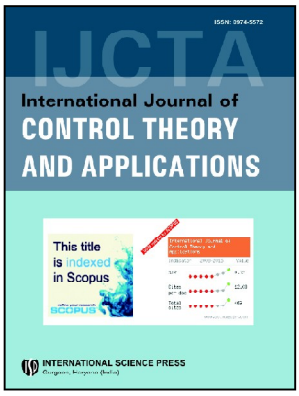



International Journal of Control Theory and Applications

ISSN : 0974-5572



Volume 10 • Number 10 • 2017

# A Technique for Encrypted Image Watermarking Using Wavelet Transformation with Classification Technique

**Ashminder Kaur[1] and Lofty Sahi[2]**

*Chandigarh Engineering College, LandranChandigarh Engineering College, Landran*
*E-mail: aashusaini6776@gmail.com[1]cecm.infotech.loftysahi@gmail.com[2]*

***Abstract:*** The digital watermarking is the inserting/hiding of info within digital record without unusually changing the file itself. Digital watermarking method is becoming more significant in this emerging society of internet. It is used to secure the information against the prohibited distribution in the form of videos, images and audios. It methods are used in numerous fields such as broadcast monitoring, copy-right protection and owner verification. Digital image watermarking method is the procedure of embedding watermark in the form of image that contain the important info then it extract and detect that important information. In this work defines a protected multi-level watermarking scenario in which the encrypted text acts as a watermark. The procedure is created on the protected supper range or frequency domain method for numeral images in discrete wavelet transformation. In the embedding process, we can apply the DWT decays an input into two components like lower bound and upper bound. The discrete wavelet transform is a valuable way designed for signal exploration as well as picture handling, chiefly in multi-resolution description. An encryption using Advance encryption standard for encrypt the images. It is a web instrument to scramble and decode content utilizing AES encryption calculation. To secure the secrete message then classify the network using BPNN. The Back Propagation (BPNN) neural network model consists of an input layer, some hidden layers and an output layer. After classification, we calculate the performance parameters like Bit error rate and peak signal to noise ratio.

***Keywords:*** Digital watermarking, discrete wavelet transformation, Back propagation neural network, Encryption algorithm and psnr and mse.

## I. INTRODUCTION

Image watermarking is the hiding of info within digital record of file without considerably changing the record file itself. Now image watermarking is including consideration due to the speed implementing in the internet rush. Image watermarking attained is famous due to its importance in authentication and copy-right protection for multi-media data [1]. It is added invisible in main image so that it can be extracted at advanced times for the proof of rightful possession. Numerous image watermarking methods are proposed for copy-right authentication of multi-media information from being misused. Image Watermarking is the procedure of embedding data into a multi-media element such as imagery, audio and video record file for the aim of authentication. The hided data

could be advanced and detect the multi-media data for security purposes [2]. Watermarking is the info about region, protection and robustness. Main block diagram of watermarking is shown in fig. 1:

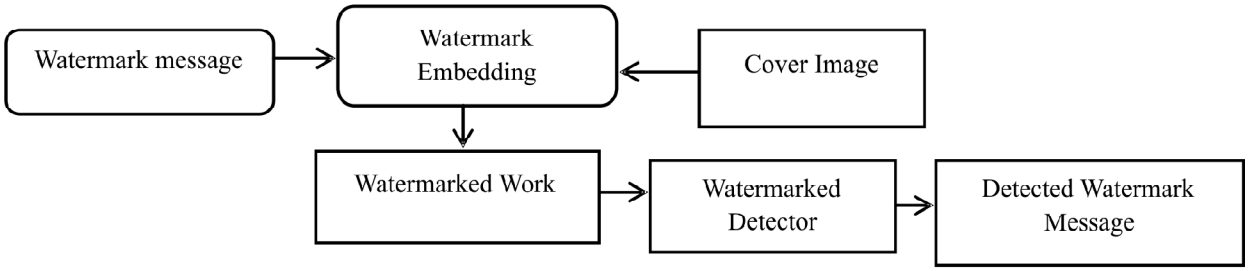



**Figure 1: Block Diagram of Watermark Hiding and Detection Procedure**

Image watermarking methods could be divided as follows:

*a)* *Spatial-Domain:* Watermarking system directly changes the major pixels of image to hide the watermark data [3].

*b)* *Transformation-Domain:* Watermarking system modifies the frequency transforms of information hide the watermark data. This has proofed to be more robust than the spatial domain watermark.

