JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Security for Digital Data and Image with Dual Steganography and Watermarking

[1]Devendra Prasad Rajwade, [2]Prof. Shivraj Singh, [3]Prof. Hemant Verma
M. Tech. Scholar[1], Assistant Professor[2], Assistant Professor[3]
Department of Electronics and Communication Engineering
Technocrats Institute of Technology, Bhopal
devrajrajwade@gmail.com, 86.shivraj@gmail.com, hemantjec2009@gmail.com

Abstract: —"Steganography" is a procedure that defeats unapproved clients to approach the pivotal information, to invisibility and payload capacity using the different technique like discrete cosine transform (DCT) and discrete wavelet transform (DWT).The available methods till date result in good robustness but they are not independent of file format. The aim of this research work is to develop a independent of file format and secure hiding data scheme. The independent of file format and secure hiding data scheme in increased by combining DWT and least significant bits (LSB) technique. Accordingly an efficient scheme is developed here that are having better MSE and PSNR against different characters.

Index Terms – DWT, DCT, SVD, PSNR, MSE, LSB

I. INTRODUCTION

The utilization of computerized watermarking is by and large for distinguishing proof of proprietorship, so it isn't subjected for any change. The methods of advanced watermarking is fit for supporting distinctive levels of durability against changes assuming any, that can be made to the substance of watermark uninterested application. The computerized watermarks debased or be crushed because of getting undesirable and destructive signs and geometric bends like symmetrical advanced change, computerized to simple transformation, editing, turn, contamination, scaling, dithering, a pressure and so on of the substance. Then again on the off chance that it utilized for the validation of the substance. Those ought to effectively break or demolished at whatever point, the substance is changed for the reason of altering the substance which is recognized [1].

Steganography gives an approach to impart furtively as long as an assailant doesn't figure out how to distinguish the message. The most appropriate kinds of documents for stenographic transmission being, media records because of their huge size. The host records covering different documents are normally called transporters. The transporter records are utilitarian documents and does not bring up an issue or excite doubt. This area records various concealing strategies that are being utilized by and by. Information can be implanted inside a document by exploiting human observation. Sound documents utilize recurrence veiling on tones with comparative frequencies and the easygoing audience does not hear the covered calmer tone [2].

Data security is the most essential resource since loss of data will prompt numerous issues in electronic world. The three systems to be specific cryptography, steganography and watermarking structure the base for secure correspondences. Cryptography is a strategy in which the mystery message is scrambled and sent in an indiscernible arrangement. It scrambles the secret information such that it gives off an impression of being waste to any unapproved client. The mystery information to be imparted is a mix of stages and substitutions and consequently ill-conceived clients couldn't get to the message [3, 4].

Steganography is a specialty of concealing the mystery data inside some other record for the most part known as the cover. The cover medium is picked deliberately so it mirrors some non-suspicious type of correspondence [5].

The primary target of steganography is to give an undercover correspondence between any two clients with the end goal that a unintended client does not access the data by simply observing the cover document. Steganography is not quite the same as cryptography. The fundamental contrast is that the last scrambles the information while the previous just conceals its essence. At the end of the day steganography conceals the information while cryptography scrambles the information. Steganography gives significantly more security when contrasted with cryptography in light of the fact that there is zero chance of any unintended client to realize that a message is being sent though in cryptography, there will dependably be a doubt that a mystery message is being sent. Consequently these are more inclined to be hacked [6].

Figure 1: General schematic description

Watermarking is for the most part utilized for validation and copyrights security. It can be utilized for making a picture with the goal that it is conspicuous. It can likewise be utilized to check an advanced document with the goal that it is proposed to be noticeable (obvious watermarking) or unmistakable just to its maker (imperceptible stamping). The principle target of watermarking is to maintain a strategic distance from the illicit duplicating or claim of responsibility for media. Cryptography and steganography could be utilized on private correspondence; typically for shared premise, however watermarking is utilized between one to numerous i.e. same watermark is implanted in numerous spreads. Fingerprinting is an uncommon sort of watermarking, which would install mark and serial number to recognize a one of a kind duplicate among a few [7].

II. DIGITAL WATERMARKING FEATURES

Joining profoundly metadata in sight and sound substance, advanced water checking systems is valuable despite the fact that, aside from accessibility of substitute components like header of a computerized record which stores meta-data. But since of following highlights the advanced watermarking system is engaging for the addition of unmistakable checks in video and pictures which additionally includes data about sound in sound clasp and so on [2].

