Journal of Engineering Science and Technology
Vol. 8, No. 5 (2013) 508 - 520

A NEW TECHNIQUE BASED ON CHAOTIC STEGANOGRAPHY AND ENCRYPTION TEXT IN DCT DOMAIN FOR COLOR IMAGE

MELAD J. SAEED

Department of Computer Science, University of Mosul, Mosul, Iraq
E-mail: meladjader@yahoo.com

Abstract

Image steganography is the art of hiding information into a cover image. This paper presents a new technique based on chaotic steganography and encryption text in DCT domain for color image, where DCT is used to transform original image (cover image) from spatial domain to frequency domain. This technique used chaotic function in two phases; firstly; for encryption secret message, second; for embedding in DCT cover image. With this new technique, good results are obtained through satisfying the important properties of steganography such as: imperceptibility; improved by having mean square error (MSE), peak signal to noise ratio (PSNR) and normalized correlation (NC), to phase and capacity; improved by encoding the secret message characters with variable length codes and embedding the secret message in one level of color image only.

Keywords: Steganography, Encryption, DCT, Chaotic, Color image.

1. Introduction

The appearance of the internet is considered to be one of the major events of the last years. Information become available on-line, all users who have a computer can easily connect to the internet and search for the information they want to find [1]. Two techniques are available to achieve this goal: one is cryptography, 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 [2]. One of disadvantages of security protection is that the cipher texts are vulnerable to attack because they usually seem to be jumbled codes [3].

The second method is steganography, where the secret message is embedded in

Nomenclatures

$C(i, j)$	Dimension of original image
M	Number of rows in the image
N	Number of columns in the image
$S(i, j)$	Dimension of Stego_image
w_i	The i plaintext character
X	Number of bits in chaotic number
$X_{o,r}$	Initial values for chaotic equation
Y	Number of bits for letters

Abbreviations

ASCII	American student code information interchange
DCT	Discrete cosine transform
LSB	Least significant bit
MSE	Mean squared error
NS	Normalize correlation
PSNR	Peak signal to noise ratio

another image or message. Using this technology even the fact that a secret is being transmitted has to be secret [4, 5]. The goal of steganography is to mask the very presence of communication, making the true message indiscernible to the observer. It must have high imperceptibility, security level and payload attributes [6].

Text information has two key properties: one is that relation of words is very close. Because of this property, attackers can deduce the whole text once they decrypt some words. The other is that transmitting the character code is strict with security. Once one bit of the character code is changed in the process of transmitting, the decipher of the character is not correct. So this paper introduces the chaotic encryption method and the error-correct method when the text information is hidden and transmitted by a still image. The characters of the given text by ASCII code are encoded and encrypt these character codes by a chaotic sequence. They are also encoded by using chaotic map and embed them into DCT coefficients of a carrier image to transmit them [7].

In the proposed method Discrete Cosine Transform (DCT) is applied to the given cover image to get the DCT coefficients. The DCT transforms cover image from an image representation into a frequency representation, by grouping the pixels into non-overlapping blocks of 8×8 pixels and transforming the pixel blocks into 64 DCT coefficients each [8-10]. A modification of a single DCT coefficient will affect all 64 image pixels in that block. The DCT coefficients of the transformed cover image will be quantized, and then modified according to the secret data. DCT coefficients determine the randomized pixel locations for hiding to resist blind steganalysis methods such as self-calibration process by cropping some pixels to estimate the cover image features. Many experimental results prove this scheme is feasible and effective [11].

2. Related Work

A simple way of steganography is based on modifying the least significant bit layer of images, known as the *LSB technique* [12]. The LSB technique directly

embeds the secret data within the pixels of the cover image. In some cases LSB of pixels visited in random or in certain areas of image and sometimes increment or decrement the pixel value [13]. Some of the recent research studied the nature of the stego and suggested new methodologies for increasing the capacity. Habes [14] proposed a new method (4 least significant) for hiding secret image inside carrier image. In this method each of individual pixels in an image is made up of a string of bits. He took the 4-least significant bit of 8-bit true color image to hold 4-bit of the secret message /image by simply overwriting the data that was already there.

