2017 International Conference on Trends in Electronics and Informatics (ICEI 2017)

Tirunelveli, India
11-12 May 2017

Pages 584-1180

IEEE Catalog Number: CFP17J32-POD
ISBN: 978-1-5090-4258-6

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number: CFP17J32-POD
ISBN (Print-On-Demand): 978-1-5090-4258-6
ISBN (Online): 978-1-5090-4257-9

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

Table of Contents

An Improved Image Steganography based on 2-DWT-FFT-SVD on YCBCR Color Space

Sunil Kumar Yadav
M.tech (Cyber Security)
Department of CSE & IT
MITS,Gwalior,M.P.(India)
mitsscholar9@gmail.com

Manish Dixit
Associate Professor
Department of CSE & IT
MITS,Gwalior,M.P.(India)
dixitmits@gmail.com

Abstract*—Steganography is technique for hiding the fact that communiqué is taking vicinity, through hiding records in different statistics. The digital images (DI) are the maximum famous because of Web amongst frequency all specific service document layouts. Image steganography (IS), achieves the secrecy with the aid of embedding statistics into cover Image (CI) and generating a stego-image (SI). There are many steganography method types all have their advantages and disadvantages. In this paper using 2-DWT, SVD and FFT in steganography technique. The new result is based on Peak Signal to Noise Ratio (PSNR), SNR, WPSNR, Structural Content (SC) and MSE is calculate to measure picture value for proposed method for higher outcome as in comparison with prior tactics of information hiding.

Keywords*—DWT, SVD, FFT, Steganography, PSNR, WPSNR, MSE, SC.

I. INTRODUCTION

The steganography set of policies, which makes use of spatial-primarily based completely embed statistics system into various pixels inside the CI right now, is one of the maximum critical techniques within the subject of records protection. Existing algorithm is kinds of camouflage which may embed encode records interested in cowl media (e.g. textual, picture, audio and video) to make stegomedia. Exclusive information can't be discovered within the stegomedia at the same time as its miles transmitted on most people communication channels in commonplace CNs. The cause of the steganography set of rules is to cover a huge quantity of mystery information and as well to broadcast the one's records with the minimal imperceptibility to the steganalysis [1].

In the SD, the records are hidden without delay into LSB of supply picture with none modification. In this domain two different kinds of methods are commonly used: LSB substitution based & LSB matching based method. There is a few upgrades complete in LSB substitution method based on the process of optimal pixel adjustment process (OPAP) [9]. The LSB matching approach is an improvement of LSB substitution method. Luo, et. Al. Have LSB proposed similar method, wherein the information are hide in the rims. Chen et. Al. Have secreted the information in edges of supply picture founded on mixture side identify. In the transform domain (TD), name of the game communication is unseen into the transform coefficients the use of a frequency orientated method which conclude of DCT, DWT, Z-rework and FT. Chang et. al. Have projected reversible statistics securing in DCT coefficients of the medium frequency apparatus into every block.

II. USING TECHNIQUE

A. *DWT*

The Wavelet transform is created via repeatedly filtering the picture coefficients on a row by way of row and column by column foundation. A 2- DWT decomposition of the picture include quite a grouping of band facts reminiscent of LL frequency approximation band, HL frequency vertical element band, LH frequency horizontal detail band and excessive-high frequency diagonal element band. DWT is used to attain just proper picture retrieval base at the low computational price.
Wavelet Feature Extraction
Wavelet ψ (t) is a function to fulfills this situation

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right)$$

DWT is a phantom evaluation method, which decomposes a characteristic or a signal into fantastic frequency sub-bands and leads to a set of wavelet coefficients. The low degree physical functions of the authentic picture are covered in those WC therefore the sign may differentiate through means of this WC.

Subdivided squares constitute pyramid sector algorithm use to IP, as it's far used on pixel squares. At every sector level the pinnacle left-hand square represents averages of nearby pixel numbers, averages fascinated approximately appreciate to the selected low-bypass filter out on the identical time because the three directions, horizontal, [4] vertical, and diagonal represent detail differences, with the three represented by using separate bands and filters. We can hold decomposition of the coefficients from low bypass filtering in each guideline similarly in the next step

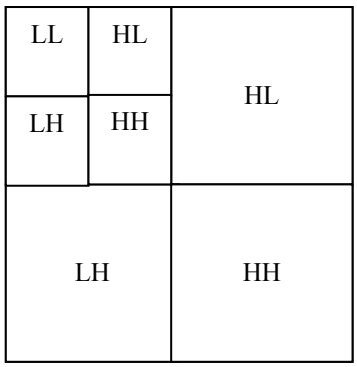


Fig. 1. Diagram of 2-DWT

B. *FFT*

FFT is a DFT set of rules which decrease the form of computations wished for N elements from 2N2 to, in which 2NlogNis the bottom-2 logarithm.