Imperceptibility
The commendations of media are of the feeling that watermarks couldn't be modified as installed watermarks are committed without error and they are factually. Noticeable relics in still pictures are not made by watermarks. The watermarks don't adjust the bit rate of video or does not permit any capable of being heard frequencies in sound signs.

Robustness
The utilization of computerized watermarking is by and large for distinguishing proof of possession, so it isn't subjected for any change. The methods of advanced watermarking is fit for supporting distinctive levels of durability against changes assuming any, that can be made to the substance of watermark unconcerned application. The advanced watermarks debased or be demolished because of getting undesirable and hurtful signs and geometric contortions like symmetrical computerized transformation, computerized to simple change, editing, turn, disease, scaling, dithering, a pressure and so on of the substance. Then again in the event that it utilized for the confirmation of the substance. Those ought to effectively break or pulverized at whatever point, the substance is altered for the reason of adjusting the substance which is identified.

Inseparability
It isn't conceivable either to particular or get again into the first position of the watermark after implant with watermark is finished.

Security
Individuals, who are not unapproved, are not permitted to identify and change the watermarks which have been settled immovably in the cover motion by the advanced watermarking method and the keys of watermark guarantee that to distinguish and adjust watermark just approved people are allowed.

III. DISCRETE WAVELET TRANSFORM

Discrete Wavelet Transform (DWT) in numerical investigation and useful examination, a Discrete Wavelet Transform (DWT) is any wavelet change for which the wavelets are disconnectedly inspected. Likewise with other wavelet changes, a key advantage it has more than Fourier changes is worldly determination: it catches both recurrence and area data (area in time). The primary element of DWT is multi-scale portrayal of capacity. By utilizing the wavelets, given capacity can be dissected at different levels of determination. The DWT is additionally invertible and can be orthogonal. The primary DWT was developed by the Hungarian mathematician Alfréd Haar. For an information spoke to by a rundown of 2 n numbers, the Haar wavelet change might be considered to just combine up input esteems, putting away the distinction and passing the whole. This procedure is rehashed recursively, blending up the entireties to give the following scale: at long last bringing about 2n - 1 contrasts and one last aggregate. The Haar DWT outlines the attractive properties of wavelets by and large. To begin with, it can be performed in O(n) activities; second, it catches not just an idea of the recurrence substance of the contribution, by looking at it at changed scales, yet in addition worldly substance, i.e. the circumstances at which these frequencies happen. Joined, these two properties influence the Fast wavelet to change (FWT) an other option to the traditional Fast Fourier Transform (FFT).

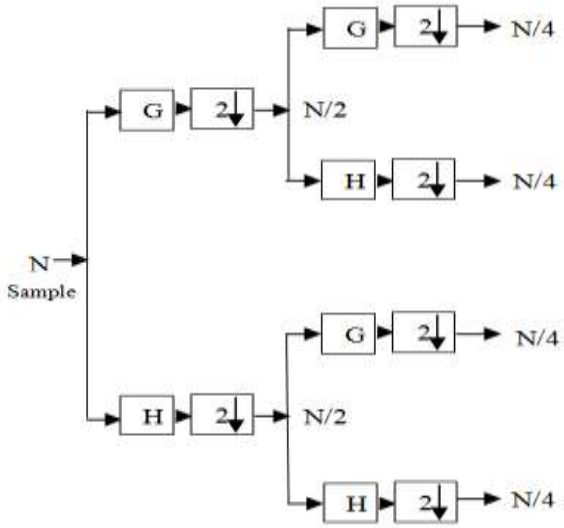

Figure 2: 2- Levels for DWT. Where G, H are the high-pass and low-pass filter coefficient

IV. **PROPOSED METHODOLOGY**

Watermarking Embedding procedure:

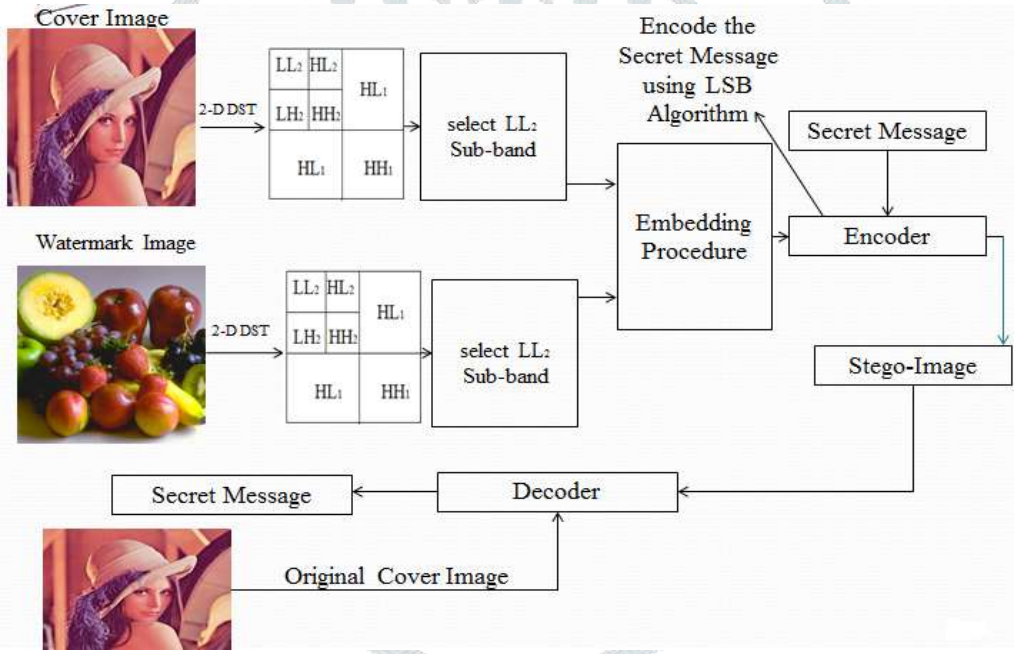

Figure 3: Flow Chart of Proposed Methodology

Algorithm for Watermark Embedding

Step 1: Input Host image, Take cover image (CI).
Step 2: Apply 2-D DWT on CI to decompose it into four sub-bands.
Step 3: Select sub-band LL2 of CI.
Step 4: Take watermark image (WI)
Step 5: Apply 2-D DWT on WI to decompose into four sub-bands.
Step 6: Select sub-band LL2 of WI.
Step 7: Embedding Process
Step 8: Enter Secret Message
Step 9: Apply LSB technique for Encoder
Step 10: Find Stego Image
Step 11: Apply Decoder Process
Step 12: Finally get secret message and watermarked image

V. SIMULATION TOOL

MATLAB is a high level technical computing language and algorithm development tool that can be used in several applications such as data visualization/analysis, numerical analysis, signal processing, control design, etc.
The mean square error (MSE) is defined as,

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[y(i,j) - x(i,j)]^2$$

Where y(i,j) is the watermark image and x(i,j) is the original image.

The peak signal to noise ratio (PSNR) is defined as

$$PSNR = 10\log_{10}\frac{M \times N}{MSE} \quad dB$$

Where M is the number of row and N is the number of column in original image.

VI. RESULTS AND DISCUSSION

The original image of 512×512 pixel value is shown in figure 5.6. This figure divided into four parts. In first part the original random image is resize of the 512×512, the resize image is passing through the 2-D discrete wavelet transform (DWT) and get low frequency image is going to embedding process. Second part shows the watermark image 512×512 pixel value, the watermark image is passing through the 2-D discrete wavelet transform (DWT) and get low frequency watermark image is going to embedding process. Original image and watermark image are passing through the embedding processing and get without noise attack watermarked image shown in third part.

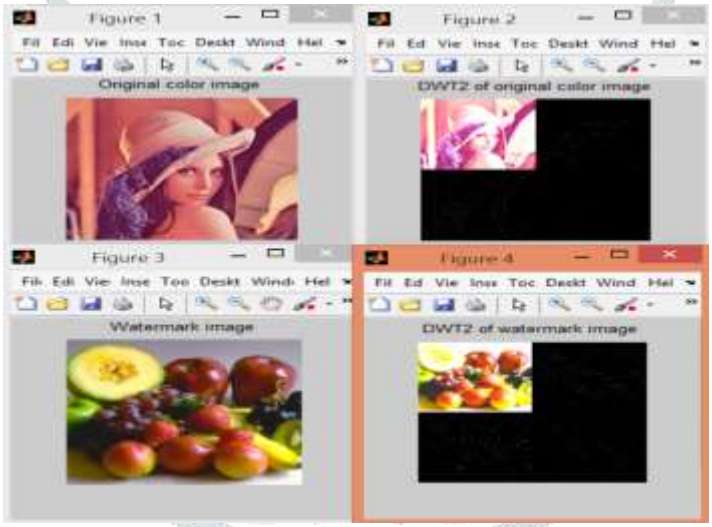

Figure 4: Original Color and Watermark Image

Figure 5: Embedding Processing of Watermark and Original Image

Figure 6: Data Hidden for Watermarked Image using Embedding LSB Stenography Technique