The schemes of the second kind embed the secret data within the cover image that has been transformed such as DCT (discrete cosine transformation). Chang et al. [9] proposed a novel steganography method based on JPEG. The DCT for each block of 8×8 pixels was applied in order to improve the capacity and control the compression ratio. Chen [15] used DCT technique in steganography in which during embedding process sender split the cover image to 8x8 pixel blocks, each block encode one secret bit. Before communication started the sender and receiver agree previously on the location of two DCT coefficients which will be used in embedding process, comparison done between these two values, if we want to embed secret bit 1, we must check these two values the first one should be greater than second value if not we must swap their positions. Same thing for embedding 0, second point should be greater than first point if not swapping done. Development has been done on previous DCT method by Zhao and Koch [16], in which they have used three points instead of two points, for comparison. Hiding secret 1, $p_1>p_2$ and $p_1>p_3$; while for embedding 0, $p_1>p_2$ and $p_1>p_3$. This will give cover image higher robustness against attacks. Banoci et al. [17] presented Code Division Multiple Access Technique, where the embedding process is carried out by hiding secret image in each block of quantized DCT coefficients. Chen et al. [18] discussed different steganography tool algorithms and classified the tools into spatial domain, transform domain, document based, file structure based and other categories such as spread spectrum technique and video compressing encoding. Agarwal and Savvides [19] proposed a steganographic method to hide biometric data in DCT coefficients of the cover image in a more robust way.

3. Chaotic Signal

The chaotic signals are like noise signals but they are completely certain, that is if we have the primary quantities and the drawn function, the exact amount will be reproduced. The advantages of this signal are as follows [20, 21]:

- **The sensitivity to the primary conditions**

This means a minor change in primary amount will cause a significant difference in subsequent measures. It means if we have a little change in the signal amount, the final signal will be completely different.

- **The apparently accidental feature**

In comparison with productive accidental natural number in which the range of the numbers cannot be produced again, the technique used for producing the accidental number in algorithm based on the chaotic function will prepare the

ground that if we have the primary quantities and the drawn function, we can produce the numbers again.

- **The deterministic work**

As the chaotic functions have the accidental manifest, they are completely exact. It means as we have the drawn function and the primary quantities we can produce and reproduce sets of numbers seemingly have no system and order. Equation (1) shows one of the most famous signals which has chaotic features and is known as the Logistic Map signal.

$$X_{n+1}=rX_n\,(1-X_n) \tag{1}$$

In which the X_n will get the numbers between [0,1], the signal shows three different chaotic features in three different range based on the division of r parameter of which the signal feature will be as well by considering $X_o = 0.3$.

- if $r \in [0,3]$, then the signal feature in the first 10 repetition showed some chaos and after that it was fixed, Fig. 1(a)[22],

- If $r \in [3, 3.57]$, then the signal feature in the first 20 repetition showed some chaos and after that it was fixed, Fig. 1(b) [6],

- If $r \in [3.57, 4]$, then the signal feature is completely chaotic, Fig. 1(c) [6].

According to the given description and the research requirements for the complete chaotic features for image steganography, the logistic map chaotic signals with the primary values of $X_o = 0.3$ and $r \in [3.57, 4]$ are used.

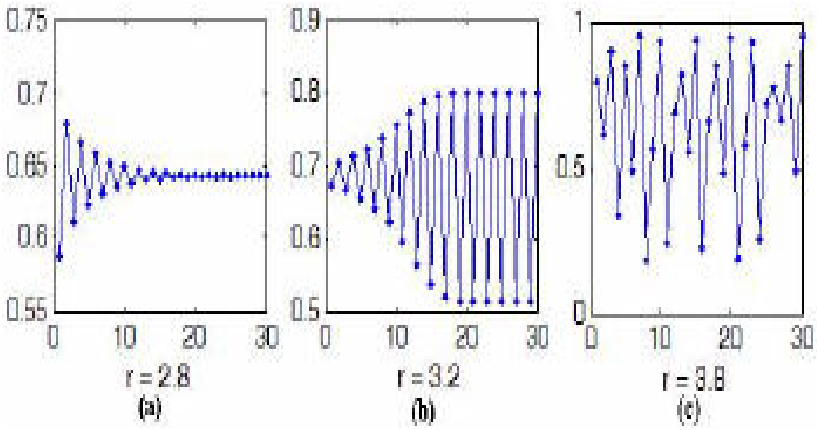


Fig. 1. The Logistic Map Chaotic Signal with $X_o = 0.3$ and (a) $r \in [0,3]$, b) $r \in [3, 3.57]$, c) $r \in [3.57, 4]$ [6, 22].

