International Journal of Computer Science
and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 3, Issue 1, Jan 2014, 63-72
© IASET

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

A NOVEL AUDIO STEGANOGRAPHY SCHEME USING DOUBLE DENSITY DUAL TREE COMPLEX WAVELET TRANSFORM SECURED WITH MODIFIED BLOW FISH ENCRYPTION

TUMMALA SANDHYA
CREC, Tirupati, Andhra Pradesh, India

ABSTRACT

The word Steganography is an information trouncing method where secret message is embedded into unwary cover signal. Good quality steganography algorithms contain perceptual precision, payload or capacity and strength. Quality of steganography scheme can be measured using metrics such as PSNR, MSE. Within this paper, a novel high capacity audio Steganography algorithm based on double density dual tree complex wavelet transform with blowfish encryption has been proposed. Hence cryptography features has been incorporated within steganographic technique. Proposed technique overcomes the drawbacks of standard DWT and double density DWT and provides phase information.

KEYWORDS: Audio Steganography, Double Density Dual Tree Complex Wavelet Transform, Blow Fish Algorithm, High Capacity Steganography

I. INTRODUCTION

In the existing time of information technology, eavesdropping can be condensed by employing cryptography or/with Steganography. Steganography is a method of embedding secret messages in a cover signal to elude illicit exposure [1]. Steganography differs from cryptography in terms of message visibility. It hides secret messages utterly compared to cryptography where the secret message is visible [2].

Steganography is recurrently used in covert communication for instance military and government communications. Habitually it requires moderately high payloads. The key necessities that should be pleased for good quality steganography algorithms contain perceptualprecision, payload or capacity and strength. High capacity is measured as an important portion for steganography. In recent years various techniques have been developed for information hiding, and many of these techniques used either image or video media but rarely use audio signal as a cover signal mainly in high rate of data embedding. This is due to the fact that Human Auditory System (HAS) is more approachable compared to the Human Visual System

In this paper, a novel steganography scheme that has high capacity and high output quality has been proposed. The proposed algorithm is based on Double Density Dual Tree Complex Wavelet Transform with blowfish encryption. The Blow fish algorithm depends on the cover message strength. Rest of the paper is organized as follows. Section II presents related work and theoretical background. Proposed hiding scheme with embedding and extraction algorithms and blowfish encryption is described in detail in Section III. Section IV demonstrates the experimental results. Finally conclusions and future work are provided in section V.

II. RELATED WORK

The simplest hiding technique in time domain with suitable capacity is the Least Significant Bits (LSB), but it is susceptible to changes in LSB that can possibly reveal the embedded message [1,2,4]. In the transform domain, there are numerous transform methods that can be engaged in hiding such as Fourier domain, discrete cosine domain, and wavelet domain [4].

Every domain has its features in signal processing and information hiding, still, the wavelet domain has a foremost advantage over the others since it divides a signal into different frequency components with different resolutions, and then each component can be used in embedded process according to its dominance.

Discrete Wavelet Transform

DWT in one-dimensional analysis splits the audio signal into two parts namely high and low frequency parts. This process of splitting is called decomposition [8]. The edge components correspond to high frequencies part. These can be analysed using high pass filters and low frequency parts can be analysed using low pass filters. The message hiding process starts by identifying redundant bits which can be modified without degrading the quality of the audio and then replace the redundant bits with the secret message [10].

DWT algorithm decomposes an audio signal into a set of coefficients where approximation coefficients consists of low frequency information and detail coefficients contains high frequency information. These coefficients can be obtained by passing the signal through low pass and high pass filters [9].

Double Density DWT

It consists of one scaling function and two distinct wavelets

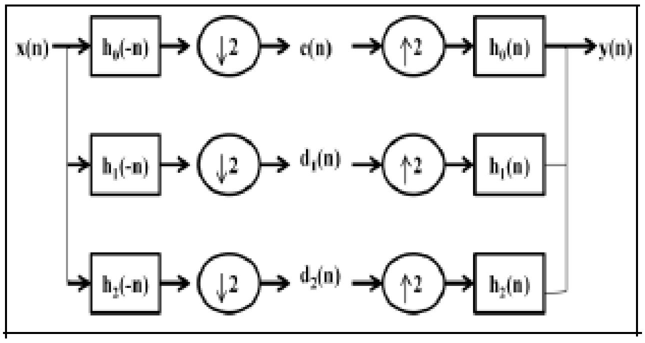

Figure 1: Filter Bank Structure of DD DWT

It includes 1 low pass filter $h_0(-n)$ and two high pass filters $h_1(-n)$, $h_2(-n)$ in analysis filter. In its inverse form, it consists of one low pass filter $h_0(n)$ and two high pass filters $h_1(n)$, $h_2(n)$.

