2i, 2i) coefficients, until the d value incline to zero with double speed.

6. PROPOSEDMETHODFORSTEGAANOGRAPHY P MESSAGE WITH Q COEFFICIENTS (SpMqC)

We have hidden 1 message with 2 coefficients and 2 messages with 3 coefficients at two previous sections. In this section, our goal is to generalize this approach with p messages and q coefficients. Therefore, we choose q coefficients and with due attention to p messages and d value, q new coefficients are replacing.

For example:
S3M4C...Steganography 3 Message with 4 Coefficients
S2M4C…Steganography 2 Message with 4 Coefficients.

The table of transferring S2M4C has shown in the following. With due attention to Table 5 and d value, we can create a table for embedding 2 messages with 4 coefficients as previous section.

Table 4. Some part of 96 states in new general convert method

n	old coefficients	Message bits	d	new coefficient
1	(2i, 2i, 2i)	(0, 0)	>0	(2i, 2i, 2i)
2	(2i, 2i, 2i)	(0, 0)	=0	(2i, 2i, 2i)
3	(2i, 2i, 2i)	(0, 0)	<0	(2i, 2i, 2i+1)
4	(2i, 2i, 2i)	(0, 1)	>0	(2i, 2i+1, 2i)
5	(2i, 2i, 2i)	(0, 1)	=0	(2i, 2i+1, 2i)
6	(2i, 2i, 2i)	(0, 1)	<0	(2i, 2i+1, 2i+1)
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
49	(2i+1, 2i, 2i)	(0, 0)	>0	(2i, 2i, 2i)
50	(2i+1, 2i, 2i)	(0, 0)	=0	(2i, 2i, 2i+1)
51	(2i+1, 2i, 2i)	(0, 0)	<0	(2i, 2i, 2i+1)
52	(2i+1, 2i, 2i)	(0, 1)	>0	(2i, 2i+1, 2i)
53	(2i+1, 2i, 2i)	(0, 1)	=0	(2i, 2i+1, 2i)
54	(2i+1, 2i, 2i)	(0, 1)	<0	(2i, 2i+1, 2i+1)
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
91	(2i+1, 2i+1, 2i+1)	(1, 0)	>0	(2i+1, 2i, 2i+1)
92	(2i+1, 2i+1, 2i+1)	(1, 0)	=0	(2i+1, 2i, 2i+1)
93	(2i+1, 2i+1, 2i+1)	(1, 0)	<0	(2i+1, 2i, 2i+1)
94	(2i+1, 2i+1, 2i+1)	(1, 1)	>0	(2i+1, 2i+1, 2i)
95	(2i+1, 2i+1, 2i+1)	(1, 1)	=0	(2i+1, 2i+1, 2i+1)
96	(2i+1, 2i+1, 2i+1)	(1, 1)	<0	(2i+1, 2i+1, 2i+1)

As we perceived in last paper [24], the most important weakness was low capacity of embedding. But we can apply this approach for T9M10C and steganography 9 messages with 10 coefficients. As a result, the capacity of embedding increases to 90%.

Transferring table has been enlarged with increasing of p and q and the steganographer should consider to more messages and coefficients. Then the time of calculations increases. Indeed, with attention to eavesdroppers how are encountering with many images in internet, on the contrary of steganographers how are always embedding one image, the calculation costs isn't important in case of increasing security.

Table 5. This table indicate the 4 new coefficients replacement according to two message bits to be 0 or 1.

Message Bit1	Message Bit1	New Coefficients
0	0	(2i,2i,2i,2i) or (2i,2i,2i,2i+1) or (2i,2i,2i+1,2i) or (2i,2i,2i+1,2i+1)
0	1	(2i,2i+1,2i,2i) or (2i,2i+1,2i,2i+1) or (2i,2i+1,2i+1,2i)or (2i,2i+1,2i+1,2i+1)
1	0	(2i+1,2i,2i,2i) or (2i+1,2i,2i,2i+1) or (2i+1,2i,2i+1,2i) or (2i+1,2i,2i+1,2i+1)
1	1	(2i+1,2i+1,2i,2i)or(2i+1,2i+1,2i,2i+1)or (2i+1,2i+1,2i+1,2i)or(2i+1,2i+1,2i+1,2i+1)

7. RESULTS AND ANALYSIS

Our proposed algorithm is applied on 20 different images. The set of USC_SIPI images have been used in the performance of algorithm. We introduce their result in Table 6. According to relation (9), the d value is accounted for 20 images and their average round is in Table 6. For example, in Table 6, d (4, 5) =7. It means that the average value of d is equal to 7 for steganography 4 messages with 5 coefficients. The cells that we don't discuss about them have specified with the sign of multiplication.
The average of d value for these 20 images is equal to 56 with using of Jsteg steganography method. As a result this method is recognized withχ^2–test.