4. Text Information Algorithms

The text algorithms for text information and the flow charts for extracting and hiding text information are shown below:

- **Algorithm for Encryption text information**

Input: Secret message.

1. Begin
2. A piece of given text information is $w^0 = (w_1^0, w_2^0, ...w_n^0) = \{ w_i^0 | i = 1,2,...,n \}$. Firstly, we encode ith character w_i^0 of the text by ASCII code (i=1, 2,…,n) and denote characters w_i^0 8 binary bits $(w_{i7}, w_{i6}, w_{i6}, w_{i5}, w_{i4}, w_{i3}, w_{i2}, w_{i1}, w_{i0})$. The secret message must ended (.).
3. Calculate number of rows that text contained and number of letters in each row.
4. Use chaotic map to generate the chaotic number using Eq. (1) that equals to number of rows.
5. Convert each chaotic number to binary, that's number of bits in equal to number of bits for letter in each row.
   X=Y X: number of bits in chaotic number
   Y: number of bits for letters
6. In each row, shift sequence of letters that equivalents to '0' to the beginning of row.
7. Repeat this step, until last row, that's number to binary bit equals the number of bit in secret text subtract eight.
   $X = Y - 8$ (for (.) which not be encrypted).
8. End

Output: Encrypted Secret message

- **Algorithm for Hiding Encrypted text information into a carrier image in DCT domain**

Input: color image, Encrypted Secret message.

1. Begin
2. Giving a carrier color image whose size is M X N.
3. Take only one level of color image (red or green or blue) to hide inside of it after convert to DCT, we choose (green).
4. Using chaotic map to create random numbers as in Eq. (1) by using value of x_o and r.
5. Convert chaotic number to decimal and use it as index in image.
6. Take the content of index in image.
7. Check, if the number is negative, get the digit 5 and 6.
   Else, get the digit 4 and 5.
8. Convert these two digits to equivalent binary numbers.
9. Remark, the position of ones in digit 4, if the number is negative, or digit if number is positive.
10. Replace the position of ones in digit 4 or 5, by bit from encrypted secret text in equivalent position in digit 5 or 6.
11. Repeat this step until the end of encrypted text.
12. Convert that level to original place in image.
13. Convert that image to spatial domain.
14. End.

Output: Stego_imag

Figure 2 shows the flowchart of Hiding Encrypted text information into a carrier image in DCT domain.