Double-Density DWT [12] enhances the features of standard DWT. But a few wavelets in this technique are directional. Though this technique utilizes more wavelets, some lack a spatial orientation. A solution to this problem is provided by the complex double dual tree wavelet transform

The proposed algorithm starts by dividing the input audio cover signal and then decomposes each segment by using double density dual tree complex wavelet transform. It combines double density discrete wavelet transform and dual tree complex wavelet transform[14,15,16].The proposed technique is similar to DD-DWT except that decomposition is performed for both high and low frequency components. The decomposed signal by DD-DT-CWT for *L* levels, yields (2^L) mechanism with equal lengths where one represents the approximation signal that has the highest control and lowest frequency, while the others are detailed signals with decreasing influence, starting from the lowest to the highest frequency detailed components. Consequently, the Inverse DD-DT-CWT (IDD-DT-CWT) is used to reconstruct the output stego signal.

III. PROPOSED HIDING SCHEME

Proposed method first divides the input audio signal into segments. Then each segment is decomposed into transform domains using forward complex double dual tree wavelet transform. The secret message is encrypted using blowfish algorithm and then embedded in the transform domains. Then inverse DD-DT-CWT is applied to reconstruct stego signal.

Double Density Dual Tree Complex Wavelet Transform

Standard DWT and double density DWT suffer from three major limitations.

Lack of Shift Invariance

When down sampling operation of signal is performed at each level, shift variance takes place. The wavelet coefficients obtained from down sampling operation varies due to shift in input signal.

Lack of Directional Selectivity

As the DWT filters are real and separable the DWT cannot distinguish between the opposing diagonal directions.

The first problem can be avoided if the filter outputs from each level are not down sampled but this increases the computational costs significantly and the resulting undecimated wavelet transform still cannot distinguish between opposing diagonals since the transform is still separable. To distinguish opposing diagonals with separable filters, the filter frequency responses must be asymmetric for positive and negative frequencies. This can be achieved by using complex wavelet filters which suppresses negative frequency components. The proposed method has improved shift-invariance and directional selectivity than the separable DWT.,

Absence of Phase Information

The initial motivation behind the earlier development of complex-valued DWT was the third limitation that is the 'absence of phase information'. The proposed hiding scheme uses complex-valued filtering (analytic filter) that decomposes the real/complex signals into real and imaginary parts in transform domain. These are used to compute amplitude and phase information, which is the information needed to describe the energy localization of oscillating functions (wavelet basis) accurately. 2-D DT-CWT is based on two scaling functions and two distinct wavelets whereas Double Density DWT is based on single scaling function and two distinct wavelets.

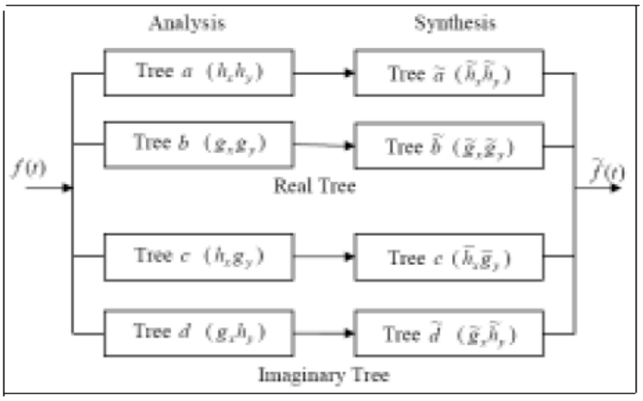
Analysis
Synthesis
Tree a $(h_x h_y)$
Tree $\tilde{a}$ $(\tilde{h}_x \tilde{h}_y)$
Tree b $(g_x g_y)$
Tree $\tilde{b}$ $(\tilde{g}_x \tilde{g}_y)$
$f(t)$
Real Tree
$\tilde{f}(t)$
Tree c $(h_x g_y)$
Tree c $(\tilde{h}_x \tilde{g}_y)$
Tree d $(g_x h_y)$
Tree $\tilde{d}$ $(\tilde{g}_x \tilde{h}_y)$
Imaginary Tree

Figure 2: Filter Bank Structure

The proposed technique not only overcomes the problem of poor directional selectivity in DWT, but can also discriminate between opposing diagonals with six different sub-bands oriented at 15^{o}, 75^{o}, 45^{o}, -15^{o}, -75^{o}, and $- 45^{o}$.