In view of the importance of the DFT in various digital signal processing applications, such as linear filtering, correlation analysis, as well as spectrum analysis, its efficient computation is a topic that received considerable attention by several mathematician, engineer, and applied scientist.

From this component, we alternate the notation that X(k), in place of y(k) in previous sections, represents the Fourier coefficients of x(n).

Essentially, the computational problem for the DFT is to compute the collection X(k) of N complicated-valued numbers given a few special series of records x(n) of duration N, in keeping with the formula

$$X(k) = \sum_{n=0}^{N-1} x(n) W_N^{kn} \ , \qquad 0 \le k \le N-1$$

$$W_N = e^{-j2\pi/N}$$

In trendy, the statistics collection x (n) is also assumed to be complex valued. Similarly, The IDFT will become

$$x(n) = \frac{1}{N \sum_{n=0}^{N-1} X(k) W_N^{-kn}} \ , \qquad 0 \le n \le N-1$$

Since DFT and IDFT involve basically the same type of computations, our discussion of efficient computational algorithms for the DFT applies as well to the efficient computation of the IDFT.

.

We have taken for every well worth of k, through subtraction of X(k) entails N difficult multiplications (4N real multiplication) and N-1 complicated accompaniments (4N-2 real additions). Thus, to calculate every one N values of the DFT calls for N2 complicated multiplications and N^2-N complicated accompaniments.

Through calculation of the DFT is largely incompetent mostly as it does no longer make maximum the symmetry and periodicity houses of the segment issue WN. Inaccurate, those two properties are:

$$symmetric\ property: W_N^{k+N/2} = -W_N^k$$

$$Periodicit\ property: W_N^{k+N} = -W_N^k$$

The computationally successful algorithms defined on this phase, regarded collectively as FFT algorithms, take advantage of those main properties of the segment element [5].

FFT algorithms normally go down in two training: decimation in time, and decimation in frequency. The Cooley-Tukey FFT set of guidelines first reorganize the enter objects in bit-reversed arrange, after which construct the output rework (decimation in time). The primary plan is to split a transform of period N into transforms of length N/2 by the individuality [6].

C. *SVD*

SVD break down into m x n real matrix A, proper in a made from three matrices $A=USV^T$ wherein U and V^T is m x n, n x n orthogonal matrices, correspondingly. S is n x n diagonal matrix. The elements of S are handiest nonzero on the diagonal and are known as the SVs of A. The watermarking approaches are described as follows [7]

III. LITERATURE SURVEY

In [8] comfortable medical facts by using joining to one report layout by steganographic techniques. In accumulation of EEG, message consists of the physician's views and affected person info within the document header of the image. There is two new IS techniques which is founded on fuzzy-logic (FL) and the comparison is planned to pick the non- sequential LSB of picture pixels.

In [9] IS the art of concealing secret message onto the source image. A desirable method to steganography must provide two attributes: high stego image quality and high embedding capacity. In existing work, a frequency domain steganography founded absolutely data cancelling procedure the use of FT is planned. Existing work used, the Fresnelet coefficients that LSB on excessive frequency sub-bands is use embed the QR coded mystery information.

In [10] a changed and easy technique for excessive capability Steganography in case of color pictures. Transform domain (TD) method WT is used to achieve excessive capability at the side of protection and preserves the high-quality of the CI which work like the key characteristic of that artwork.

In [11] an IS method is proposed to cover audio sign in the picture inside the TD using WT. The audio register any layout (MP3/WAV or each different kind) are encrypted and accepted by using picture lacking informative life to everybody. Whenever undisclosed records are conceal inside service end output are stego sign. These paintings, effects give you an idea about proper best stego signal and stego signal is examine that unique attacks. Its observed that process is strong and it could endure the attacks. The effects display top values for those metrics.

