A New Technique of Hiding Data Using Genetic and Integer Wavelet Algorithms with OPAP Process

[a]M. A. Khader Khan, [b]Sadia Najmus Saher, [c]Syed Abdul Sattar,
[a]Associate Professor, Dept.of ECE, Royal Institute of Technology and Science, Chevella, Telangana, India
[b]Associate Professor, MCA, Presidency School of Management and Computer Science, Hyderabad, Telangana, India
[c]Director, R & D, Nawabshah Alamkhan College of Engineering and Technology, Hyderabad, Telangana, India

Abstract

Steganography is used to hide a secret password within a cover image, resulting in a stego image removing even the minute bit of the presence of secret information . The purpose of steganography is to connect two operators secretly. Steganography has different technical challenges namely imperceptibility and high hiding capacity. In this proposed work a modern steganographic technique such as Integer Wavelet transform (IWT) and double key has been used to achieve high hiding capacity, good visual quality and high security. Here cover image is converted in to wavelet coefficients and these coefficients are selected randomly by using Key1 for data embedding, Key2 is used to find the number of bits to be embedded in the indiscriminately selected coefficients. Lastly the Optimum Pixel Adjustment Process OPAP is applied to the stego image to reduce the error during data embedding.

KEYWORDS- Steganography, integer wavelet transform (IWT), optimum pixel adjustment (OPA) process.

I INTRODUCTION

Internet and other peer to peer communication networks though have a dominant role in the digital communications; have turned a blind eye to the privacy of its users. With communication technologies defining new pinnacles every day and people's injustice to information is sky rocketing, there is a calamitous need to safeguard the treasure house of intelligence, which gathers a great deal of valuable information. Researchers under the support of computer security, information security and information declaration are cerebrating new algorithms to combat illegitimate attacks and protect the information they used to store, process and transmit. one such algorithm Steganography, which involves communicating secret data in a suitable multimedia carrier, e.g. Video files, image files, audio information files.

Steganography of image, has gained much impulsion and status in the recent past (1-18) . It comes under the general postulation that if the feature is visible, the point of assault is evident. Thus the goal here is to always obscure the lucidity of the embedded data. The basic sculpt of secret key steganography consists of cover, secret data, stego image and embedding key. Any information in digital files such as image, video, audio files will be used as cover. This cover is also called as cover_object or cover_ image, is

the plain digital image with no secret information deposited in it, after embedding it is called the stego _image or stego_ object [1, 2, 3, 10]. In steganography of image [1] the critical information is masked in a cover image with immense agility.Some of the other objectives which are of equal concern and are undetectable, heftiness (resistant to various image processing techniques and compression) and capacity of the hiding data. All these factors discriminate it from various counterparts such as watermarking and cryptography [1, 10].

The word capacity refers to the amount of important information that can be hidden in the cover_object, secure from an eavesdropper's intruder's capability to perceive hidden data, and heftiness is the amount of modification the stego_object can withstand before an antagonist can destroy hidden information[7]. Image Steganography includes several techniques to go on board with the payload within the cover_image. The most popular hiding techniques are Spatial Domain Techniques and Transform Domain Techniques. Spatial domain based steganography contains the Least Significant Bit (LSB) technique, Pixel value comparing (differencing) etc [2, 13, 17] and the latter includes DCT [9], DWT [6, 14] and IWT [4-6, 8].

A useful, practical steganographic method should be robust and should retain the hidden data even after many pixel values have been modified. One approach to this problem is to transform the image and embed the data in the transformed pixels [4-6,8,9]. We say that the original image exists in the spatial domain and the transformed image in the respective transformed domain. Then data is embedded in the transformed pixels and the image is transformed back to the spatial domain. The idea is that the image may now be focused to various operations that will change the pixels, when this modified image is transformed again, the hidden data will still be embedded in the transformed pixels. The disadvantage of the DCT based stegano technique [9, 13], is the capacity to hide data. Contemporary researchers are directed to use DWT, since it is used in the new image compression format JPEG2000 and MPEG4. Techniques that use DWT found in[4-6,8], Wavelet transform based stego technique provides high capacity as much as possible. In [4] the secret message is embedded into both high and low frequency coefficients of the wavelet transform to high hiding capacity, but it provides less PSNR at high hiding rate. In this paper we propose a new modified methodology (4) where we can embed a larger quantity of data in integer wavelet transform domain with high PSNR.