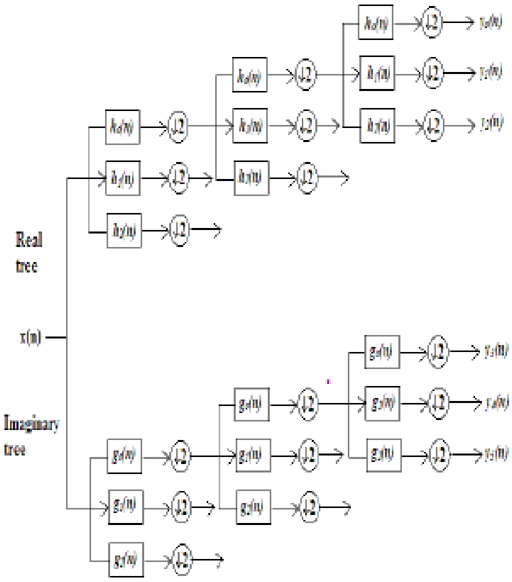

Figure 3: Analysis Filters of DD-DT-CWT

The DD-DT-CWT is based on two scaling functions and four distinct wavelets, each of which is specifically designed such that the two wavelets of the first pair are offset from one other by one half, and the other pair of wavelets form an approximate Hilbert transform pair.

As shown in Figure 2 there are two separate filter banks denoted by *hi(n)* and *gi(n)* where *i* = 0, 1, 2. The filter banks *hi(n)* and *gi(n)* are designed in such a way that the subband signals of the upper DWT can be interpreted as the real part and the subband signals of the lower DWT can be interpreted as the imaginary part. Using synthesis filters, signal is reconstructed perfectly

Embedding Algorithm

The embedding algorithm includes following steps:

- The secret message to be embedded is secured using Blow fish encryption.
- Decompose the signal into low and high sub-bands using DD-DT-CWT.
- Embed the secret data in the sub bands.
- Obtain the stego-signal by taking the inverse transform to the modified signal.

Extraction Algorithm

It consists of the following steps:

- Load the stego signal and transform it into sub bands using DD-DT-CWT.
- Extract the message from signal by using decryption method.
- Reconstruct the audio signal using inverse DD- DT-CWT**.**

Modified Blow Fish Algorithm

Blowfish algorithm [17] is used to provide security to secret message before embedding into transform domain. Each segment of the input audio cover signal is decomposed using L-levels of DD-DT-CWT to obtain 2^Lsignals one represents the approximation coefficients signal and the others symbolize details coefficients signal. We are using modified Blowfish algorithm [18] for Encryption and Decryption of data which serves as a better solution both in terms of performance and as well as security.

Encryption

It consists of a function that iterates 16 times where each round contains permutation that is independent of key and a substitution that depends on data. This function includes XOR operations and additions on 32-bit words. The additional operations present are four indexed array data lookup tables for each round.

Decryption

The process applied for encryption can used for decryption except that the sub-keys are supplied in reverse order. The Feistel network ensures the swapping of every half for the next round except for the last two sub-keys .s

IV. RESULTS AND DISCUSSIONS

The proposed algorithm was implemented by using Matlab (2013a) programming. The proposed algorithm was tested using five audio cover signals: male speaker, female speaker, male song, female song, jazz, kid song. Each signal has resolution of 16 bits per sample and sampling frequency 44.1k samples/sec. The quality of output signal in each test was computed using PSNR.