In [12] a unique approach for info hiding inside TD color pictures. Our technique is founded on separating a picture into block, then making use of the planned remodel on unique blocks and unseen the name of the match message inside those. Security may be improved through following this approach since it depends on a one-of-a-kind form of rework which is primarily founded on irreducible polynomial mathematics. The matters and similarity contain demonstrated high potential besides preserving a less expensive stage of imperceptibility.

In [13] a changes cozy and high potential primarily founded definitely steganography pattern of unseen a big-size mystery photograph into a small-size CI. Arnold transformation is finished to jumbles the name of the match picture. DWT is done in each pictures and observed by manner of Alpha mixing process. Then the Inverse IDWT is applied to get the SI. Probe overall presentation of our scheme by using judge against numerous functions of SI and CI. Outcomes represents projected set of regulations for changed steganography is fairly protected with positive potency similarly of accurate perceptual unseeable.

IV. PROPOSED METHODOLOGY

We provided a presentation analysis of excessive robustness steganography of color pictures utilizing 2DWT-FFT-SVD. Let the size of the color CI is MXN and size of the color PI is NXN. Firstly, divide CI and PI into three planes. After that, take all components of the CI and take all components of first PI, after that all Additives are normalized to achieve the pixel ranging from (zero,1) instead of (0,255). This process is improving the security of image.In this algorithm, hide secret information image into CI in low and high frequency band of image which is produced by 2-DWT and it is further modify by FFT. Finally, it is used to modifying the singular parameters and produces a secure final SI using SVD method. Subsequently, The individual combined resulting matrix of SI is gained by the accumulation of decomposition matrix of the particular components i.e. R, G, and B of the CI and PI that's given by means of the subsequent equation 4.

Embedding Algorithm
Input: Cover Image (CI) and Payload Image (PI)
Output: Stego Image (SI)

1) Read CI and PI, then separate each the picture I (N×N×3) to 3 color RGB schemas.
2) Normalize all of the 3 additives in each instance.
3) Perform 2-DWT on the CI and PI to break down this in 4 non-overlapping multi-decision coefficient units LLa1,LHa1,HLa1,HHa1 and LLb1,LHb1,HLb1,HHb1
4) Perform FFT on LHa1 and LHb1 for further processing.
5) Apply SVD on both the FFT coefficients.
6) Perform SVD on the Red (R), Green (G) and Blue (B) coefficient of the FFT coefficients of cover image.

$$[U_i, S_i, V_i] = svd(I_i) \quad (1)$$

Where U_i, V_iAre orthogonal matrices of an picture and Si is singular matrix and imply a level of SVD, I_i is 3 planes of CI

7) Present SVD on the R, G and B coefficient of the FFT coefficients of PI.

$$[U_j, S_j, V_j] = svd(W_i) \quad (2)$$

Where U_j ,V_j are orthogonal matrices of a picture and Sj = singular matrix and that i represents a level of SVD, W_i represents PI

8) Change singular value (SV) of S_i aside embedding the of PI.

$$hide = S_i + \gamma \times S_j \quad (3)$$

Where conceal is custom designed singular matrix of S_i & S_j and γ represents scaling detail, apply for strength over the power of payload sign. It goes up 0.1 to 0.7.

9) embedded singular matrices by orthogonal matrices for final SI as W with under method:

$$W = U_i * hide * V_i' \quad (4)$$

10) Combine the R, G and B plane for reconstructing the SI.

Input: Stego Image
Output: Attacked Image

11) Apply noise attack with 0.2 noise density, HE attack, motion blur attack and rotate attack on 60 degree on SI for safety and roubstness.

Extraction Algorithm
Input: Attacked Image
Output: Extracted Payload Image

12) Use SVD to R,G and B sub band i.e.,

$$[U_m, S_m, V_m] = svd(P_m) \quad (6)$$

13) Change the SV of S_i by removing the SV of SI such that

$$S_j = (S_m - S_i)/\gamma \quad (7)$$

14) take out singular matrices with orthogonal matrices for end removed PI as W with beneath formula:

$$W = U_m * S_j * V_m' \quad (8)$$

15) PSNR and MSE - It calculates the value of SI and CI. Higher PSNR is better, lower MSE is better for image.

