A Modified High Capacity Image Steganography Technique Based on Wavelet Transform

Ali Al-Ataby[1] and Fawzi Al-Naima[2]
[1]Department of Electrical Engineering and Electronics, University of Liverpool, UK
[2]Department of Computer Engineering, Nahrain University, Iraq

Abstract: *Steganography is the art and science of concealing information in unremarkable cover media so as not to arouse an eavesdropper's suspicion. It is an application under information security field. Being classified under information security, steganography will be characterized by having set of measures that rely on strengths and counter measures (attacks) that are driven by weaknesses and vulnerabilities. Today, computer and network technologies provide easy-to-use communication channels for steganography. The aim of this paper is to propose a modified high-capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security.*

Keywords*: Steganography, security, wavelets, cryptography, and information hiding.*

Received August 17, 2008; accepted August 3, 2009

1. Introduction

Steganography is a type of hidden communication that literally means "covered writing" (from the Greek words *stegano* or "covered" and graphos or "to write"). The goal of steganography is to hide an information message inside harmless cover medium in such a way that it is not possible even to detect that there is a secret message [8, 12, 13].

Oftentimes throughout history, encrypted messages have been intercepted but have not been decoded. While this protects the information hidden in the cipher, the interception of the message can be just as damaging because it tells an opponent or enemy that someone is communicating with someone else. Steganography takes the opposite approach and attempts to hide all evidence that communication is taking place.

Essentially, the information-hiding process in a Steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity). The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. Modern steganography's goal is to keep its mere presence undetectable, but steganographic systems, because of their invasive nature, leave behind detectable traces in the cover medium through modifying its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium's statistical properties. The process of finding these distortions is called Statistical Steganalysis.

2. Information-Hiding System Features

An information-hiding system is characterized be having three different aspects that contend with each other as shown in Figure 1: capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information [6].

Generally speaking, information hiding relates to both watermarking and steganography. A watermarking system's primary goal is to achieve a high level of robustness-that is, it should be impossible to remove a watermark without degrading the data object's quality. Steganography, on the other hand, strives for high security and capacity, which often entails that the hidden information is fragile. Even trivial modifications to the stego medium can destroy it.

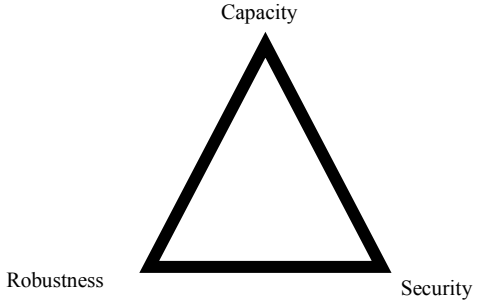


Figure 1. Information-hiding system features.

3. Steganography System

A classical steganographic system's security relies on the encoding system's secrecy. Although such a system might work for a time, once it is known, it is simple enough to expose the entire received media (e.g., images) passing by to check for hidden messages ultimately, such a steganographic system fails.

Modern steganographic system, as shown in Figure 2 attempts to be detectable only if secret information is known namely, a secret key. In this case, cryptography should be involved, which holds that a cryptographic system's security should rely solely on the key material. For steganography to remain undetected, the unmodified cover medium must be kept secret, because if it is exposed, a comparison between the cover and stego media immediately reveals the changes [4, 6].

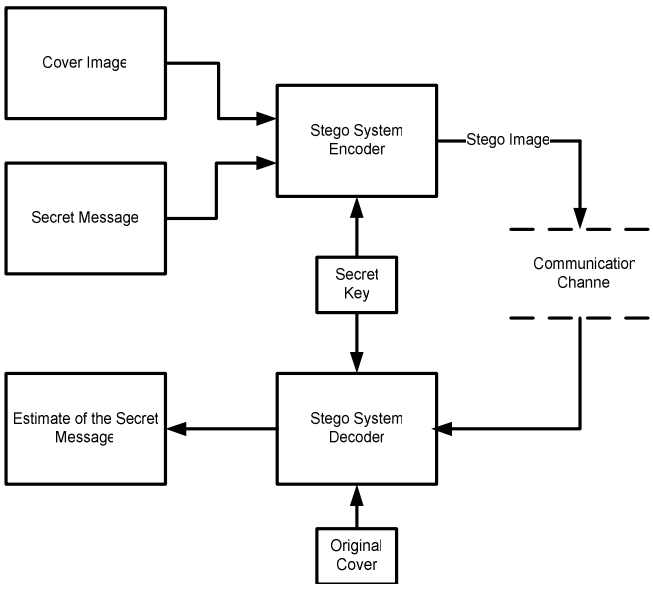


Figure 2. A modern steganography system.