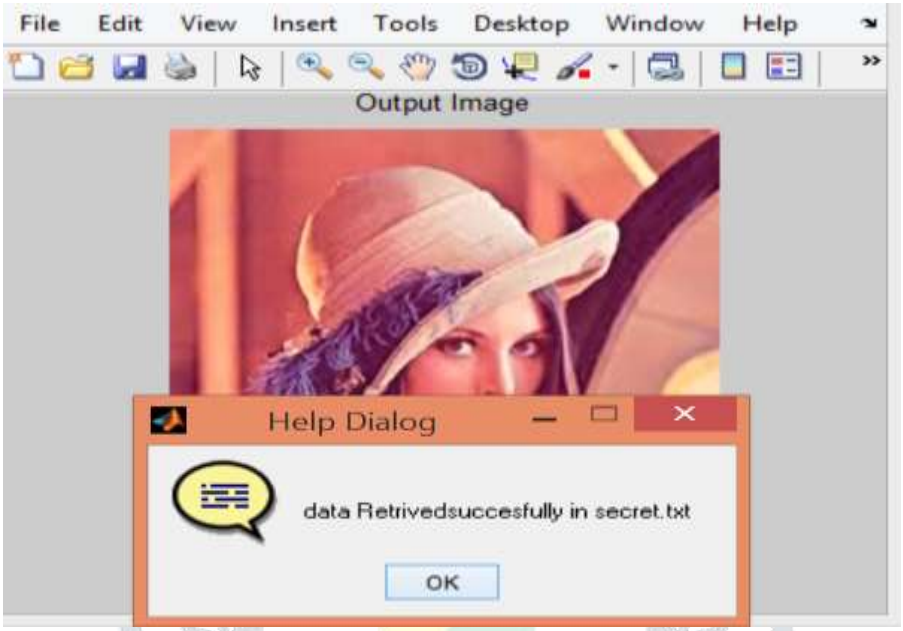

Figure 7: Received Output Image with Retrieved Message

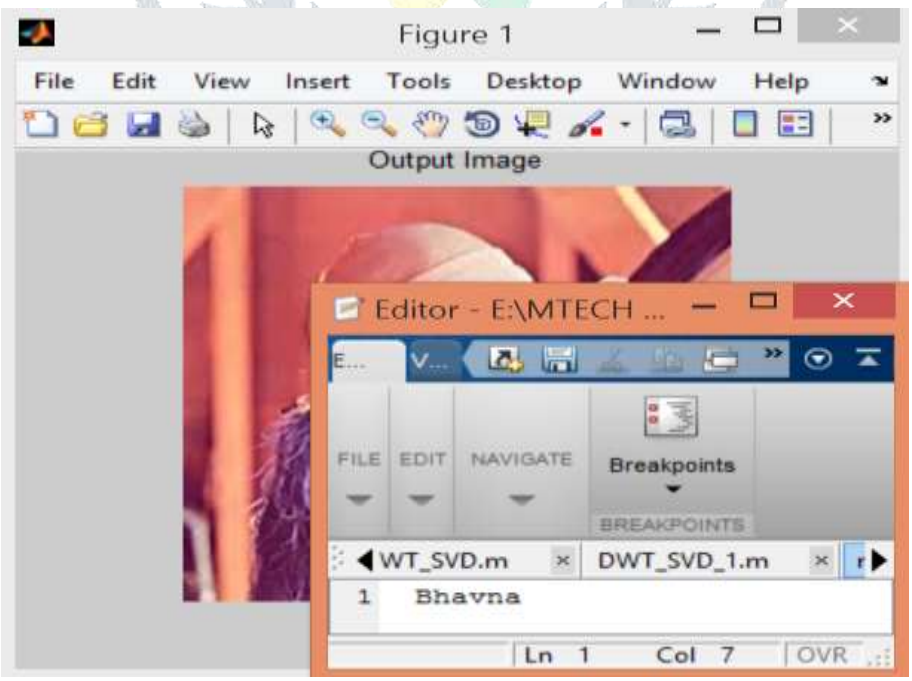

Figure 8: Received Message

Table I: Result for .jpg Image with 50 Characters

Image	Image Type	Characters	Parameter		
			MSE	PSNR	Correlation
Lena Image	.jpg	50	0.0017	52.34 dB	0.9983
Baboon Image	.jpg	50	0.0014	53.54 dB	0.9978
Pepper Image	.jpg	50	0.0012	53.98 dB	0.9932