II RELATED WORK

A. Integer Wavelet Transforms

The use of Wavelet transform will mainly address the capacity and robustness of the features of Information_Hiding system. The Haar_ Wavelet Transform is the simplest among different wavelet transformations. In Haar_ Wavelet the low frequency wavelet components or coefficients are generated by averaging the two pixel values and high frequency components (coefficients) are generated by taking half of the difference of same two pixels. The four bands obtained are L_fL_f band L_fH_f band H_fL_f band and H_fH_f bands which is shown in fig 1 .The approximation band L_fL_f, which consists of wavelet coefficients of low frequency, and contains important part of the spatial domain image.

The other bands are referred as detail bands which contains high frequency coefficients and also the edge details of the image in spatial domain . Integer wavelet transform can be achieved through lifting scheme. Lifting scheme is a technique which converts DWT coefficients to Integer coefficients without losing information. [5, 8]

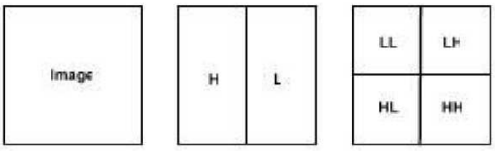


Figure 1 Image and its transform domain bands.

B. Forward Lifting scheme in IWT.

Step1: Column wise processing to get H and L

$H_f = (C_o - C_e)$ (1)

$L_f = (Ce - H_f/2)$ (2)

Where C_o is the odd column and C_e even column wise pixel values

Step 2: Processing row wise to get L_fL_f,L_fH_f,H_fL_f and H_fH_f, Separate odd and even rows of H_f and odd and even rows of L_f,

Namely, $H_{f\,odd}$ – odd row of H_f $L_{f\,odd}$- odd row of L_f $H_{f\,even}$- even rowof H_f $L_{f\,even}$- even rowof L_f

$L_f H_f = L_f\,odd - L_f\,even$ (3)

$L_f L_f = L_f\,even - (L_f H_f / 2)$ (4)

$H_f L_f = H_f\,odd - H_f\,even$ (5)

$H_f H_f = H_f\,even - (H_f L_f / 2)$ (6)

C. Reverse Lifting scheme in IWT

Inverse Integer wavelet transform is formed by Reverse lifting scheme.And is same as the forward lifting scheme.

D. LSB Embedding

Simple LSB embedding [2]is detailed in this section. Consider a 8-bit gray scale image matrix consisting m × n pixels and a k bits of secret message . The message first bit o is embedded into the LSB of the first pixel and the message second bit is embedded into the second pixel and so on. The resultant stego _ image which contains the secret

message and it is a 8-bit gray scale image where difference between the cover image and the stego-image is not visually identifiable This can be further enlarge, and any number of LSB's are modified in a pixel. But quality of the image, however reduces with the increase in number of LSB's. Generally up to 4 LSB's can be modified without significant degradation in the message. Mathematically, the pixel value 'X' of the chosen pixel for storing the k-bit message M_k is modified to form the stego-pixel 'Xs' as follows:

$$X_s = X - \text{mod}(X, 2^k) + M_k \quad (7)$$

The embedded message bits can be retained by

$$M_k = \text{mod}(X_s, 2^k) \quad (8)$$

method which improves the quality of the LSB substitution is Optimal Pixel adjustment Process (OPAP)[2].

E. Optimal Pixel adjustment Process

The proposed procedure for Optimal Pixel adjustment (OPAP) reduces the error caused by the LSB substitution process. In OPAP method the pixel value is attuned after the secret data is hidden. It is done to improve the stego image quality without disturbing the hidden data .

F Adjustment Process

- Let 'n' LSBs be substituted in each pixel.
- Let p= decimal value of the pixel after the substitution.
- p1 = decimal value of last n bits of the pixel.

