High Capacity Image Steganography Based on Curvelet Transform

Ali A. Al-Ataby
Department of Electrical Engineering and Electronics
University of Liverpool
Liverpool, UK
ali.al-ataby@liverpool.ac.uk

Fawzi M. Al-Naima *FIETE*
Department of Computer Engineering
College of Engineering, Nahrain University
Baghdad, Iraq
fawzi.alnaima@ieee.org

***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 is 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 based on curvelet transform with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security.**

Keywords-Steganography, security, wavelet transform, curvelet transform, cryptography, information-hiding, image processing.

I. 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 [1, 2, 3].

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 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 statistical properties. The process of finding these distortions is called statistical steganalysis.

II. INFORMATION-HIDING SYSTEM FEATURES

An information-hiding system is characterized by having three different aspects that contend with each other. These are, capacity, security, and robustness as shown in Fig. 1. 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 [4].

Generally speaking, information hiding relates to both watermarking and steganography. A watermarking system 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.

III. 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 attempts to be detectable only if secret information is known, as shown in Fig. 2. 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

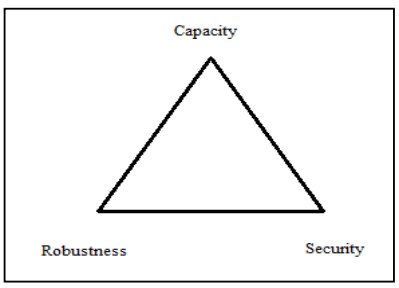


Figure 1. Information-hiding system features

978-0-7695-4593-6/11 $26.00 © 2011 IEEE
DOI 10.1109/DeSE.2011.13

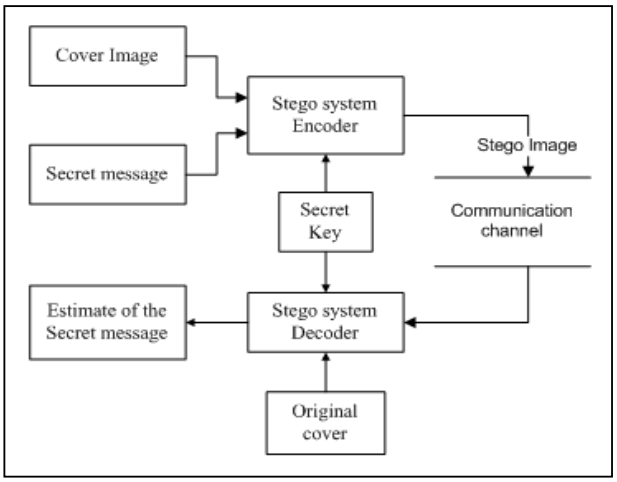


Figure 2. A modern steganography system

exposed, a comparison between the cover and stego media immediately reveals the changes [4, 5].

Three basic types of Stego systems are available [3]:

- 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 uses secret key to encrypt a hidden message that is encapsulated inside a cover media.

IV. THE CURVELET TRANSFORM

Along with the wavelet transform and the ridgelet transform, the curvelet transform is based on sparsity theory [6]. It is introduced to address the problem of optimally finding sparse representations of objects with discontinuities along edges. This curvelet transform inherits the ridgelet conception and is constructed without using ridgelets [6, 7].

Let μ be the triple (j, l, k) in the frequency plane; j = 0, 1, 2, … is a scale parameter; l = 0, 1, … 2^j is an orientation parameter; and $k = (k_1, k_2)$, $k_1, k_2 \in Z$ is a translation parameter pair. A curvelet coefficient is simply the inner product between an element $f \in L^2(R^2)$ and a curvelet ϕ_μ given by [7, 8]:

$$C_\mu \equiv \langle f, \phi_\mu \rangle = \int_{R^2} f(x)\overline{\phi_\mu(x)}dx = \frac{1}{(2\pi)^2}\int \hat{f}(\omega)U_j(R_{\theta_k}\omega)e^{i\langle x_k^J, \omega\rangle}d\omega \quad (1)$$