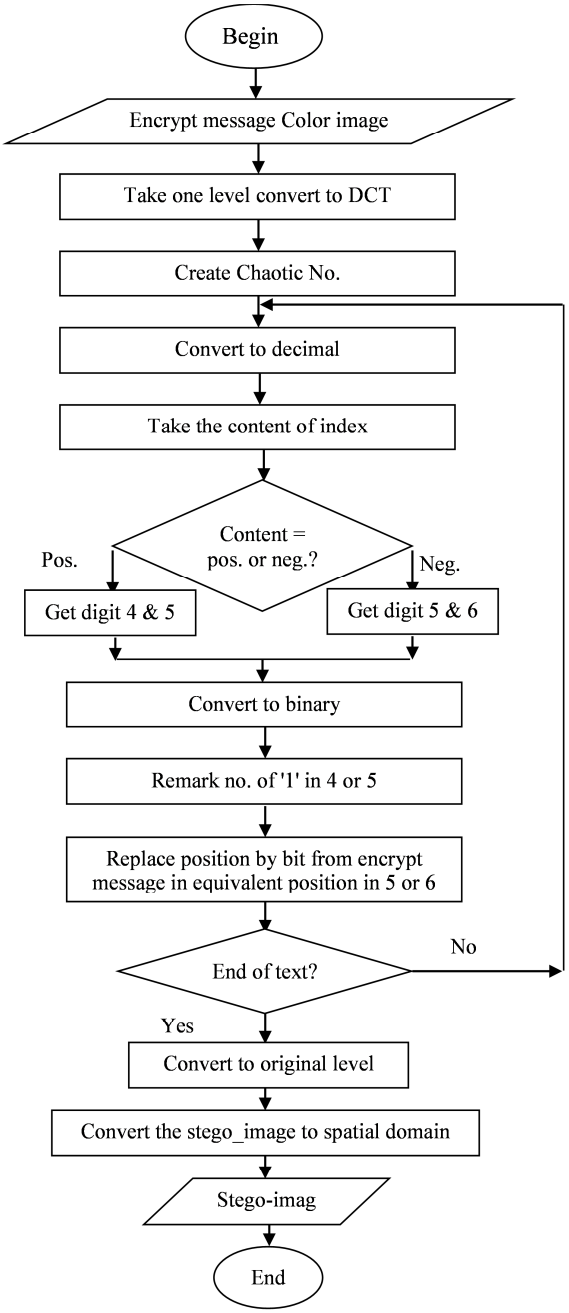


Fig. 2. Flowchart of Hiding Text Information into a Carrier Image in DCT Domain.

- **Algorithm for Extracting text information from the embedded image in DCT**

Input: Stego_imag

1. Begin
2. Get the level of stego-image that contains the secret text (green).
3. Convert the stego_imag to DCT domain.
4. Using chaotic map to create random numbers as in Eq. (1) by using the same value of x_o and r that using in algorithm of hiding.
5. Convert chaotic number to decimal and use it as index in image.
6. Take the content of index in image.
7. Check, if the number is negative, get the digits 5 and 6.
   Else, get the digits 4 and 5.
8. Convert these two digits to equivalent binary numbers.
9. Remark, the position of ones in digit 5, if the number is negative, or digit 4 if number is positive.
10. Take the bit from the equivalent place in digit 6 or 5 that equal bits of encrypted secret massage.
11. Repeat steps 7, 8, 9, and 10.
12. Using chaotic map to create random numbers as in Eq. (1)
13. Convert the random number to binary numbers.
14. Return the bits '0' that shifted to the begin of rows, to original place depend on position in binary no..
15. Block the encrypted massage to block of 8 bits.
16. Convert each block to character.
17. If character equal to '.' go 18 else, repeat 7, 8, 9, 10
18. End

Output: secret message, color image.

Figure 3 shows the flowchart of extracting text information from the embedded image in DCT.

5. Simulation Results

In order to evaluate validity of the proposed schema, three color samples used as host images as shown in Fig. 4. A secret text of different size is used to embed.

First, the secret message encrypted using algorithm (Encryption text information) that uses $X_0[0 \le X_0 \le 1]$, and r $[3.5 \le r \le 4]$; which are the two keys for encryption, choose $X_0 = 0.00015$ and $r = 3.6$ as shown in Fig. 5.

Second, use the image and encrypted message as the input to algorithm (Hiding text information into a carrier image in DCT domain) that use chaotic map with $X_0 = 0.88$ and $r = 4$, to produce stego_image as shown in Fig. 6. Flowchart of extracting process is shown in Fig. 7.

From Figs. 8(a) and (b) it can be seen that they are almost the same. This means that the algorithm did not damage the cover image. To test the equality of the approach for embedding secrete message in DCT image, the following measures are used. The Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Normalize Correlation (NC) are given by

$$\text{MSE}= \frac{1}{[N \times N]^2} \sum_{i=1}^{N} \sum_{j=1}^{N} [C(ij) - S(ij)]^2 \quad (2)$$

$$PSNR = 10 \log_{10} 255^2 / MSE \quad db \tag{3}$$

$$NC = \sum_i \sum_j C(i,j) S(i,j) / \sum_{i=1}^{n} \sum_{j=1}^{n} [C(i,j)]^2 \tag{4}$$