Each and every watermarking method creates tradeoffs amongst them, taking into consideration about the application domain. In the next subsections we explain each of the features stated above, as well as talk over in what way its significance as well as its explanation differs with application. The essential features of watermarking are given as follows:

a) Robustness[4]

b) Security

c) Fragility

d) Capacity

In this section described that the section I explain the image watermarking, methods of watermarking and advantages of image watermarking. Section II we described that the previous work of this topic. Section III explained that the issues arise in the watermarking. In Section IV described that the simulation work in (a) discrete wavelet transformation (b) Encryption algorithm using Watermarking system and Classified the encrypted data using Back propagation neural network. In section V described that the result and discussions and last one section VI defined the conclusion and future work.

## II. RELATED WORK

In this section described the previous work of this topic (image watermarking) It studies diverse sorts of existing strategy for picture compression. Compression of a picture is essentially distinctive then compression of twofold crude information. Presently there is inquiry may be emerge that how to picture pack and which sorts of procedure is utilized. For this reason there are essentially two sorts are system are presented specifically lossless and lossy picture compression methods [5].

**[6] Qing-Cheng Li et al**; **2008** presents a novel text watermarking technique but for the Chinese text merely. In his or her technique he's mentioned this some bitstream design of the text on the basis of which the merging can be done .His approach also defines the pictographic approach of the text and the visual potential of

the person. This technique will be despite the fact that comes with a usefulthinking but the difficult is as the Chinese language is so sophisticated, it fits there but not with all and every terminology. His / her algorithm may be intended particularlyfor Chinese characters & hence this algorithm cannot be used for global language.**[7] Zeneca JaliI, Hamza Aziz Saad Bin Shahidet al; 2010** presented a zero text watermarking system in the international conference of 2010. According to them, existing text watermarking algorithms are not robust against random insertion and removal attacks on particular text document. By means of growing capacity of attack, the existence of watermark in the text file turn out to be challenging and hence they developed a novel text watermarking algorithm that can be used for copyright protection of textual materials. They were matched their results along with many other existing algorithms of the same contrast and their results are found to be effective enough to get proceeded for change.**[8] Makarand L. Mali et al; 2013** presented a watermarking scheme on the basis of NEURAL networks. It was a fantastic hint to introduce Neural Networks into the contrast associated with encryption. The Neural Network produces weight for all and every input provided to it rather than taking everything as an input stream. The pattern altering of neural network is quite similar to SVM as it also converts the entire input according its simplification & then precedes Hence his technique is quite effective and can be considered for future development process.**[9] Nidhi Divecha et al; 2013** presented a watermarking structure based on the wavelet quantization method which is again an appreciable work in this filed. DWT stands for Discrete Wavelet Transformation and it changes the entire data scenario into waves. Preceding the scripts as wave is a unique technique in this type of enactment. The time and effort accomplished simply through Indi had only one negative aspect , It did not mention the kind of wavelet transformation she is using as there are a lot of wavelet change like Dabuchi , Symlet and others and hence her method can be tried with the overhead mentioned wavelet family members .

## III. PROBLEM FORMULATION

Lots of paper Study, we found Digital watermarking is the process of introducing a digital signal or pattern into digital satisfied. The signal, known as a watermark, can be used to identify the owner of the work, to authenticate the content, and to trace prohibited copies of the work [10]. A watermark is a form, image or text that is captivated onto paper, which offers indication of its authenticity. Digital watermarking is an allowance of this concept in the digital world. The system implements visible watermarking. With development of digital systems, the presentation of picture, digital cameras as well as audio devices is also improved. The content of digital picture/ audio/video can easily be modified so that it is very difficult to detect what changes has been taken place. In the circumstance of quite delicate legal papers and medical pictures, this becomes progressively significant to verify the authenticity of original content. For authentication, a watermark is embedded in original satisfied which is used to appraise the strength of such type of content. If the data is changed via any attacker unkindly, the watermark gets different and therefore the content will be considered non-genuine. So, the existing work will use wavelet transformation along with evolutionary algorithm in hybridization.The main purpose of the watermark is to recognize who the proprietor of the digital data is, but it can also verify the intended recipient. The problem of this research work is to classify the current architecture by introducing DWT with AES Algorithm and Back Propagation Neural Network [11].