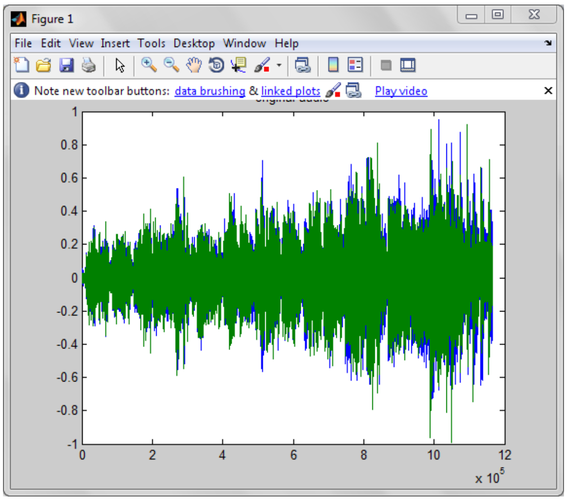
Figure 1
File Edit View Insert Tools Desktop Window Help
Note new toolbar buttons: data brushing & linked plots Play video
1
0.8
0.6
0.4
0.2
0
-0.2
-0.4
-0.6
-0.8
-1
0
2
4
6
8
10
12
x 10^5

Figure 4: Input Signal

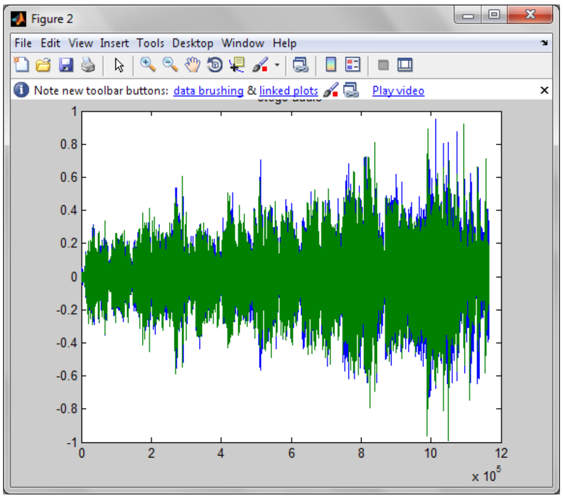
Figure 2
File Edit View Insert Tools Desktop Window Help
Note new toolbar buttons: data brushing & linked plots Play video
1
0.8
0.6
0.4
0.2
0
-0.2
-0.4
-0.6
-0.8
-1
0
2
4
6
8
10
12
x 10^5

Figure 5: Stego Signal

Table 1: PSNR & MSE Values for Existing Techniques

AUDIO	DWT		DD-DWT	
	MSE	PSNR	MSE	PSNR
Male Song	0.012	43.425	0.0156	61.969
Female Song	0.045	42.135	0.01786	63.974
Male Voice	0.055	43.999	0.0186	62.056
FemaleVoice	0.812	41.751	0.09183	65.841
Kid Song	0.625	42.814	0.01652	63.412

Table 2: PSNR & MSE Values for DD-DT-CWT

AUDIO	DD-DT-CWT	
	MSE	PSNR
Male Song	0.9228	82.154
Female Song	1.0576	81.531
Male Voice	1.0987	83.643
Female Voice	1.284	81.432
Kid Song	0.928	80.165

Table 3: PSNR & MSE Values for Music Samples

AUDIO	DWT		DD-DWT	
	MSE	PSNR	MSE	PSNR
Jazz	0.031	40.352	0.5901	60.815
Pop	0.513	43.631	0.3974	62.612
Rock	0.423	41.788	0.1812	64.991
Heart	0.158	41.682	0.0135	65.154

Table 4: PSNR & MSE Values for Music Samples

AUDIO	DD-DT-CWT	
	MSE	PSNR
Jazz	0.9361	79.635
Pop	1.6649	81.999
Rock	1.5926	83.714
Heart	1.9714	80.693