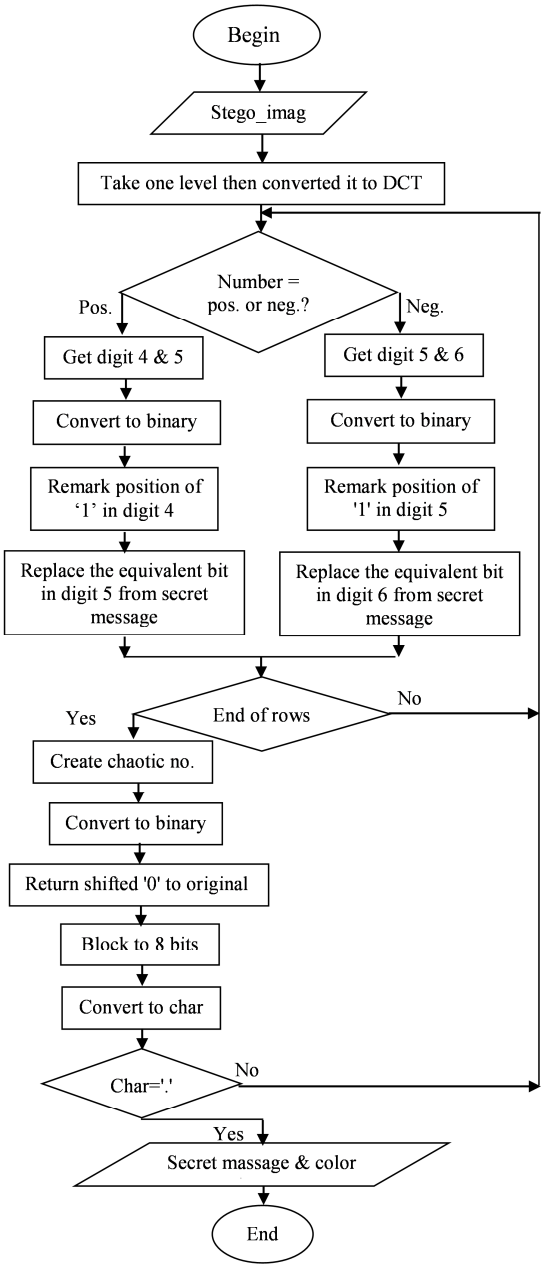


Fig. 3. Flowchart of Extracting Text Information from the Embedded Image in DCT.

Fig. 4. Cover Images.

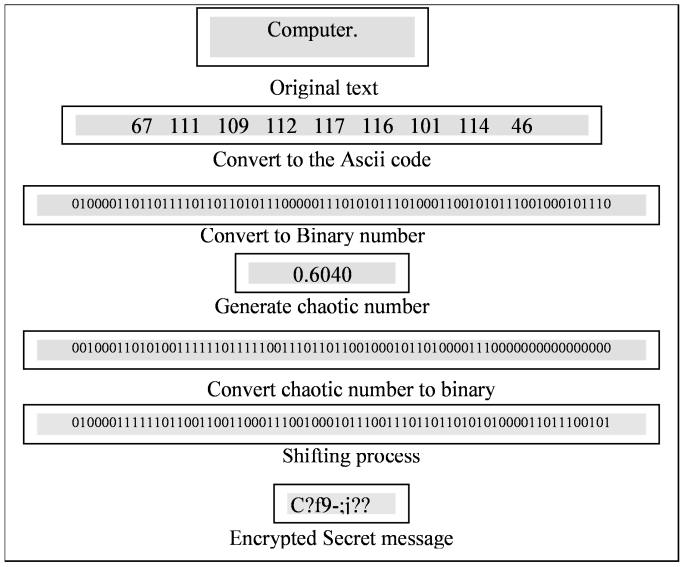


Fig. 5. Encrypting Process.

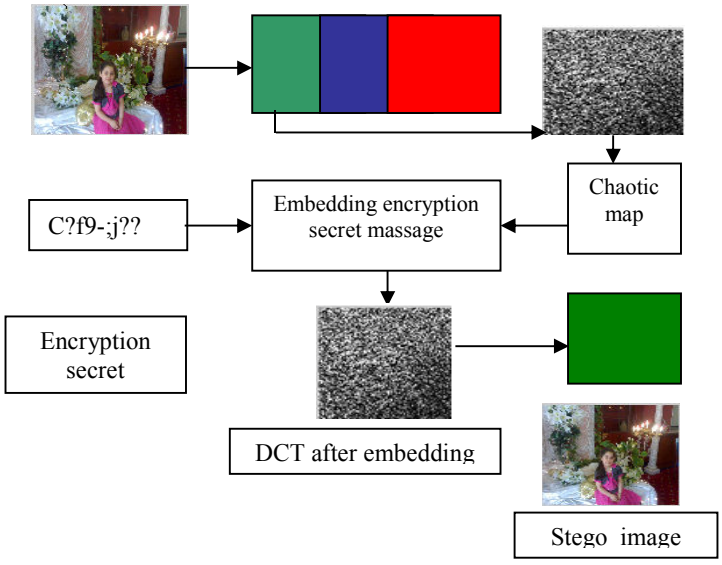


Fig. 6. Embedding Process.