Three basic types of stego systems are available:

- Pure stego systems - no key is used.
- Secret-key stego systems - secret key is used.
- Public-key stego systems - public key is used.

The technique that is followed in this paper will use secret key to encrypt the hidden message that will be encapsulated inside a cover media.

4. The Use of Wavelet Transform in Steganography

The Wavelet domain is growing up very quickly. A lot of mathematical papers and practical trials are published every month. Wavelets have been effectively utilized as a powerful tool in many diverse fields, including approximation theory; signal processing, physics, astronomy, and image processing [1, 15].

Many practical tests propose to use the Wavelet transform domain for steganography because of a number of advantages that can be gained by using this approach. The use of such transform will mainly address the capacity and robustness of the Information-Hiding system features. The work described in this paper implements steganography in the Wavelet domain. The hierarchical nature of the Wavelet representation allows multi-resolutional detection of the hidden message, which is a Gaussian distributed random vector added to all the high pass bands in the Wavelet domain. It is shown that when subjected to distortion from compression, the corresponding hidden message can still be correctly identified at each resolution in the Discrete Wavelet Transform (DWT) domain [1, 14, 15].

A Wavelet is simply, a small wave which has its energy concentrated in time to give a tool for the analysis of transient, non-stationary or time-varying phenomena. A signal can be better analyzed if expressed as a linear decomposition of sums of products of coefficient and functions. A two-parameter system is constructed such that one has a double sum and coefficient with two indices. The set of coefficients are called the DWT of a signal. In Wavelet transform, the original signal (1-D, 2-D, 3-D) is transformed using predefined wavelets. The wavelets are orthogonal, orthonormal, or biorthogonal, scalar or multiwavelets [2, 10].

The DWT used in this paper is implemented using the functions available with MATLAB to simplify the analysis and minimize development time. The following discussion illustrates the idea of Wavelet transformation as applied to the area of image processing [10].

4.1. One-Dimensional Wavelet Decomposition

A single- level one- dimensional Wavelet decomposition with respect to either a particular Wavelet or particular Wavelet decomposition filters is illustrated in Figure 3.

Starting from a signal s, two sets of coefficients are computed: approximation coefficients *cA1*, and detail coefficients *cD1*. These vectors are obtained by convolving *s* with the low-pass filter *Lo_D* for approximation and with the high-pass filter *Hi_D* for detail, followed by dyadic decimation. The length of each filter is equal to *2N*. If *n* is the length of s, the signals *F* and *G* are of length *n + 2N - 1*, and then the coefficients *cA1* and *cD1* are of length *[(n-1)/2] +N*.

4.2. Multilevel 2-D Wavelet Decomposition

For images, an algorithm similar to the one-dimensional case is possible for two-dimensional Wavelets and scaling functions obtained from one-dimensional ones by tensor product [4]. This kind of two-dimensional DWT leads to a decomposition of

approximation coefficients at level j in four components: the approximation at level $j+1$, and the details in three orientations (horizontal, vertical, and diagonal), as depicted in Figure 4.

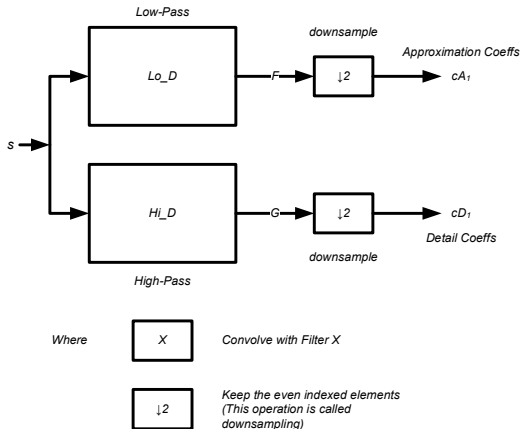


Figure 3. One dimensional wavelet decomposition filters.