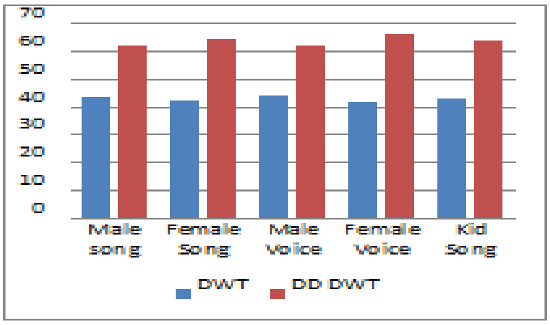

Figure 6: PSNR Values for Existing Techniques

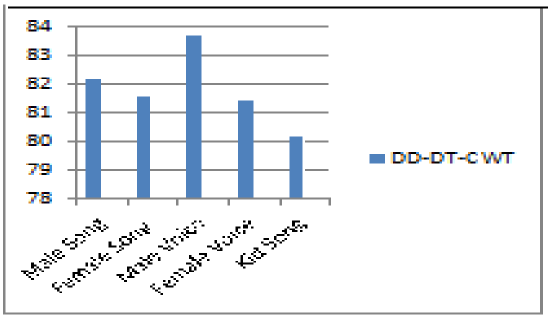

Figure 7: PSNR Values for Proposed Technique

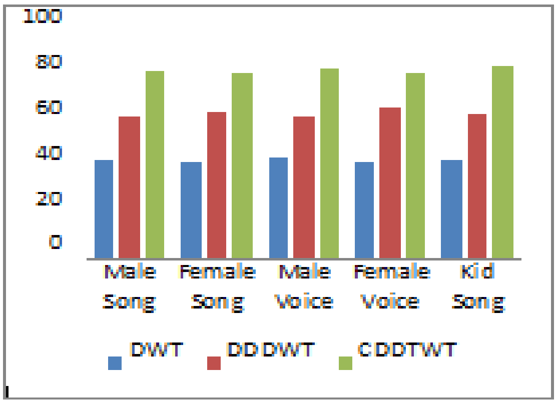

Figure 8: Comparison of PSNR Values for Different Techniques

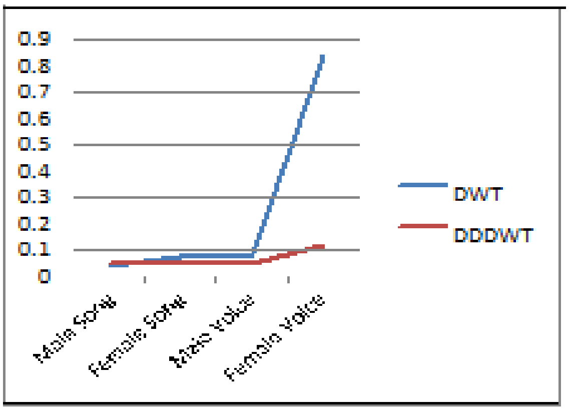

Figure 9: MSE Values for Existing Methods

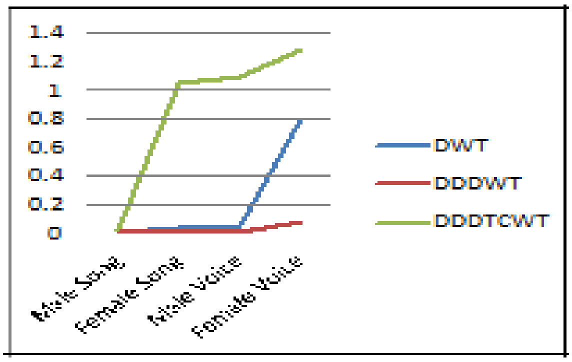

Figure 10: Comparison of MSE Values for Audio Samples

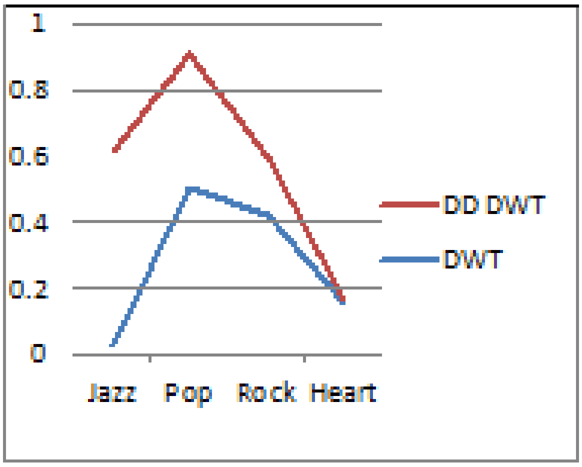

Figure 11: MSE Values for Music Samples for Existing Techniques

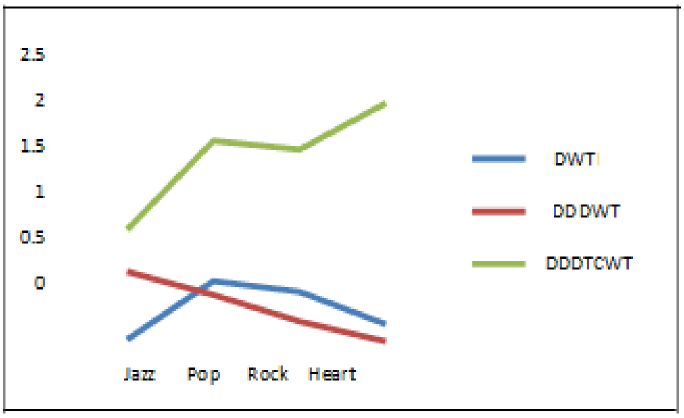

Figure 12: Comparison of MSE Values for Music Samples

CONCLUSIONS AND FUTURE WORK

In this paper, audio steganography using double density dual tree complex wavelet transform has been developed which outperforms DWT and Double Density DWT in terms of embedding capacity. Message embedding capacity can be measured using PSNR and MSE. From results, it is clear that the proposed technique yields better PSNR values than the existing techniques. It also provides Phase information which is needed for perfect reconstruction of audio sample. By using modified blow fish algorithm, secret message is secured before embedding into transform domain.

In future, this paper can be extended to make the steganography system resistant to attacks to increase robustness.

REFERENCES

1. Johnson, N.F. and Jajodia. S., " Exploring Steganography: Seeing the Unseen", *IEEE Computer, Vol.31, No.2, Feb, 1998*
2. H. Wang and S. Wang, "Cyber warfare : Steganography vs Steganalysis", *Communications of the ACM magazine, Vol. 47, No.10, Oct 2004*
3. Ross J. Anderson, Fabien A.P. Petitcolas, "On The Limits of Steganography", *IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998*
4. Masoud Nosrati, Ronak Karimi, Mehdi Hariri, "Audio Steganography: A Survey on Recent Approaches", *World Applied Programming, Vol. 2, No. 3, Mar 2012.*
5. Ali Al-Ataby and Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", *The International Arab Journal of Information Technology, Vol. 7, No. 4, Oct 2010*
6. Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", *International Journal of Applied Science and Engineering, Vol. 4, No. 3, 2006*