- p2 = decimal value of n bits hidden in particular pixel.
- If(p1~p2)<=(2^n)/2

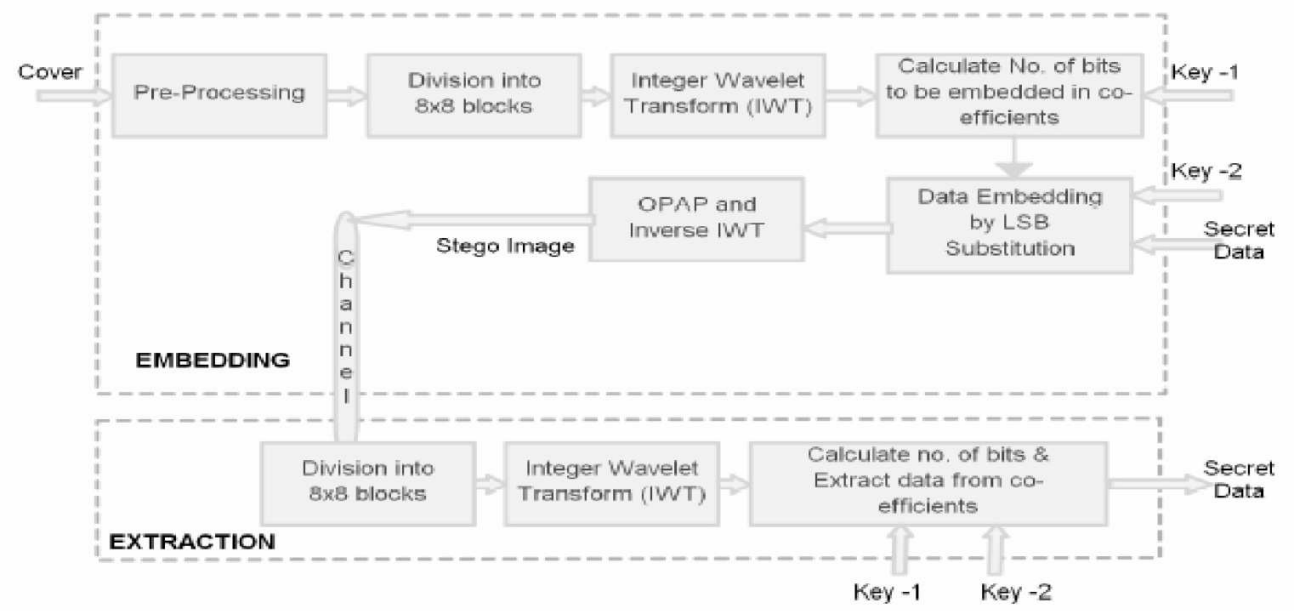
then no adjustment is made in that particular pixel. Else
If (p1<p2)
p = p – 2^n.
If(p1>p2)
p = p + 2^n.

This p is transformed to binary and return back to pixel.

III . PROPOSED METHODOLOGY

Fig no 2 shows the proposed system which is a high capacity steganography system. Preprocessing includes R, G and B plane separation and modification Histogram.Applying Integer wavelet transform to the cover_ image to get wavelet coefficients of cover_ image. Wavelet coefficients are arbitrarily selected by using key-2 for embedding the secret data. A binary matrix of order nxn (as Key-2 and n=8) in which data to be embedded is denoted as "1" in the corresponding wavelet coefficients and no

data represents “0”



present in the wavelet coefficients. Key-1(K1) is a decimal number varying from 1 - 4 and it will choose the number of bits to be embedded in the cover object .This bit length calculation is the modified version of one in [4]. High capacity is achieved by varying the key-1(K1) value.

A. Embedding Algorithm

Step 1: Read the cover- image as a 2Dimension file with size of 256×256 pixels.

Step 2: R, G and B planes are separated

Step 3: Consider a secret data as text file. Here each character will take 8 bits.

Step 4: Histogram modification [16] is done in all planes, as the secret data is to be embedded in all the planes, embedding integer wavelet coefficients produces stego-image pixel values which are more than 255 and less than zero. Hence the pixel values will be from 15 to 240.

Step 5 : Each plane is divided into 8×8 blocks

Step 6: Apply Haar Integer wavelet transform to 8 × 8 blocks of all the planes, This method gives results in LL1 sub bands, LH1 sub bands, HL1sub bands and HH1 sub bands

Step 7: Using Key-1(K1) calculate the Bit length (BL) for corresponding wavelet co-efficient and modified version of Bit length calculation is used [4]. Using the following

equation, we get the high capacity steganography.