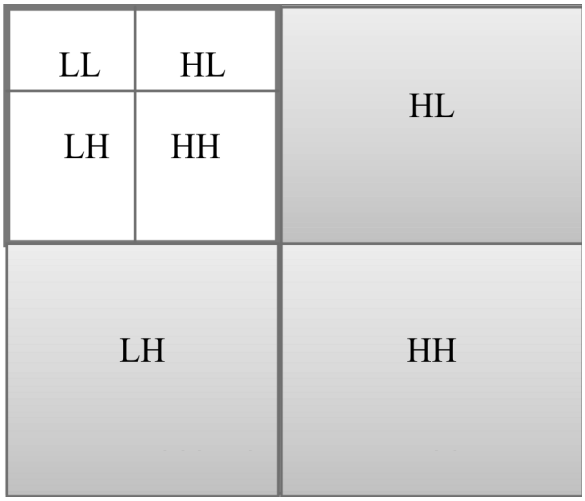
## IV. SIMULATION WORK

In this section, we implement the discrete wavelet transformation used for divide the information in lower bound and upper bounds, AES algorithm for secure the hiding information and Classify the secure information.

### (A) Discrete Wavelet Transformation

Discrete wavelet transform in image procedure is to multi differentiated decomposing the image sub-image diverse spatial domain and independent frequency district and the transform coefficient of sub imagery [13].

After the real image has been Discrete Wavelet Transformation transformed, it is decomposed into four frequency descripts which is one lower frequency district and 3 high frequency districts. If the information of low-frequency district is discrete wavelet transformation transformed, the sub-level frequency district info will be obtained. A two-dimensional image after thrice of times DWT de-composed can be shown in figure 1;




Where L represents low pass filter, H defines that the High pass filter. The real image could be decomposed of districts of frequency of HL, LH, HH and LL[14].

The low frequency information also could be de-composed into sub level frequency information of LL, HL, HL and HH. By completing this real image would be de-composed for n-level wavelet transformation. The info of low frequency district is an image nearest to the original image is in this frequency district. The frequency districts of LH, HL and HH respectively, represent the level information detail, the up-right information and the diagonal information of the real image.

## (B) Advanced Encryption Algorithm

The encryption procedure utilizes a group of particularly derivative keys which are known as round keys. These are further applied, alongside through some other processes, on an array of information which embraces precisely solitary block of information that is the information/data to be encoded. This particular array entitled as the state array.

| *Algorithm in Encryption* |
|---|
| Step 1: We proceeds to the subsequent steps to encode a 128-bit block: |
| Step 2: Develop the group of round keys from the cipher key. |
| Step 3: Initialize the state array using the block data (i.e. plaintext). |
| Step 4: Add the primary round key to the beginning state array. |
| Step 5: Execute9th rounds of state manipulation. |
| Step 6: Execute the 10th as well as the final round of state manipulation. |
| Step 7: Duplicate the finishing state array out as the encoded data (cipher text). |

| Algorithm in Decryption |
|---|
| Step 1: Execute the initial decryption round of state manipulation. |
| Step 2: Execute nine full decryption rounds of state manipulation. |
| Step 3: Perform final round of state manipulation. |
| Step 4: Copy the finishing state array out as decode (decrypted) data. |

The purpose due to which the rounds have been scheduled as "nine followed by a final tenth round" is for the reason that the tenth round encompasses a slightly dissimilar manipulation as of the others.Each one of these operations is applied to the current state array and produces a new version of the state array. In some of theinfrequentinstances, the given state array is changed by the operation [15].

## (C) Back Propagation Neural Network

The Back propagation neural network used is capable of perform the preprocessing of the training data. As the data doesn't have the uniform representation so the neural network doesn't applied to the unprocessed data. For Training purpose, winner value has highest value. The randomly obtained initial synaptic weights of the neural network covers a range between -0.5 and 0.5.Best method of testing a neural network is to test a software application if all the coverage conditions are satisfied.

It iteratively learns a set of weights for prediction of class label tuples. The predicted output is compare with target value to check the error. This algorithm is type of supervised learning and used in feed forward neural network to train the network.

## (D) Planning of work

In methodology we will follow these steps:

Step 1 : First, we should take the plain image.

Step 2 : Then we will call DWT for image sub-division.