$$MSE(x) = \frac{1}{N}||x - x\hat{}||^2 = \frac{1}{N}\sum_{i=1}^{N}(x - x\hat{})^2 \quad (9)$$

x represents CI, x^ is SI, N is dimension of the CI

$$PSNR(x) = \frac{10 \times \log10((double(m).\hat{}2))}{MSE(x)} \quad (10)$$

Where m is the highest value of the CI

16) Weighted PSNR- It calculates the value of WPSNR between CI and SI.

$$WPSNR(x) = \frac{20\ X\ \log10((255))}{\sqrt{MSE(x)} \times NVF} \quad (11)$$

The system to compute this element as a basic function is:

$$NVF = NORM\left(\frac{1}{1 + \delta^2_{block}}\right)$$

Where δ represents the luminance variance for the 8 × 8 blocks of the picture and NORM correspond to the normalization function value. usually values for the WPSNR in lossyneed to be extra than 40 which imply excessive quality.

17) SNR - It measures the value of the rebuilded signal. Higher the value enhanced is the SI.

$$SNR = 10\ \times\ \log10\left(\frac{\sigma_x^2}{\sigma_y^2}\right)$$

Where $\sigma_x^2$and σ_y^2 represent the mean square value of the CI and the mean square dissimilarity b/w the CI and SI.

18) Structural Content (SC) - It is used for calculating correspondence content among CI & SI.

$$SC = \frac{(2\mu_x\mu_y - c_1)(2\sigma_{xy} - c_2)}{(\mu_x^2 - \mu_y^2 - c_1)(\sigma_x^2 - \sigma_y^2 - c_2)}$$

Where $\mu_x$is the common of x, $\mu_y$is the standard of y, σ_{xy} is the covariance of x and y, c_1=$(K_1L)^2$, c_2= $(K_2L)^2$,K_1= 0.01 and K_2= 0.03 by default and L is the dynamic variety of pixel values.

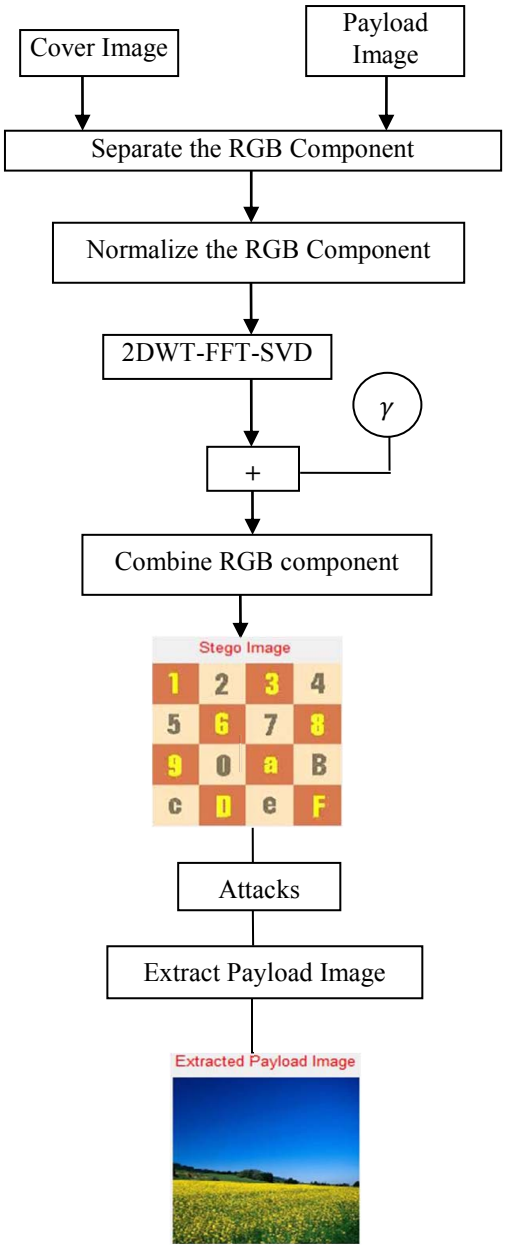


Fig. 2. Flow Chart of Proposed Architecture

V. RESULT SIMULATION

In this work, the result analysis is evaluated on MATLAB platform using Image Processing (IP) toolbox. The resultant output is presented on payload image with varying weights. The performance measure is evaluated on many parameters. The simulation results endorse that this method keeps excellent picture fine. It is mighty in assessment with extraordinary IP operations. Fig 2. Display the normal CI and PI. Fig. 3 indicates the different types of attack namely; noise attack, HE attack, rotate attack and motion blur attack respectively.