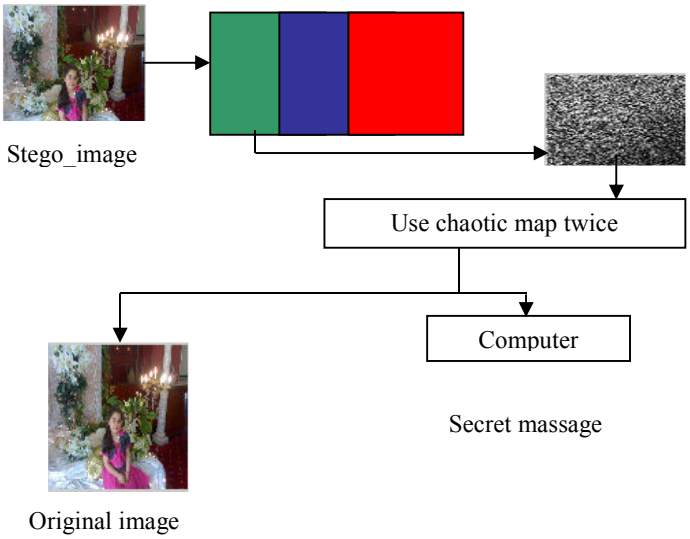
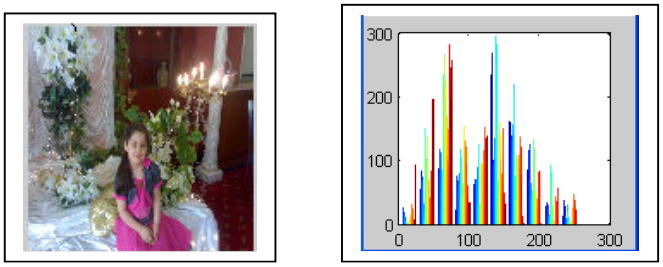
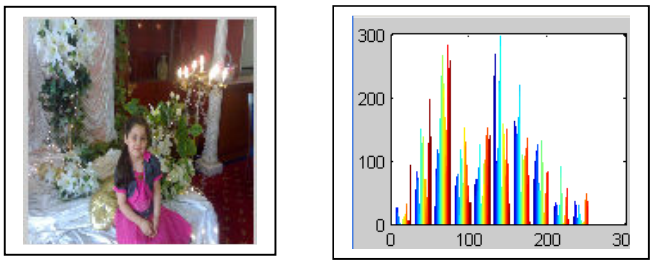


Fig. 7. Extracting Process.



(a) Cover image with its histogram.



(b) stego_image with its histogram.

Fig. 8. Girl Image before and after Embedding Secret Message with Histogram.

Table 1 shows the measurement of MSR, PSNR and NC of our proposed algorithm for three samples:

Table 1. The Measurements MSR, PSNR and NC.

Name of image	MSE	PSNR	NC	Stego_image
Girl	0.0584	60.5072	1	
Boy	0.0315	63.1627	1	
Sun	0.0516	61.0275	1	

The capacity of this algorithm depends on numbers of ones in digits after converted to binary, if the digit content a lot of ones the capacity increases, if not the capacity decreases.

With this new technique, we got very good result through satisfying and improving the most important properties of steganography such as: imperceptibility, improved by having the MSE near to (0) and PSNR greater than 60, security, improved by using Encryption and steganography with chaotic.

6. Conclusions

A new algorithm hiding technique is proposed in this paper using chaotic logistic map. This algorithm is simple, fast, and efficient and has high imperceptivity. The chaotic logistic map has been used in encrypting and embedding with DCT which increases the security and imperceptivity because the sensitivity of logistic map to initial condition leads to generate different sequence with different initial value. As seen in experimental results using DCT in embedding will not damage cover images which reflect by value of correlation that equal 1, it means high identical between the cover before and after embedding.

Acknowledgments

The researcher would like to thank the anonymous reviewers for their valuable suggestions.