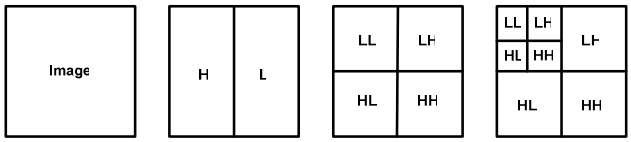


Figure 4. Two dimensional wavelet transformation of an image.

Figure 5 describes the basic decomposition step for images using the 2D Wavelet transform. Also, different levels of Wavelet transform were tried in this paper (up to 5). Increasing the levels will add complexity and computational overhead, but the robustness of the steganography method will be enhanced [10].

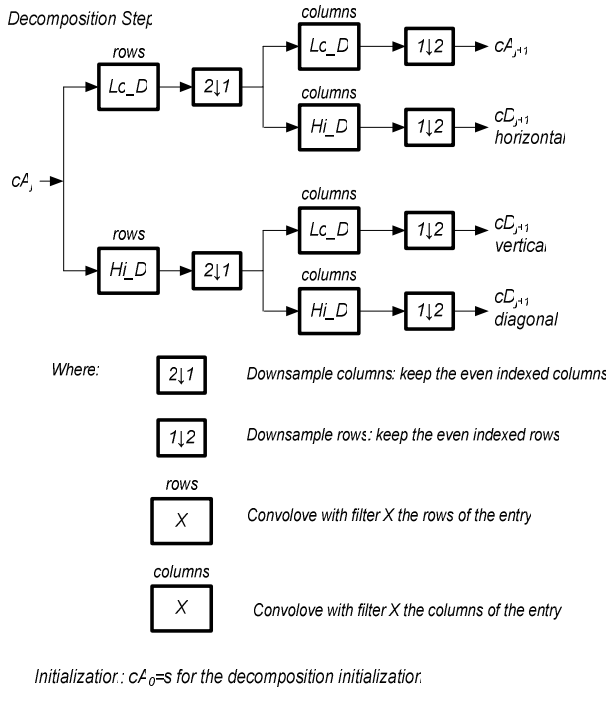


Figure 5. Two dimensional wavelet decomposition.

4.3. Wavelet Filters

In order to use the Wavelet transform, Wavelet filters should be selected and used in the transformation and inverse-transformation. For that purpose, a lot of theoretical work is available to illustrate different Wavelet filters with different features. For the purpose of fast analysis and development, the Wavelet filters available with MATLAB Wavelet toolbox were selected and tested [10, 14, 15]. Available orthogonal or biorthogonal Wavelets are listed in the Table 1 [10].

Table 1. Wavelet families.

Wavelet Families	Wavelets (MATLAB Notation)
Daubechies	'db1' or 'haar', 'db2', ... ,'db10', ... , 'db45'
Coiflets	'coif1', ... , 'coif5'
Symlets	'sym2', ... , 'sym8', ... ,'sym45'
Discrete Meyer	'dmey'
Biorthogonal	'bior1.1', 'bior1.3', 'bior1.5' 'bior2.2', 'bior2.4', 'bior2.6', 'bior2.8' 'bior3.1', 'bior3.3', 'bior3.5', 'bior3.7' 'bior3.9', 'bior4.4', 'bior5.5', 'bior6.8'
Reverse Biorthogonal	'rbio1.1', 'rbio1.3', 'rbio1.5' 'rbio2.2', 'rbio2.4', 'rbio2.6', 'rbio2.8' 'rbio3.1', 'rbio3.3', 'rbio3.5', 'rbio3.7' 'rbio3.9', 'rbio4.4', 'rbio5.5', 'rbio6.8'

In this paper, different Wavelet families were tried in the transformation. However, sym4 was chosen as a case study.

5. Cryptography and Steganography

The use of cryptography as a way to secure the hidden message mainly addresses the security requirement in the Information-Hiding system. For the purpose of steganography, symmetric encryption is followed. The symmetric encryption is a method of encryption that uses the same key to encrypt and decrypt a message. If one person encrypts and decrypts data, that person must keep the key secret. If the data is transmitted between parties, each party must agree on a shared secret key and find a secure method to exchange the key [9].