Looking at the Table 6, we realize that the χ^2-test doesn't effect on the proposed methods perfectly. In addition, the capacity of embedding in proposed methods increased rather than previous method [24]. For instance, the capacity of embedding got 66% for S2M3C method (in row 2 and column 3) and the capacity of embedding got 77% for S7M9C method (in row 7 and column 9).

Table 6. This table indicates applied result of proposed algorithm on 20 images. Each cell show value d for Steganography p Message with q Coefficients.

P \ Q	1	2	3	4	5	6	7	8	9	10
1	56	1	0	0	0	0	0	0	0	0
2	×	56	1	0	0	0	0	0	0	0
3	×	×	56	3	0	0	0	0	0	0
4	×	×	×	56	7	1	0	0	0	0
5	×	×	×	×	56	10	2	0	0	0
6	×	×	×	×	×	56	12	3	1	0
7	×	×	×	×	×	×	56	13	4	1
8	×	×	×	×	×	×	×	56	15	5
9	×	×	×	×	×	×	×	×	56	17

The number of cells increases with adding messages and coefficients and it is default for us to find the best converted table. We use the casual tables in this research and reach a good result that shows deceit of χ^2 algorithm with these methods. To find out the method which specifies the best table for more messages and coefficients will be considered in future.

REFERENCES

[1] P Moulin, R Koetter. Data-hiding codes. Proceedings of the IEEE. 2005; 93(12): 2083-2126.
[2] S Lyu, H Farid. Steganalysis using higher-order image statistics. *IEEE Transactions on Information Forensics and Security*. 2006; 1(1): 111–119.
[3] Katzenbeisser S, Petitcolas FAP. *On Defining Security in Steganographic Systems.* Proceedings of SPIE: Electronic Imaging 2002, Security and Watermarking of Multimedia Contents. California. 2002; 4675.
[4] N Provos, P Honeyman. Hide and seek: an introduction to steganography. *IEEE Security & Privacy*. 2003; 1(3): 32-44.
[5] Qingzhong Liu, Andrew H Sung, BernardeteRibeiro, Mingzhen Wei, Zhongxue Chen, Jianyun Xu. Image complexity and feature mining for steganalysis of least significant bit matching steganography. *Information Sciences*. 2008; 178(1): 21-36.
[6] K Bailey, K Curran. An evaluation of image based steganography methods. *Multimedia Tools and Applications*. 2006; 30(1): 55–88.
[7] VM Potdar, S Han, E Chang. *Fingerprinted secret sharing steganography for robustness against image cropping attacks*. Proceedings of IEEE Third International Conference on Industrial Informatics (INDIN), Perth, Australia. 2005: 717–724.
[8] G Cancelli, GJ Do¨err, M Barni, IJ Cox. *Acomparativestudyof±1 steganalyzers*. Proceedings of IEEE 10th Workshop on Multimedia Signal Processing, MMSP. 2008: 791–796.
[9] AI Hashad, AS Madani, AEMA Wahdan. *A robust steganography technique using discrete cosine transform insertion.* Proceedings of IEEE/ITI Third International Conference on Information and Communications Technology, Enabling Technologies for the New Knowledge Society. 2005: 255–264.
[10] K Bailey, K Curran. An evaluation of image based steganography methods. *Multimedia Tools and Applications*. 2006; 30(1): 55–88.
[11] B Chen, GW Wornell. Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding. *IEEE Trans. Information Theory.* 2001; 47(4): 1423–1443.
[12] B Li, YQ Shi, J Huang. *Steganalysis of YASS.* Poceedings of 10th ACM Workshop on Multimedia and Security. Oxford, United Kingdom. 2008; 139–148.