Table II: Result for .bmp Image with 50 Characters

Image	Image Type	Characters	Parameter		
			MSE	PSNR	Correlation
Lena Image	.bmp	50	0.0066	53.65 dB	0.9922
Baboon Image	.bmp	50	0.0072	51.76 dB	0.9905
Pepper Image	.bmp	50	0.0074	50.54 dB	0.9946

Table III: Result for .png Image with 50 Characters

Image	Image Type	Characters	Parameter		
			MSE	PSNR	Correlation
Lena Image	.png	50	0.0096	46.55 dB	0.9967
Baboon Image	.png	50	0.0094	48.54 dB	0.9933
Pepper Image	.png	50	0.0098	45.32 dB	0.9956

Table IV: Comparison Result for PSNR (dB)

	Previous Algorithm		Proposed Algorithm
Image	**DCT Technique**	**SVD Technique**	**DWT-SVD Technique**
Lena Image	42.65	41.24	61.959
Baboon Image	41.37	38.89	58.618
Pepper Image	42.65	41.38	54.242

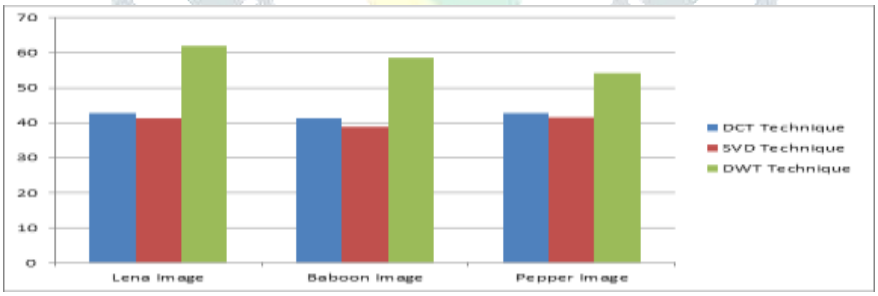

Figure 9: Bar Graph of Previous and Proposed Algorithm

Figure 9 shows the graphical illustration of the performance of proposed method discussed in this research work in term of PSNR. From the above graphical representation it can be inferred that the proposed algorithm gives the best performance for Lena images.

Table V: Comparison Result for MSE

	Previous Algorithm		Proposed Algorithm
Image	**DCT Technique**	**SVD Technique**	**DWT-SVD Technique**
Lena Image	0.0056	0.0036	0.0017
Baboon Image	0.0049	0.0032	0.0014
Pepper Image	0.0073	0.0029	0.0012

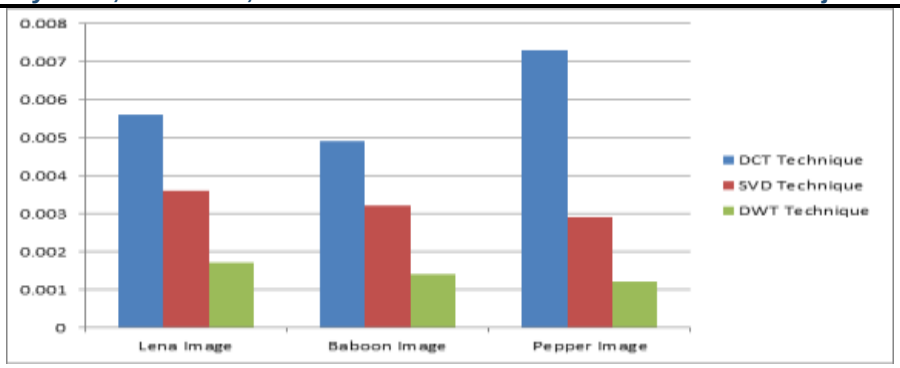

Figure 10: Bar Graph of Previous and Proposed Algorithm

Figure 10 shows the graphical illustration of the performance of proposed method discussed in this research work in term of MSE. From the above graphical representation it can be inferred that the proposed algorithm gives the best performance for Pepper images.