Fig. 3. Shows Cover image and Payload image

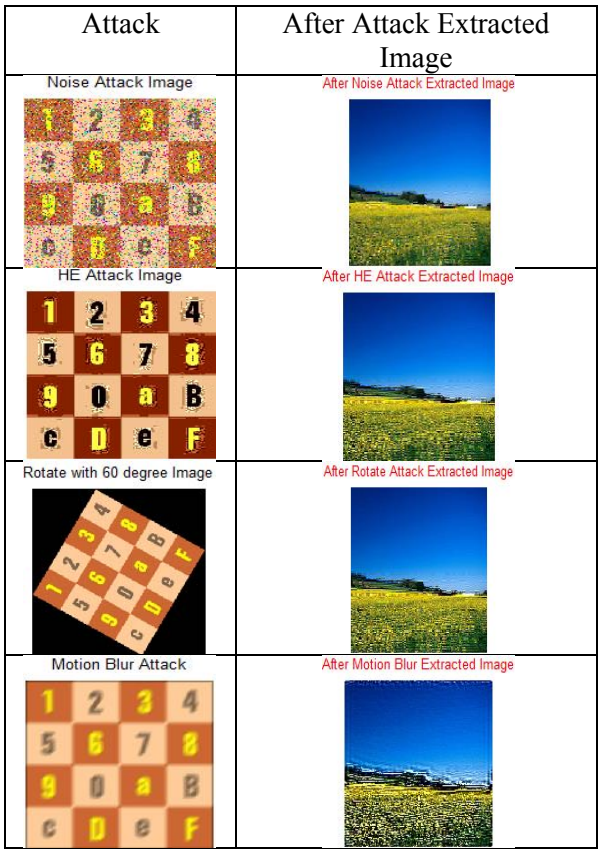


Fig. 4. Attack Image and Extracted attack image comparision

TABLE I. IMAGE QUALITY PARAMETERS FOR ALPHA= 0.2

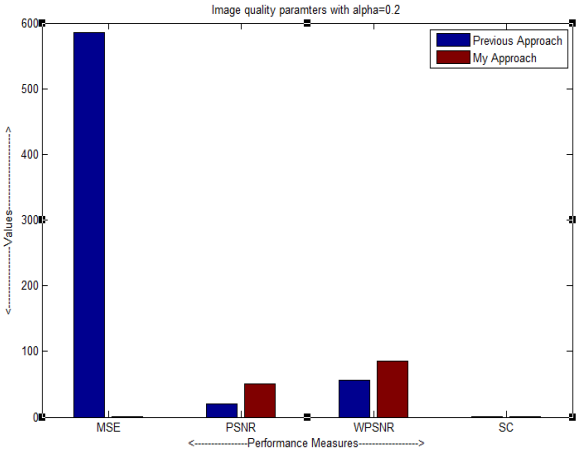
Performance Measure	Previous Approach	My Approach
MSE	585.698	0.4182
PSNR	20.4541	50.252
WPSNR	56.7123	85.335
SC	0.9564	0.9968

TABLE II. IMAGE QUALITY PARAMETERS FOR VARYING ALPHA

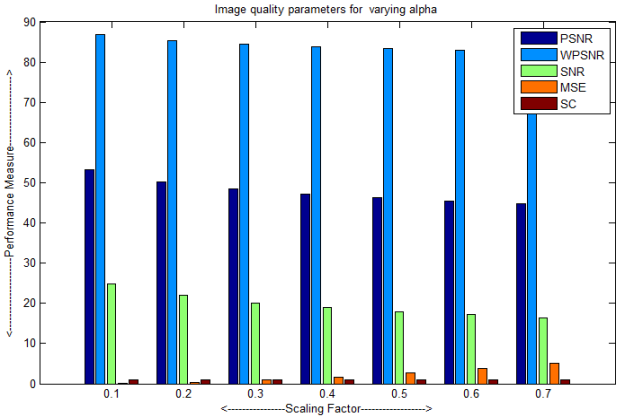
Scaling Factor	Stego Image				
	PSNR	WPSNR	SNR	MSE	SC
0.1	53.262	86.840	24.925	0.1045	0.999
0.2	50.252	85.335	21.915	0.4182	0.9968
0.3	48.491	84.455	20.154	0.9410	0.9933
0.4	47.242	83.8303	18.904	1.6730	0.9886
0.5	46.272	83.345	17.935	2.614	0.9832
0.6	45.4811	82.949	17.143	3.7643	0.9771
0.7	44.811	82.615	16.474	5.1236	0.9706