[13] T Zhang, X Ping. *A Fast and Effective Steganalytic Technique against JSteg-like Algorithms.* Proc. 8th ACM Symp. Applied Computing. 2003.
[14] RSA Data Security. The RC4 Encryption Algorithm. 1992.
[15] K Solanki, A Sarkar, BS Manjunath. *YASS: yet another stegano- graphic scheme that resists blind steganalysis.* Proceedings of the Ninth International Workshop on Information Hiding, Saint Malo, France. 2007; 4567: 16–31.
[16] NielsProvos. *Defending Against Statistical Steganalysis.* Proceedings of the10th USENIX Security Symposium. 2001: 323-335.
[17] J Fridrich, T Pevny, J Kodovsky. *Statistically undetectable JPEG steganography: dead ends, challenges, and opportunities*. Proceedings of the ACM NinthWorkshop on Multimedia & Security. Texas, USA. 2007: 3–14.
[18] J Fridrich, M Goljan, D Hogea. *Steganalysis of JPEG Images: Breaking the F5 Algorithm*. Proc. 5th Int'l Workshop Information Hiding. Springer-Verlag. 2002.
[19] GW Wallace. The JPEG Still Picture Compression Standard. Communications of the ACM. 1991; 34(4): 30–44.
[20] AC Popescu. Statistical tools for digital image forensics. Ph.D. Dissertation, Department of Computer Science, Dartmouth College, USA, 2005.
[21] AM Fard, M Akbarzadeh-T, F Varasteh-A. A new *genetic algorithm approach for secure JPEG steganography*. Proceedings of IEEE International Conference on Engineering of Intelligent Systems. 2006; 1–6.
[22] Gonzalez & Woods Digital *Image Processing*.
[23] P Civicioglu, M Alci, E Besdok. Impulsive noise suppression from images with the noise exclusive filter, EURASIP *Journal on Applied Signal Processing*. 2004; (16): 2434–2440.
[24] Zainab Famili, Karim Faez, Abbas Fadavi. A NewSteganography based on χ^2 Technic. CIARP 2009, LNCS5856. Springer-Verlag Berlin Heidelberg. 2009: 1062-1069.

BIOGRAPHIES OF AUTHORS

Zeinab Famili was born in Semnan, Iran in 1980. He received his B.Sc. degree in Electronic Engineering from Azad university of Garmsar, Garmsar, Iran, in 2005 and the M.Sc. degree in Electronicfrom Islamic Azad UnivercityGazvin, Semnan, Iran in 2009. His researchinterests include Image Processing, Neural Networks.z_electron590@yahoo.com

Karim Faez was born in Semnan, Iran. He received his BSc. degree in Electrical Engineering from Tehran Polytechnic University as the first rank in June 1973, and his MSc. and Ph.D. degrees in Computer Science from University of California at Los Angeles (UCLA) in 1977 and1980 respectively. Professor Faez was with Iran Telecommunication Research Center (1981-1983) before Joining Amirkabir University of Technology (Tehran Polytechnic) in Iran in March1983, where he holds the rank of Professor in the Electrical Engineering Department. He was the founder of the Computer Engineering Department of Amirkabir University in 1989 and he has served as the first chairman during April 1989-Sept. 1992. Professor Faez was the chairman of planning committee for Computer Engineering and Computer Science of Ministry of Science, Research and Technology (during 1988-1996). His research interests are in Biometrics Recognition and authentication, Pattern Recognition, Image Processing, Neural Networks, Signal Processing, Farsi Handwritten Processing, Earthquake Signal Processing, Fault Tolerance System Design, Computer Networks, and Hardware Design. Dr. Faez coauthored a book inLogic Circuits published by Amirkabir University Press. He also coauthored a chapter in the book: *Recent Advances in Simulated Evolution and Learning*, Advances in Natural Computation, Vol. 2, Aug. 2004. World Scientific. He published about 300 articles in the above area. He is a member of IEEE, IEICE, and ACM, a member of Editorial Committee of Journal of IranianAssociation of Electrical and Electronics Engineers, and International Journal of Communication Engineering. Emails: kfaez@aut.ac.ir, kfaez@ieee.org, kfaez@m.ieice.org.

Abbas fadavi was born in Sari, Iran in 1978. He received the B.S. degree in electronic engineering from Azad university of Garmsar, Garmsar, Iran, in 2005 and the M.Sc. degree in Mechatronics from Science and Research Branch, Islamic Azad Univercity Semnan, Semnan, Iran in 2012. His research interests include Image Processing, Pattern Recognition, Algoritm Optimization, and Neural Networks.