Step 8: Using key2 select the position and coefficients for embedding the "BL" length data using LSB substitution [2]. Here data is embedded only in LH1 sub bands,HL1 sub bands and HH1 sub bands. Here data is not embedded in LL1 sub bands because they are very sensitive and also to maintain excellent visual quality after data embedding . An example of key2 is shown below.

$$BL = \begin{cases} K1+2 & \text{if } WC \geq 2 \\ K1+3 & \text{if } WC \geq 2 \\ K1+1 & \text{if } WC \square 2 \end{cases} \quad (9)$$

$$Key\text{-}2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & & & & & & & \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \quad (10)$$

Step 9: Applying Optimal Pixel adjustment Procedure (OPAP) reduces the error caused by the LSB substitution method.

Step 10: Take inverse wavelet transform to each 8×8 block and combine R,G&B plane to produce stego image.

B. Extraction Algorithm

Step 1: Read the Stego image as a 2D file with size of 256 × 256 pixels
Step 2: R, G and B planes are separated
Step 3: Each plane is divided into 8×8 blocks.
Step 4: Apply Haar IWT to N×N where N=8 blocks of all the planes, This process results LL1,LH1,HL1 and HH1 sub bands.
Step 5: Using Key-1 calculate the Bit length (BL) for corresponding wavelet co-efficient and using the 'BL' equation used in Embedding procedure.
Step 6: Using key-2 select the position and coefficients for extracting the 'BL' length

data.
Step 7: Combine all the bits and then divide it in 8 bits to obtain the text message.

IV. ERROR METRICS

A performance measure in the stego image is measured by means of two parameters namely, Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). The MSE is calculated by using the equation, where M, N denote total no of pixels in vertical & horizontal dimensions of image, xi-j represents original image,yi-j

$$MSE= \quad (1/MN)\sum_{I=1}^{M}\sum_{j=1}^{N}(x_{i,j} - y_{i,j})^2$$

Represents the pixels of the stego_image. The Peak Signal to Noise Ratio (PSNR) is expressed

$$PSNR=10Log_{10}(I^2_{max}/MSE)dB$$

V. RESULT AND DISCUSSION

In this present implementation, Lena and baboon 256 × 256 × 3 color digital images have been taken as cover images, as shown in Figure 3&4- a, b, c & d, tested with key-2(key-J) and various key-1s. The effectiveness of the stego process proposed has been studied by calculating MSE and PSNR for the two digital images in RGB planes and tabulated.
First analysis is used to select the Key-2 for random selection of coefficients for embedding data (in this analysis Key-1 has been set as K1=1) and the results are tabulated in Table-I for various Key-2 using the proposed method. From table –II we will understand that Key-J provides high capacity and Key – A provides low capacity

In the second analysis, Key-J will be taken with various 'K1' values and the results are tabulated in Table-I. Combining Key-J with K1=4 will yield high hiding capacity with highPSNR.

Table – I MSE, PSNR for fixed Key-2(Key-J) with varying Key-1 in all the three planes

Key-1	Cover Image	Total No. of bits embedded	Channel - I Red		Channel - II Green		Channel - III Blue	
			MSE	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)
K1=1	Lena	180454	2.8472	43.5866	2.3196	44.4766	1.852	45.4544
K1=2	Lena	241201	4.9872	41.1522	4.4826	44.4766	3.8033	45.4544
K1=3	Lena	310800	4.9326	41.2	4.4964	41.6022	1.3412	46.8558
K1=4	Lena	330012	5.943	40.3907	5.0457	41.1016	5.5904	40.6564
K1=1	Baboon	330012	5.943	40.3907	5.0457	41.1016	5.5904	40.6564
K1=2	Baboon	336404	5.2519	40.9276	4.3689	41.7271	4.7826	41.3341
K1=3	Baboon	358860	9.777	38.2287	8.9648	38.6054	9.3528	38.4214
K1=4	Baboon	375161	15.712	36.1685	15.1689	36.3213	15.6867	36.1755