where R_θ is the rotation by θ radians, $J = (j, l)$ is the index of a wedge for all k within it, and U_j is the polar "wedge" window of radial dialation and angular translation [6]. Define coarse scale curvelets as:

$$\phi_{j_0,k}(x) = \phi_{j_0}(x - 2^{-j_0}k), \hat{\phi}_{j_0}(\omega) = 2^{-j_0}A_0(2^{-j_0}|\omega|) \quad (2)$$

where A_0 is a radial window and the curvelet is isotropic. For $j \geq j_0$, a reconstruction formula is:

$$f = \sum_\mu \langle f, \phi_\mu \rangle \phi_\mu \quad (3)$$

Similar to other mutiscale pyramids, curvelets transform images into several frequency scales.

Suppose that there is an object supported in $[0,1]^2$ which has a discontinuity across a nice curve, and which is otherwise smooth. Then, using a standard Fourier representation and approximating it with $\hat{f}_m^F$ built from the best m nonzero Fourier terms, the same way used to define the m term approximation $\hat{f}_m^W$ in wavelet and $\hat{f}_m^C$ in curvelet transform, then [6, 7, 8]:

$$\lim_{m\to\infty} \| f - \hat{f}_m^F \| = m^{-1/2},$$
$$\lim_{m\to\infty} \| f - \hat{f}_m^W \| = m^{-1}, \quad (4)$$
$$\lim_{m\to\infty} \| f - \hat{f}_m^C \| = C.m^{-2}(\log m)^3$$

Clearly, the last result is the smallest and nearly as good as m^{-2} in regards to adaptive representation asymptotically [7]. Even the hot dual-tree wavelet is no sparser than the ordinary wavelet [6,7,8].

Conceptually, the curvelet transform is a multiscale pyramid with many directions and positions at each fine scale and needle-shaped elements at fine scales. These help to obtain a sparser representation than other multi-scale representations, such as wavelets. Roughly speaking, to represent an edge to squared error $1/N$ requires $1/N$ wavelets and only about $1/\sqrt{N}$ curvelets [6, 8]. Based on the curvelet transform, it is possible to cast hidden messages onto more significant components and spread the modifications to more space locations.

Two implementations of the curvelet transform are available [6]. The first is the fast discrete curvelet transform (FDCT) based on unequally-spaced fast Fourier transform (abbreviated FDCT-USFFT), while the second is the FDCT based on frequency wrapping of specially selected Fourier samples (abbreviated FDCT-FW). The two implementations essentially differ by the choice of spatial grid used to translate curvelets at each scale and angle. Both transformations return a table of digital curvelet coefficients indexed by a scale parameter, an orientation parameter, and a spatial location parameter. Both implementations are fast in the sense that they run in $O(n^2 \log n)$ flops for n by n Cartesian arrays; in addition, they are also invertible, with rapid inversion algorithms of about the same complexity [6,7, 8].

A MATLAB toolbox called CurveLab which implements both transforms is available in [6]. In this paper the FDCT-FW version was used.

V. 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, then this 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, 10]. Table 1 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 [9,10,11].

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 2 shows the average time (theoretically) required to decrypt an encrypted massage versus key length using the brute force attack. Increasing key length increases the strength of the encryption algorithm on the expense of complexity and computation overhead [9, 11].

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.