The security of encrypted data depends on the secrecy of the key. If someone gains knowledge of the secret key, he or she can use the key to decrypt all the data that was encrypted with the key [9, 11]. Table 2 shows common algorithms for symmetric key encryption.

No encryption method is completely secure. Given knowledge of the algorithm and enough time, attackers can reconstruct most encrypted data. A strong algorithm (the one that is built on sound mathematical methods, creates no predictable patterns in encrypted data, and has a sufficiently long key) can deter most attacks [3, 9, 11].

Table 2. Common algorithms for symmetric key encryption.

Algorithm	Key Length
Data Encryption Standard	56-Bit Key
Triple DES	Three DES Operations, 168-Bit Key
Advanced Encryption Standard (AES)	Variable Key Lengths
International Data Encryption Algorithm (IDEA)	128-Bit Key
Blowfish	Variable Key Lengths
RC4	Variable Key Lengths

When a strong algorithm is used, the only way to break the encryption is to obtain the key. An attacker can obtain a key by stealing it, by tricking someone into revealing the key (a form of social engineering), or by trying all possible key combinations. This last method is commonly known as a brute force attack. Increasing the key length exponentially increases the time that it takes an attacker to perform a brute force attack.

Table 3 shows the average time (theoretically) required to decrypt an encrypted massage versus key length using the brute force attack. Increasing key length will increase the strength of the encryption algorithm on the expense of complexity and computation overhead [3, 9].

Table 3. Decryption time using Brute force attack method.

Key Length (in bits)	Time to Decrypt
10	Less than 1 second
20	21 seconds
30	6 hours
40	255 days
64	Almost 12,000 years
128	Over 200 septillion years (a number with 27 digits), longer than the life of the universe

Going through the details of the encryption algorithms is out of the scope of this paper. In order to utilize the encryption in this work, a Microsoft encryption utility program is used to encrypt the hidden message. This utility encrypts a stream of data with different algorithms (IDEA, DES, Triple DES, MDC, and RC4) depending on the user choice. As a case study, RC4 method was used in this paper with 56-bit key.

6. The Proposed Method

Although steganography is applicable to all data objects that contain redundancy, in this paper, JPEG images are considered only. People often transmit digital pictures over email and other Internet communication, and JPEG is one of the most common formats for images. Moreover, steganographic systems for the JPEG format seem more interesting because the systems operate in a transform space and are not affected by visual attacks. (Visual attacks mean that steganographic messages can be seen on the low bit planes of an image because they overwrite visual structures; this usually happens in BMP images).

Figure 6 shows a general representation of the proposed steganography method. The proposed method contains the following steps that were implemented using MATLAB 7.6.

Step 1: image statistics-aware test.

Input: Cover image
Output: Cover image
Action: Test the cover image:
If the cover image contains unrecognizable patterns and passes the histogram test then the cover image is accepted
Else search for another cover image.
End

Step 2: image pre-processing and correction.

Input: Cover image
Output: Pre-processed cover image
Action: The following corrections will be done:
For each pixel in the cover image apply level correction end
For each pixel in the cover image apply contrast correction end
For each pixel in the cover image apply color balance correction end
End

Step 3: DWT transformation.

Input: Pre-processed cover image
Output: DWT transformed cover image
Action: Convert the pre-processed cover image to Wavelet domain through 2D Wavelet transform
End

Step 4: threshold calculation/ identification of the size of redundancy.

This step will calculate the threshold (T) that will be used to define what is the size (the space) of the redundancy in the cover image that can be used to imbed the message (or part of the message) in. Calculation of the threshold is done via statistical means. The following is one of the possibilities that have been followed in this paper:

$$T = \frac{\alpha}{N} \sum^{N} |J_w| \quad (1)$$

where J_w's are the coefficients of the DWT for the cover image, N is the number of coefficients. From practical best practice, it was found that this equation should be scaled by a correction factor α (between 0

and 1). Note that this factor is a function of the message nature and will affect the size of the cover image that will be used to embed the hidden message. The step is summarized as follows:

Input: DWT transformed cover image
Output: size of the information (s) that can be hidden inside the cover image, DWT of the cover image
Action: threshold (T) calculation
For each pixel in the transformed cover image do
get next DWT coefficient
if the value of the DWT coefficient < T, then store the index of the coefficient, s=s+1
end
End

Step 5: message partitioning.