References

1. Popa, R. (1998). *An analysis of steganographic techniques*. The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering.
2. Negrat, k.; Smko, R.; and Almarimi, A. (2010). Variable length encoding in multiple frequency domain steganography. *2nd International Conference on Software Technology and Engineering* (*ICSTE*), V1-305-V1-309.
3. Liu, N.; and Guo, D. (2007). Multiple image information hiding technique based on chaotic sequences. *International Conference on Convergence Information Technology*, 1720-1725.
4. Lenti, J. (2000). Steganographic methods. *Periodica Polytechnica*, *Electrical Engineering and Computer Science*, 44(3-4), 249-258.
5. Anderson, R.; and Petitcolas, F.A.P. (1998). On the limits of steganography. *IEEE Journal of Selected Areas in Communications*, *Special Issue on Copyright & Privacy Protection*, 16(4), 474-482.
6. Katzenbeisser, S., and Petitcolas, F.A.P. (1999). *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House Print on Demand.
7. Yang, S.-G.; Li, C.-X.; and Sun, S.-H. (2007). Text information hiding method based on chaotic map and BCH code in DWT domain of a carrier image. *The first International Symposium on Data, Privacy, and E-commerce*, 239-241.
8. Krenn, R. (2004). Steganography and Steganalysis. http://www.krenn.nl/ univ/cry/steg/article.pdf.
9. Chang, C.-C.; Chen, T.-S.; and Chung, L.-Z. (2002). A steganographic method based upon JPEG and quantization table modification. *Information Sciences*, 141(1-2), 123-138.
10. Chu, R.; You, X.; Kong, X.; and Ba, X. (2004). A DCT-based image steganographic method resisting statistical attacks. *Proceedings of (ICASSP '04), IEEE International Conference on Acoustics, Speech, and Signal Processing*, 5, V-953-6.
11. Danti, A.; and Acharya, P. (2010). Randomized Embedding Scheme Based on DCT Coefficients for Image Steganography. *IJCA Special Issue on "Recent Trends in Image Processing and Pattern Recognition*", 2, 97-103.
12. Zhi, L.; Fen, S.A.; and Xian, Y.Y. (2003). A LSB steganography detection algorithm. 14th *IEEE Proceedings on Personal*, *Indoor and Mobile Radio Communications*, 3, 2780-2783.
13. Fridrich, J.; and Goljan, M. (2003). Digital image steganography using stochastic modulation. In *Security and Watermarking of Multimedia Contents V*, Vol. 5020, 191-202.
14. Habes, A. (2005). 4 least significant bits information hiding implementation and analysis. *ICGST Int. Conf. on Graphics, Vision and Image Processing* (GVIP-05), Cairo, Egypt.
15. Chen, P.-C. (1999). *On the study of watermarking application in www-modeling, performance, analysis, and applications of digital image watermarking systems*. Master Thesis, National Tsing Hua University.

16. Zhao, J.; and Koch, E. (1995). Embedding robust labels into image for copyright protection. *In Proceedings of the International Congress on Intellectual Property Rights for Information, Knowledge and New Techniques*, Munchen, Wein, Oldenbourge Verlag.
17. Banoci, V.; Bugar, G.; and Levicky, D. (2009). Steganography systems by using CDMA techniques. *International Conference on Radioelectronika*, 183-186.
18. Chen, M.; Zhang, R.; Niu, X.; and Yang, Y. (2006). Analysis of current steganographic tools: Classifications and features. *International Conference on Intelligent Hiding and Multimedia Signal Processing*, 384-387.
19. Agarwal, N.; and Savvides, M. (2009). Biometric data hiding: A 3 factor authentication approach to verify identity with the single image using steganography, encryption and matching. *International Conference on Computer vision and pattern recognition*, 85-92.
20. Enayatifar, R.; Mahmoudi, F.; and Mirzaei, K. (2009). Using the chaotic map in image steganography. *International Conference on Information Management and Engineering*, 491-495.
21. Enayatifar, R.; Mohamad, F.; and Mirzaei, K. (2008). Image encryption with chaotic map and binary search tree. *5th Iranian Conference on Machine Vision and Image Processing*.
22. Ahmed, H.E.H.; Kalash, H.M.; and Farag Allah, O.S. (2007). An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption. *Informatica*, 31(1), 121-129.