TABLE 1. 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

TABLE 2. DECRYPTION TIME USING BRUTE FORCE ATTACK METHOD THAT ATTEMPTS 100,000 KEYS PER SECOND FOR DIFFERENT SYMMETRIC KEY LENGTHS

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

VI. 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.

Fig. 3 shows a general representation of the proposed steganography method. At the receiving end, opposite operations are followed to get the hidden message. 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

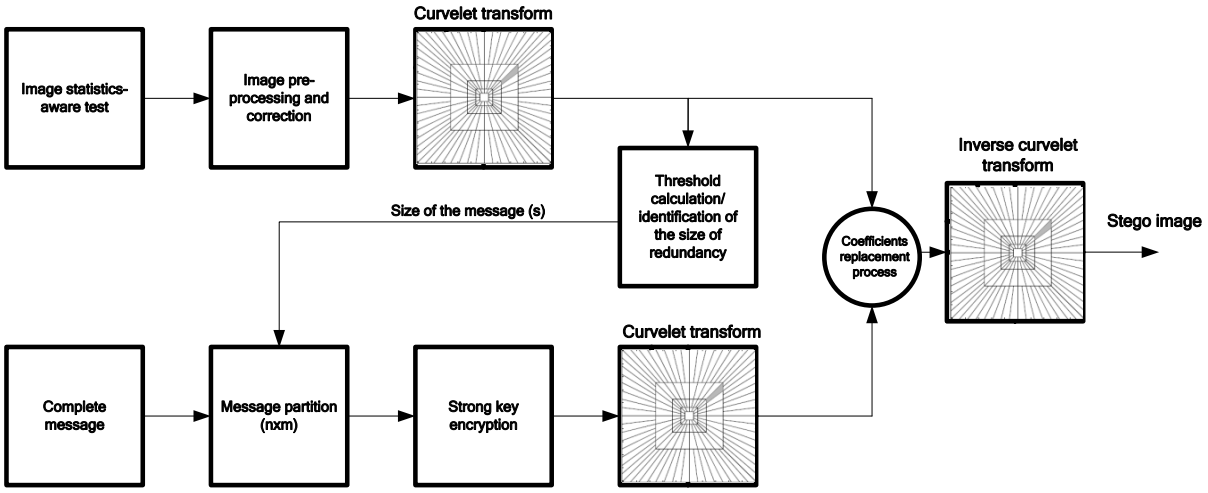


Figure 3. General representation for the proposed method

Step 3: FDCT-FW Transformation:

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

Step 4: Threshold Calculation/Identification of the size of redundancy:

This step calculates the threshold (*T*) that is used to define what is the size (the space) of the redundancy in the cover image, that can be used to embed 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:

$$T = \frac{\alpha}{N}\sum^{N}|J_w| \tag{5}$$

where J_w s are the coefficients of the FDCT-FW 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 affects the size of the cover image that is used to embed the hidden message. The step is summarized as follows:
Input: FDCT-FW transformed cover image
Output: Size of the information (s) that can be hidden inside the cover image, FDCT-FW of the cover image
Action: Threshold (*T*) calculation
For each pixel in the transformed cover image **do**
get next FDCT-FW coefficient
if the value of the FDCT-FW 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 FDCT-FW Transformation:
Input: Encrypted bit stream of the message
Output: FDCT-FW transform of the encrypted message.
Action: Transform the encrypted bit stream of the message to curvelet domain
End

Step 8: Stego Image Formation:
Input: FDCT-FW of the cover image (Step 4), FDCT-FW transform of the encrypted message.
Output: Stego image
Action:

- Place the FDCT-FW coefficients of the encrypted message in the location specified previously in the FDCT-FW of the cover message.
- Inverse FDCT-FW transform the result.

End

VII. 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 curvelet domain according to the threshold value *T* given by (5). Hence, the payload is linked directly to the threshold factor. From practical observations, it was found that the value of *T* increases 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*) [12,13, 14]:

$$PSNR = 10Log_{10}(S^2 / MSE) \tag{6}$$

where:

$$S^2 = \frac{1}{m*n}\sum_{i=1}^{m}\sum_{j-1}^{n} J^2(i,j) \tag{7}$$

And the *MSE* is the Mean Square Error defined as:

$$MSE = \frac{1}{m*n}\sum_{i=1}^{m}\sum_{j=1}^{n}[J(i,j) - J'(i,j)]^2 \tag{8}$$

where *J'* is 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. *It* is defined as follows:

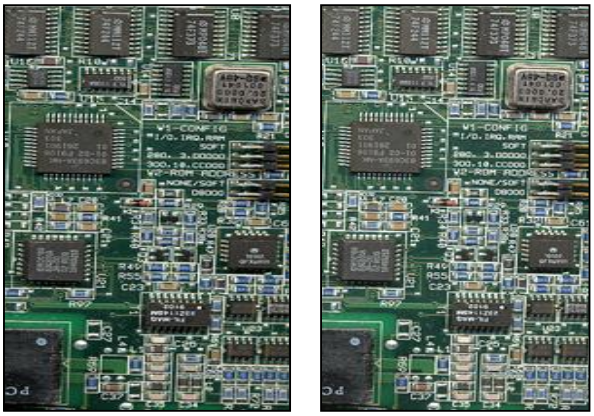
$$RMSE = \sqrt{MSE} = \sqrt{\frac{1}{m*n}\sum_{i=1}^{m}\sum_{j=1}^{n}[J(i,j) - J'(i,j)]^2} \tag{9}$$

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

$$\alpha \uparrow \quad MSE \uparrow \quad RMSE \uparrow \quad Payload \uparrow \quad PSNR \downarrow \tag{10}$$

In other words, the higher the value of α (refer to (1)), the higher the values for *MSE*, *RMSE*, and Payload, and the lower the value of *PSNR*, and vice versa. Fig. 4 shows an output for the proposed method.

Table 3 shows some simulation results (for the same image shown in Fig. 4) after applying the proposed method using the FDCT-FW compared to the use of DWT. Note that the results shown in the table vary depending on the nature of the cover image. 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 than the theoretical boundaries).



(a) (b)

Figure 4. Experimental result from the proposed method on an image with (306x648) pixels.
(a) Original image, (b) Stego image with payload=74.89 % and MSE=1.64 % (α=0.5)

TABLE 3. THE EFFECT OF α ON *MSE*, PAYLOAD (CAPACITY) AND *PSNR*, A COMPARISON BETWEEN DWT AND FDCT-FW (FOR THE IMAGE OF FIG. 4)

α	*MSE* %		Payload %		*PSNR* dB	
	DWT	FDCT-FW	DWT	FDCT-FW	DWT	FDCT-FW
0.3	0.70	0.63	49.99	60.56	40.98	60.67
0.4	1.24	1.12	56.83	69.12	36.29	57.81
0.5	1.93	1.64	61.92	74.89	32.57	52.56
0.6	2.77	2.34	65.84	77.90	29.58	49.38
0.7	3.79	3.45	69.01	78.73	27.02	45.78
0.8	4.96	4.67	71.61	80.32	24.81	39.99
0.9	6.27	5.97	73.83	83.45	22.84	36.89

It was found practically that the proposed method generates a stego image that is immune to statistical steganalysis using histogram technique and other filtering and image inspection methods using some of the available commercial software. 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 curvelet domain before placing it in the curvelet version of the cover image. This leads to more effective embedding of the message inside the cover image.

VIII. CONCLUDING REMARKS

As far as data hiding using steganography is concerned, two primary objectives are interesting: the technique that is 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 is correctly recovered. Then, it uses curvelet transform to transform both the cover image and the hidden message. Curvelet transform allows perfect embedding of the hidden message and reconstruction of the original image.

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*). Also, the method shows high robustness against attacks, but this area needs more investigation.

The results of the proposed method were compared with those obtained after applying the same techniques mentioned above but with the transform being wavelet transform, namely, DWT [15]. The comparison was in favor of FDCT-FW due to the ability of curvelet transform to highly compress the data and introducing more sparsity, hence increasing the capacity or payload of the steganography process.