Input: value of s, secret message
Output: 1D bit stream of the message with size s
Action: convert the message to 1D bit stream
End

Step 6: strong key encryption.

Input: 1D bit stream of the message with size s
Output: encrypted bit stream of the message
Action: encrypt the 1D bit stream of the message with RC4, key length=56
End

Step 7: encrypted message DWT transformation.

Input: encrypted bit stream of the message
Output: DWT transform of the encrypted message.
Action: transform the encrypted bit stream of the message to Wavelet domain
End

Step 8: stego image formation.

Input: DWT of the cover image (step 4), DWT transform of the encrypted message.
Output: stego image
Action:

a. *Place the DWT coefficients of the encrypted message in the location specified previously in the DWT of the cover message.*
b. *Inverse DWT transform the result.*

End

7. Experimental Results

Over 500 JPG images were tested using the proposed method. Fundamentally, data payload (capacity) of a steganographic system is used as one of the evaluation criteria. Data payload can be defined as the amount of information it can hide within the cover media. As with any method of storing data, this can be expressed as a number of bits, which indicates the max message size that might be inserted into an image. It can be expressed as a percentage from the full image size.

According to the proposed method, the redundancy is expressed in the Wavelet domain according to the threshold value T as shown in equation 1. Hence, the payload will be linked directly to the threshold factor. From practical observations, it was found that the value of T will increase if the size of the image increases (this in fact is expected due to the wide image range).

Usually, the invisibility of the hidden message is measured in terms of the Peak Signal-to-Noise Ratio (PSNR) [5, 7]:

$$PSNR = 10 Log_{10} (S^2 / MSE) \quad (2)$$

where:

$$S^2 = \frac{1}{m * n} \sum_{i=1}^{m} \sum_{j-1}^{n} J^2(i, j) \quad (3)$$

and the Mean Square Error (MSE) defined as:

$$MSE = \frac{1}{m * n} \sum_{i=1}^{m} \sum_{j=1}^{n} [J(i, j) - J'(i, j)]^2 \quad (4)$$

where J' represents the pixel in the stego image (the result of the steganography system). The Root Mean Square Error (RMSE) is used also as a measurement criterion. *RMSE* is defined as follows:

$$RMSE = \sqrt{MSE} = \sqrt{\frac{1}{m * n} \sum_{i=1}^{m} \sum_{j=1}^{n} [J(i, j) - J'(i, j)]^2} \quad (5)$$

Usually, the high payload (or capacity) requirement will conflict with the high PSNR requirement. Generally speaking, when the payload increases, the MSE (or RMSE) will increase, and this will affect the PSNR inversely. So, a trade-off should be made between payload (capacity) and *PSNR* requirements. It was found from practical observation that:

$$\alpha \uparrow \quad MSE \uparrow \quad RMSE \uparrow \quad Payload \uparrow \quad PSNR \downarrow \quad (6)$$

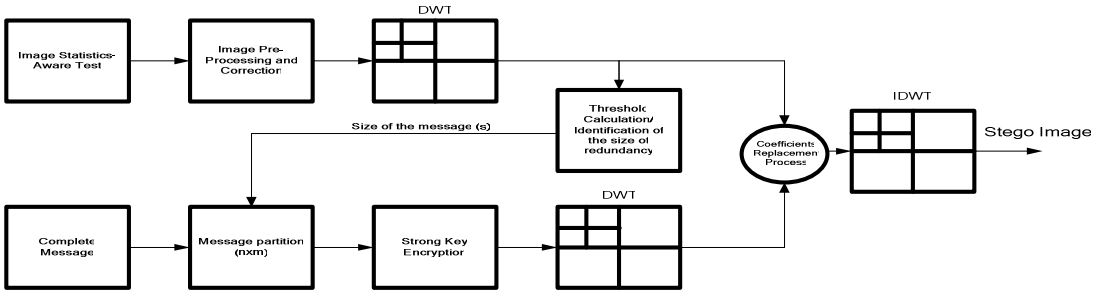
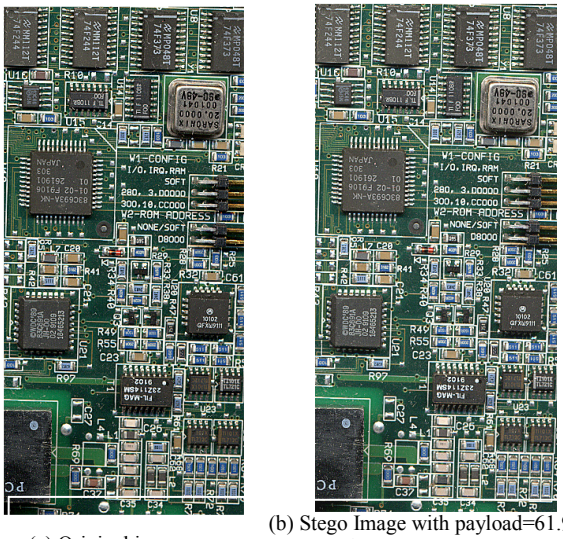