TABLE III. PERFORMANCE ANALYSIS ON MY APPROACH USING DIFFERENT ATTACKS

Attack	Extracted Image After Attack		
	SNR	PSNR	WPSNR
Noise	1.219	29.862	74.987
HE	1.204	29.838	74.9801
Rotate with 60°	1.204	29.837	74.9801
Motion Blur	1.058	29.611	74.906



Graph1.Image quality parameters for alpha= 0.2.



Graph2. Image quality parameters for varying alpha.

CONCLUSION

Now days, it is very risky to handle the data in internet against intruders. Data is usually within the shape of textual content, audio, video and photo. Steganography is one of the pleasant techniques to percentage the facts secretly and securely. Secret data may in the form of text, image or even in the form of video and audio. Hiding secret information in video file is known as video steganography.In this paper, using 2-DWT, SVD and FFT is presented. The PSNR is 50.252(dB) after the hiding process which shows the robustness against attacks. The error is also reduced in this proposed upto 0.4182(dB).The performance analysis validates that the obtainable steganography method has good imperceptibility too. The comparison outcomes with 2DWTFFTSVD based algorithm. We checked robustness of this proposed work on varying scaling factor and it proved better on each value. This algorithm is also applied on different types of attacks and retrieve payload image with efficiently.It shows that the superiority of our method. In the future scope, improve the attack process for image quality parameters.

REFERENCES

[1] Nameer N.,El-Emam and Mofleh Al-Diabat," A novel algorithm for colour image steganography using a new intelligent technique based on three phases", Applied Soft Computing 2015.

[2] Naveen Kumar Ahirwar,Manish Dixit "Face and Eye Recognition on Gray Image Using DWT with RBFSVM method" 2016 International Journal of Signal Processing,Image Processing and Pattern Recognition Vol.9,No.6(2016),pp.-369-378.

[3] Jeyanthi Prabhu and Jawahar Senthil Kumar "Wavelet Based Content Based Image Retrieval Using Color And Texture Feature Extraction By Gray Level Coocurence Matrix And Color Coocurence Matrix" Journal of Computer Science 10 (1): 15-22, 2014.

[4] Barnali Gupta Banik and Prof. Samir K. Bandyopadhyay," A DWT Method for Image Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013, pp. 983-989.

[5] http://www.cmlab.csie.ntu.edu.tw/cml/dsp/training/coding/transform/fft.html

[6] http://mathworld.wolfram.com/FastFourierTransform.html

[7] Kor Ashwini N, Prof. N.M.Kazi," A Survey of Water Mark Technique", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Issue 2, February 2014, pp: 7126- 7131.

[8] R. Karak, Güler, Çapraz and E. Bilir," A NOVEL FUZZY LOGIC-BASED IMAGE STEGANOGRAPHY METHOD TO ENSURE MEDICAL DATA SECURITY", Computers in Biology and Medicine 2015

[9] S. Uma Maheswari, D. Jude Hemanth," Frequency domain QR code based image steganography using Fresnelet transform", Int. J. Electron. Commun. (AEÜ) 69 (2015) 539–544

[10] Siraj Sidhik, S.K. Sudheer, V.P. Mahadhevan Pillai," Performance and analysis of high capacity Steganography of colorimages involving Wavelet Transform", Optik 126 (2015) 3755–3760

[11] Hemalatha S, U. Dinesh Acharya and Renuka A," Wavelet transform based steganography technique to hide audio signals in image", Procedia Computer Science 47 (2015) 272 – 281

[12] Wafaa Mustafa Abduallah , Abdul Monem S. Rahma and Al-Sakib Khan Pathan," Mix column transform based on irreducible polynomial mathematics for color image steganography: A novel approach", Computers and Electrical Engineering 40 (2014) 1390–1404

[13] Prabakaran. G and Bhavani.R," A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform", 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET], pp: 1096- 1100.