VII. CONCLUSION

It has been demonstrated that the utilization of DWT-LSB with combination technique has enhanced the security of the watermarking plan. Specific consideration is given to the proposed plan to ensure secure watermark inserting and simple extraction. The watermark is intangible to the human eye and recoverable more often than not. The watermarked pictures were evaluated for loyalty by utilizing PSNR and MSE. The new strategies could offer huge focal points to the computerized watermark field and give extra advantages to the copyright security industry. The developed technique is increase the PSNR is 33.43% for Lena image and decrease the MSE is 52.77% for Lena image.

VIII. FUTURE SCOPE

The proposed design is also applied to cryptography and secures the data in image of different file format. We can also calculate the other parameter i.e. structural similarity (SSIM), Normalized mean square error (NMSE), Pearson correlation.

REFERENCES

[1] Nazir A. Loan, Nasir N. Hurrah, Shabir A. Parah, Jong Weon Lee, Javaid A. Sheikh, and G. Mohiuddin Bhat, “Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption”, Received January 4, 2018, accepted February 7, 2018, date of publication March 16, 2018, date of current version April 25, 2018.

[2] N. Senthil Kumaran, and S. Abinaya, “Comparison Analysis of Digital Image Watermarking using DWT and LSB Technique”, International Conference on Communication and Signal Processing, April 6-8, 2016, India.

[3] Aase, S.O., Husoy, J.H. and Waldemar, P. (2014) A Critique of SVD-Based Image Coding Systems, IEEE International Symposium on Circuits and Systems VLSI, Orlando, FL, Vol. 4, Pp. 13-16.

[4] Ahmed, F. and Moskowitz, I.S. (2014) Composite Signature Based Watermarking for Fingerprint Authentication, ACM Multimedia and Security Workshop, New York, Pp.1-8.

[5] Akhaee, M.A., Sahraeian, S.M.E. and Jin, C. (2013) Blind Image Watermarking Using a Sample Projection Approach, IEEE Transactions on Information Forensics and Security, Vol. 6, Issue 3, Pp.883-893.

[6] Bidyut Jyoti Saha, Kunal Kumar Kabi and Arun, “Non Blind Watermarking Technique using Enhanced One Time Pad in DWT Domain”, International Conference of Digital Signal and Processing, ICCCNT, IEEE 2014.

[7] M. Kim, D. Li, S. Hong, "A Robust Digital Watermarking Technique for Image Contents based on DWT-DFRNT Multiple Transform Method", *International Journal Multimed. Ubiquitous Eng.*, vol. 9, no. 1, pp. 369-378, Jan. 2014.

[8] Jiann-Shu Lee and Fei-Hsiang Huang, “A New Image Watermarking Scheme Using Non-dominated Sorting Genetic Algorithm II”, International Symposium on Biometrics and Security Technologies, IEEE 2013.

[9] Baloshi Mathews and Madhu S. Nair, “Modified BTC Algorithm for Gray Scale Images using max-min Quantizer”, Automation, Computing, Communication, Control and Compressed Sensing, PP. 01-05, 2013 IEEE.

[10] Wang Santosh, U. V. S. Sitarama Varma, K. S. K Chaitanya Varma, Meena Jami, V. V. N. S Dileep, “Absolute Moment Block Truncation Coding For Color Image Compression,” International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-2, Issue-6, PP. 53-59, May 2013.

[11] Lee, J. S., Huang, F. H., & Kuo, H. C., “A New Image Watermarking Scheme Using Non-dominated Sorting Genetic Algorithm II,” In Biometrics and Security Technologies (ISBAST), International Symposium, pp. 56-61, IEEE 2013.

[12] Teruya Minamoto and Ryuji Ohura, “A non-blind digital image watermarking method based on the dual-tree complex discrete wavelet transform and interval arithmetic”, Ninth International Conference on Information Technology- New Generations, IEEE 2012.

[13] Minamoto, T., Ryuji, O., “A non-blind digital image watermarking method based on the dual-tree complex discrete wavelet transform and interval arithmetic,” In Information Technology: New Generations (ITNG), Ninth International Conference, April, pp. 623-628, IEEE 2012.

[14] Pradhan, C., Saxena, V., & Bisoi, A. K., “Non blind digital watermarking technique using DCT and cross chaos map,” In Communications, Devices and Intelligent Systems (CODIS), International Conference, pp. 274-277, IEEE 2012.

[15] Chen and K. V. Karthik, “A Modified Three Level Block Truncation Coding _or Image Compression”, International Conference on Pattern Analysis and Intelligent Robotics, PP.31-35, June 2011 IEEE.