Various key -2	Cover Image	Total No. of bits embedded	Channel - I Red		Channel - II Green		Channel - III Blue	
			MSE	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)
Key - A	Lena	52345	1.3495	46.8291	0.7531	49.362	0.4904	51.2249
	Baboon	94061	2.7146	43.7938	1.8565	45.4438	2.2742	44.5624
Key - B	Lena	63138	1.6245	46.0235	1.0736	47.8225	0.7534	49.3606
	Baboon	92959	2.5767	44.0201	1.7415	45.7215	2.2435	44.6215
Key - C	Lena	53951	1.0511	47.9142	0.4232	51.8652	0.1797	55.5854
	Baboon	105293	1.4987	46.3737	0.631	50.1304	1.076	47.8128
Key - D	Lena	57827	1.5049	46.3557	0.9188	48.4985	0.6162	50.2333
	Baboon	93444	2.6619	43.8789	1.8482	45.4633	2.255	44.5993
Key - E	Lena	57656	1.5093	46.3431	0.9483	48.3613	0.6183	50.2187
	Baboon	93576	2.6487	43.9004	1.8139	45.5447	2.2222	44.663

Key - F	Lena	55760	1.2789	47.0625	0.6721	49.8567	0.3985	52.1262
	Baboon	99528	2.1079	44.8923	1.232	47.2246	1.6526	45.9491
Key - G	Lena	116364	1.9767	45.1715	1.4113	46.6347	1.0676	47.8467
	Baboon	192884	3.8383	42.2894	3.0182	43.3334	3.442	42.7627
Key - H	Lena	110891	1.7881	45.6069	1.2721	47.0855	0.9333	48.4305
	Baboon	193245	3.8444	42.2825	3.0907	43.2302	3.5234	42.6612
Key - I	Lena	111813	1.6711	45.9008	1.0663	47.8518	0.7775	49.2239
	Baboon	199022	3.2595	42.9992	2.4182	44.2959	2.8326	43.6089
Key - J	Lena	180454	2.8472	43.5866	2.3196	44.4766	1.852	45.4544
	Baboon	330012	5.943	40.3907	5.0457	41.1016	5.5904	40.6564