Figure 6. General representation for the proposed steganography method.

In other words, the higher the value of α refer to equation 1, the higher the values for *MSE*, *RMSE*, and Payload, and the lower the value of *PSNR*, and vice versa (as expected). Figure 7 shows an output for the proposed method.



(a) Original image.

(b) Stego Image with payload=61.92 % and *MSE*=1.93 % (α=0.5).

Figure 7. Experimental result from the proposed method on an image with (306x648) pixels.

Table 4 shows some simulation results (for the same image shown in Figure 7. Note that the results shown in the table will vary depending on the nature of the cover image.

Table 4. The effect of α on MSE, payload (capacity) and Peak SNR (For the image of Figure 7).

α	MSE %	Payload %	PSNR dB
0.3	0.70	49.99	40.98
0.4	1.24	56.83	36.29
0.5	1.93	61.92	32.57
0.6	2.77	65.84	29.58
0.7	3.79	69.01	27.02
0.8	4.96	71.61	24.81
0.9	6.27	73.83	22.84

Note that the payload values shown in the table are the maximum ones. In real life scenarios, lower values of payload will be used (the actual embedding into the cover image is less that the theoretical boundaries.).

It was found practically that the proposed method generates a stego image that will be immune to statistical steganalysis (using histogram technique and other methods [16]). The variation in the envelope of the stego image will not indicate that there is hidden message inside the image. Recall that the cover image was processed before using it in the proposed method. Also, the hidden message was converted to the Wavelet domain before placing it in the Wavelet version of the cover image. This will lead to more effective embedding of the message inside the cover image.

8. Concluding Remarks

As far as data hiding using steganography is concerned, two primary objectives are interesting: the technique that will be used for steganography should provide the maximum possible payload, and the embedded data must be imperceptible to the observer. It should be stressed on the fact that steganography is not meant to be robust. Any modifications to the file, such as conversions between file types, standard image processing (compression, filtering, …etc.,), or geometrical editing (rotation, resizing, cropping, *..etc.*,) are expected to affect (and may remove) the hidden bits from the file.

The proposed method pre-adjusts the original cover image in order to guarantee that the reconstructed pixels from the embedded coefficients would not exceed its maximum value and hence the message will be correctly recovered. Then, it uses Wavelet transform to transform both the cover image and the hidden message. Wavelet transform allows perfect embedding of the hidden message and reconstruction of the original image [5, 7].

It was found that the proposed method allows high payload (capacity) in the cover image with very little effect on the statistical nature of it. This is of course on the expense of reducing PSNR and increasing the MSE (and hence RMSE). The results of the proposed method were compared with the results obtained after applying the same techniques mentioned above but with the transform being FFT. The comparison was in favor of DWT as expected due to the ability of Wavelet transform to compress data and introducing sparsity, hence increasing the capacity or payload of the steganography process. Wavelet transform has been used extensively in the last few years in the image processing field, ranging from noise suppression or de-noising to image coding and compression.

The extraction of the hidden message was not shown and it is out of the scope of this paper. In general, the extraction will follow a reverse approach to that shown above, with knowledge of the secret key and the places of the hidden message coefficients in the cover image.

The drawback of the proposed method is the computational overhead. The method requires resources from the computer hardware (mainly processor speed and memory (RAM)). With the fast development in the hardware manufacturing area, this problem will become trivial.

Finally, steganography subject is still young, not mature, and the work on it will continue to increase the capacity, security, and robustness. Since these factors contend with each other, the new methods will try to make the best trade-off.