7. Abikoye Oluwakemi C, Adewole Kayode S and Oladipupo Ayotunde J, "Efficient Data Hiding System using Cryptography and Steganography*", International Journal of Applied Information Systems, Vol. 4, No.11, Dec 2012*
8. Youssef Bassil, "A Two Intermediates Audio Steganography Technique", *Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No.11, Nov 2012*

9. Dalal N. Hmood, Khamael A. Khudhiar and Mohammed S. Altaei "A New Steganographic Method for Embedded Image In Audio File", *International Journal of Computer Science and Security, Vol. 6, No. 2, 2012*

10. Siwar Rekik, Driss Guerchi,Habib Hamam & Sid-Ahmed Selouani, "Audio Steganography Coding Using the Discrete Wavelet Transforms", *International Journal of Computer Science and Security, Vol. 6, No.1 , 2012*

11. Jisna Antony, Sobin c. c and Sherly A. P, "Audio Steganography in Wavelet Domain – A Survey", *International Journal of Computer Applications, Vol. 52, No. 13, Aug 2012*

12. Siwar Rekik, Driss Guerchi, Habib Hamam & Sid-Ahmed Selouani, "Audio Steganography Coding Using the Discrete Wavelet Transforms", *International Journal of Computer Science and Security,Vol. 6, No. 1, 2012*

13. Aruna Mittal, "A Highly Secure Skin Tone Based Optimal Parity Assignment Steganographic Scheme Using Double Density Discrete Wavelet Transform", *International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, No. 9, Nov 2012*

14. Jingyu Yang, Yao Wang, Wenli Xu, and Qionghai Dai, "Image Coding Using Dual-Tree Discrete Wavelet Transform*" IEEE Transactions On Image Processing, Vol. 17, No. 9, Sep 2008*

15. Ivan W Selesnick, "The Double- Density Dual-Tree DWT", *IEEE Transactions on Signal Processing, Vol 52, No.5, May 2004*

16. Sushil Kumar and S. K. Muttoo, "Image Steganogaraphy Based on Complex Double Dual Tree Wavelet Transform", *International Journal of Computer and Electrical Engineering, Vol. 5, No. 2, Apr 2013*

17. Afaf M. Ali Al-Neaimi, Rehab F. Hassan, "New Approach for Modifying Blowfish Algorithm by Using Multiple Keys", *International Journal of Computer Science and Network Security, Vol .11 No. 3, Mar 2011*

18. Monika Agrawal, Pradeep Mishra, "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm*", International Journal of Engineering and Advanced Technology, Vol. 1, No. 6, Aug 2012*