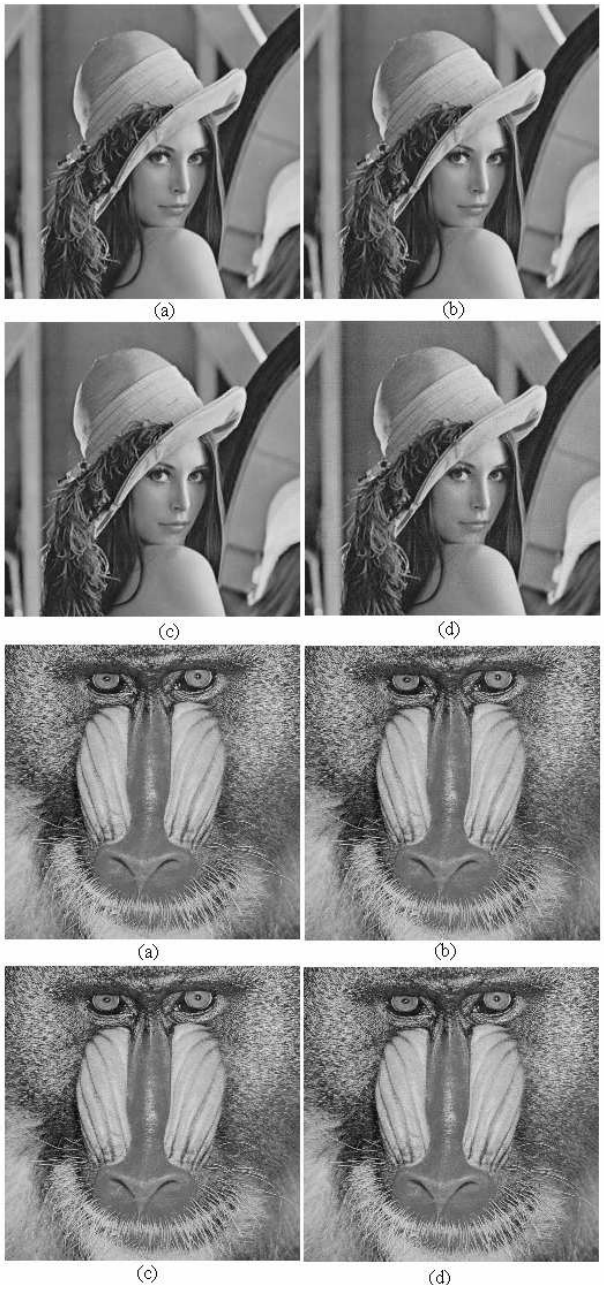


Figure 3. K1=1,2,3 & 4 respecively

Figure 4. K1=1,2,3 & 4 respecively

V1 CONCLUSION

Data hiding using steganography has two primary objectives firstly that steganography should provide the maximum possible payload, and the second, embedded data must not be accessible to the observer. It should be stressed on the fact that steganography doesnot meant to be robust. It was found that the proposed method gives high payload (capacity) in the cover image with small error. which is at the expense of decreasing PSNR and increasing the MSE. By modifying the equation (9) to get high capacity for the various applications using wavelet transform, Key-1 and Key-2 provides high security. The

drawback of the proposed method is the computational overhead. This can be reduced by high speed computers.

VII REFERENCES

[1] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt,Digital image steganography: Survey and analysis of current methodsSignal Processing", 90 (2010),727–752.
[2] C.K. Chan, L.M. Chen, "Hiding data in images by simple LSBsubstitution", Pattern recognition, 37 (3) (2004), 469–474.
[3] R.Amirtharajan, Adarsh D, Vignesh V and R. John Bosco Balaguru, "PVD Blend with Pixel Indicator - OPAP Composite for HighFidelity Steganography", International Journal of ComputerApplications 7(9),(October 2010),31–37.
[4] R.O. EI Safy, H. H. Zayed, A. EI Dessouki, "An AdaptiveSteganographic Technique Based on Integer Wavelet Transform",International conference on Networking and media convergenceICNM-(2009), 111 - 117.
[5] Guorong Xuan; Jidong Chen; Jiang Zhu; Shi, Y.Q.; ZhichengNi; Wei Su," Lossless data hiding based on integer waveletransform" , IEEE Workshop on Multimedia Signal Processing,Vol.2,(2002), 29-32.
[6] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach forImage Steganography", International Journal of Applied Science and Engineering 4,(2006), 275-290.
[7] Saeed Sarreshtedari and Shahrokh Ghaemmaghami, "High CapacityImage Steganography in Wavelet Domain", IEEE CCNC 2010 proceedings,(2010),1-5.
[8] Cheng jiang Lin, Bo Zhang, Yuan F. Zheng," Packed Integer WaveletTransform Constructed by Lifting Scheme", IEEE Transactions on Circuits and Systems for Video Technology, (Dec 2000), 1496 –1501
[9] KokSheik Wong, Xiaojun Qi, Kiyoshi Tanaka A DCT-based Mod4steganographic method, Science Direct-Signal Processing ,87 (2007) 1251–1263.
[10] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniquesfor Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000.
[11] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography", IEEE Security Privacy Mag.,1 (3) (2003) 32–44.
[12] B. Lai and L. Chang, "Adaptive Data Hiding for bnages Based on Harr Discrete Wavelet transform" , Lecture Notes in Computer Science, Volume 4319,(2006).
[13] R.Amirtharajan.R.Akila. P.Deepikachowdavarapu, " Article: A Comparative Analysis of Image Steganography", International Journal of Computer Applications 2(3)(2010) 41–47.
[14] W.Y.Chen,"Color image steganography scheme using set partitioning hierarchical trees coding, digital Fourier transform and adaptive phase modulation", Applied Mathematics and Computation 185(1)(2007)432–448.
[15] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, "Information Hiding-A Survey", Proceedings of the *IEEE*, special issue on protection of multimedia content, 87(7), (July 1999), 1062- 1078.
[16] Yildiray Yalman, Ismail Erturk, "A New Histogram Modification Based Robust Image Data Hiding Technique", 24th International Symposium on Computer and Information Sciences, ISCIS 2009, 39 - 43.

[17] Dr. V. Vijayalakshmi, Dr. G. Zayaraz, and V. Nagaraj, A Modulo Based LSB Steganography Method, IEEE International conference on Control, Automation, Communication and Energy Conservation,(2009),1 - 4.
[18] Rengarajan Amirtharajan and John Bosco Balaguru Rayappan, "*Tri- Layer Stego for Enhanced Security – A Keyless Random Approach*" - IEEE Xplore, DOI, 10.1109/IMSAA.2009.5439438