References

[1] Bilgin A., Sementilli J., Sheng F., and Marcellin W., "Scalable Image Coding Using Reversible Integer Wavelet Transforms," *Computer Journal of Image Processing IEEE Transactions*, vol. 9, no. 4, pp. 1972 - 1977, 2000.

[2] Calderbank R., Daubechies I., Sweldens W., and Yeo L., "Lossless Image Compression Using Integer to Integer Wavelet Transforms," *in Proceedings of International Conference on Image Processing*, USA, pp. 596-599, 1997.

[3] Fridrich J., Goljan M., Soukal D., and Holotyak T., "Forensic Steganalysis: Determining the Stego Key in Spatial Domain Steganography," *in Proceeding of Electronic Imaging SPIE*, Spain, pp. 631-642, 2005.

[4] Johnson N. and Jajodia S., "Steganography: Seeing the Unseen," *IEEE Computer Magazine*, vol. 25, no. 4, pp. 26-34, 1998.

[5] Lee K. and Chen H., "A High Capacity Image Steganographic Model," *in IEEE Proceedings on Vision Image and Signal Processing*, China, pp. 288-294, 2000.

[6] Lin T. and Delp J., "A Review of Data Hiding in Digital Images," *in Proceedings of the Image Processing, Image Quality, and Image Capture Conference*, Georgia, pp. 274-278, 1999.

[7] Lo Y., Topiwala S., and Wang J., "Wavelet Based Steganography and Watermarking," *Wavelets Reports*, Cornell University, http://dukiedoggie.tripod.com/cornell/wavelets/report.html, 1998.

[8] Lu S., *Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property*, Idea Group Publishing, 2005.

[9] Microsoft Press, *Fundamentals of Network Security*, Microsoft Official Curriculum, 2003.

[10] Misiti M., Misiti Y., Oppenheim G., and Poggi J., *Wavelet Toolbox for Use with MATLAB*, User Guide MathWorks Inc., 2000.

[11] Naor M. and Reingold O., "On the Construction of Pseudo Random Permutations," *Computer Journal of Cryptography*, vol. 12, no. 1, pp. 29-66, 1999.

[12] Popa R., "An Analysis of Steganographic Techniques," *Working Report on Steganography,* Faculty of Automatics and Computers, 1998.

[13] Provos N. and Honeyman P., "Hide and Seek: An Introduction to Steganography," *Computer Journal of IEEE Security and Privacy Magazine*, vol. 2, no. 3, pp. 32-40, 2003.

[14] Tolbal F., Ghonemy A., Taha A., and Khalifa S., "Using Integer Wavelet Transforms in Colored Image Steganography," *International Journal on Intelligent Cooperative Information Systems,* vol. 4, no. 2, pp. 230-235, 2004.

[15] Walker S., *A Premier of Wavelets and Their Scientific Applications*, CRC Press, 1999.

[16] Westfeld A. and Bohme R., "Exploiting Preserved Statistics for Steganalysis," *in Proceedings of 6th International Workshop on Information Hiding*, Canada, pp. 82-96, 2004.

Ali Al-Ataby received both degrees of BSc (first place at the university with Honors) in electronics and communications engineering, and MSc in circuits and systems engineering from Nahrain University, Baghdad, Iraq in 1997 and 1999, respectively. He was awarded the undergraduate's prize for inter-university superior student competition for the academic year 1994/1995, and the graduate's prize for inter-university graduate student competition for the academic year 1996/1997. Since 1998, Eng. He is studying now towards his PhD degree at the Electrical Engineering and Electronics Department, University of Liverpool, Liverpool, UK. He is a member of the signal processing group at the same department.

Fawzi Al-Naima received both degrees of BSc (first Class honors), and PhD in electrical engineering from the University of Newcastle upon Tyne, UK in 1971 and 1976, respectively. He worked as a lecturer and associate professor in Al-Rasheed College of Engineering, Baghdad, Iraq from 1977 to 1989. He has been with the College of Engineering, Nahrain University, Baghdad, Iraq since 1989. He served as Head of Department of Electronics and Communication Engineering from 1992 to 2000, and Head of Department of Computer Engineering from 2000 to 2003, and then a Dean of the College of Engineering from 2003 to 2007 in the same university.