Curvelet transform was developed in recent years in an attempt to overcome inherent limitations of traditional multiscale representations such as wavelets. It is interesting because it efficiently addresses very important problems where wavelet ideas are far from ideal. Examples are: optimally sparse representation of objects with edges, optimally sparse representation of wave propagators, and optimal image reconstruction in severely ill-posed problems. Both FDCT implementations run in $O(n^2 \log n)$ flops for n by n Cartesian arrays, and are also invertible, with rapid inversion algorithms of about the same complexity. To substantiate the pay-off, consider one of these FDCTs, namely, the FDCT via wrapping: first and unlike earlier discrete transforms, this implementation is a numerical isometric; second, its effective computational complexity is 6 to 10 times that of an FFT operating on an array of the same size, making it ideal for deployment in large scale scientific applications.

The extraction of the hidden message was not shown and it is out of the scope of this paper. In general, the extraction follows 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-offs. Also, curvelet transform needs thorough investigation and analysis to accommodate it with the area of watermarking and steganography and to get useful practical implementations.

REFERENCES

[1] C-S. Lu, Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, Chapter I, pp. 1-47, Idea Group Publishing, 2005.

[2] R. Popa, "An analysis of steganographic techniques," Working Report on Steganography, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, University of Timisoara, pp. 168-189, 1998.

[3] N. Provos, and P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security and Privacy Magazine, IEEE Computer Society, May-June pp. 32-40, 2003.

[4] E.T. Lin, and E.J. Delp, "A review of data hiding in digital images," Proceedings of the Image processing, Image Quality, and Image Capture Conference (PICS), Savannah, Georgia, pp. 274-278, April 1999.

[5] F.N. Johnson, and S. Jajodia, "Steganography: Seeing the unseen," IEEE Computer Magazine, pp. 26-34, February 1998.

[6] E. Candès, L. Demanet, D. Donoho, and L. Ying, "Fast discrete curvelet transforms," Tech Rep., Appl. Comput. Math., California Institute of Technology, 2005.

[7] C. Zhang, L. Cheng, Z. Qiu, and L. Cheng, "Multipurpose watermarking based on multiscale curvelet transform," IEEE Transactions on Information Forensics and Security, Vol. 3, No. 4, pp. 611-619, 2008.

[8] T. Peining, S. Dexter, and A. Eskicioglu, "Robust digital image watermarking in curvelet domain," Proceedings of SPIE, International Society for Optical Engineering, ISSN 0277-786X , Vol. 6819, pp. 1-12, 2008.

[9] Microsoft Press, Fundamentals of Network Security, Microsoft Official Curriculum, course number 2810, ch. 4, pp. 230-255, 2003.

[10] M. Naor, and O. Reingold,"On the construction of pseudo random permutations," Journal of Cryptography, Vol. 12, No. 1, pp. 29-66, 1999.

[11] J. Fridrich, M. Goljan, D. Soukal, and T. Holotyak, "Forensic steganalysis: Determining the stego key in spatial domain steganography," Proceeding of EI SPIE, Vol. 5681, pp. 631-642, San Jose, CA, 2005.

[12] Y-K. Lee, and L.H. Chen, "A High capacity image steganographic model," IEEE Proceedings Vision, Image and Signal Processing, Vol. 147, pp. 288-294, 2000.

[13] H-Y. Lo, S. Topiwala, and J. Wang,"Wavelet based steganography and watermarking," Wavelets Reports, Computer Science Department, Cornell University, 1998.

[14] A. Westfeld, and R. Bohme, "Exploiting preserved statistics for steganalysis," Proc. of 6th International Workshop on Information Hiding, Vol. 3200, pp. 82-96 Toronto, Canada, May, 2004.

[15] A. A. Al-Ataby, and F. M. Al-Naima, " A modified high capacity image steganography technique based on wavelet transform," Int. Arab Journal of Information Technolgy (IAJIT), Vol. 7, No. 4, pp. 358-364, 2010.