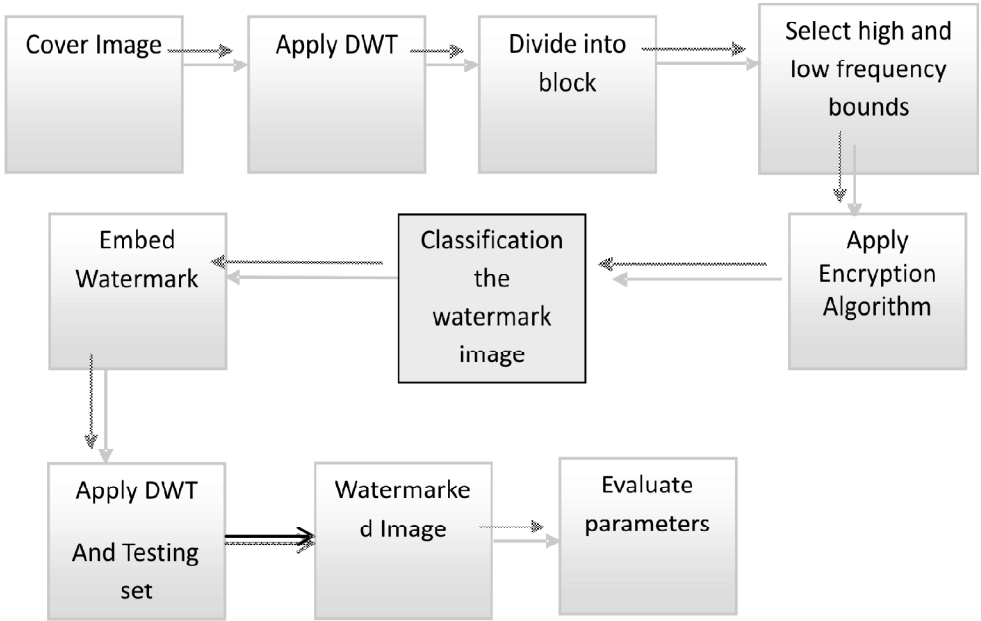



**Figure 3: Flow Chart of proposed work**

Step 3 : Then the DWT component will be taken for watermarking.

Step 4 : Get image that is to be watermarked of same size or large size.

Step 5 : Then AES algorithm will be used for security or image watermarking Stop.

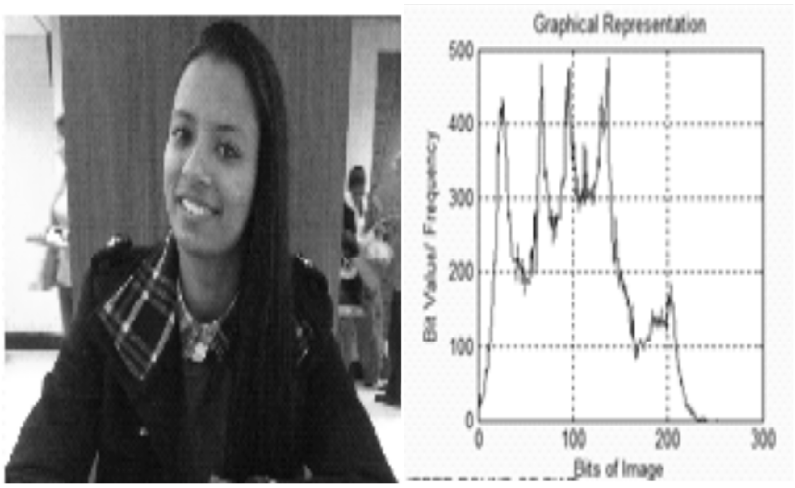
Step 6 : Then after this procedure it would be watermarked.

Step 7 : Last one Classify the watermark images for training and testing.

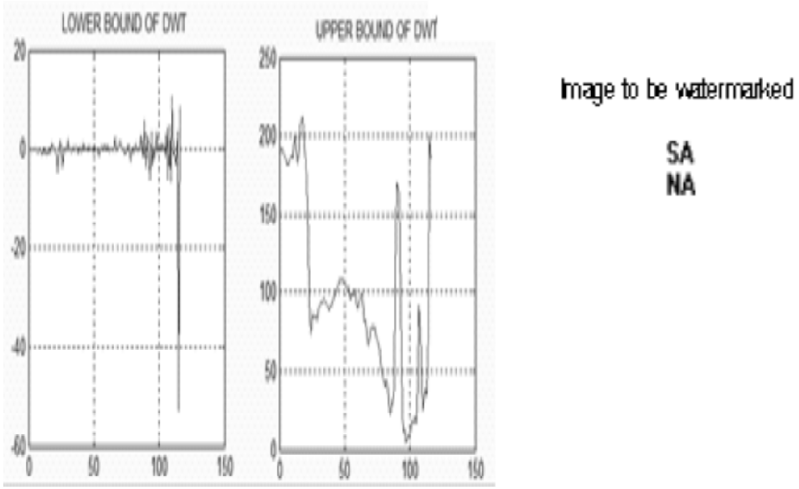
Step 8 : In the end, we will evaluate the results based on BER, PSNR and MSE parameter.

## V. RESULT AND DISCUSSIONS

The subsequent Development Tools has been used in the expansion of this work. There may also be other tools which can be used in this development as it depends person to person and his interest. Therefore the used tools are: (i) least amount of 3 GB of RAM (ii) Intel Pentium III Processor or overand (iii) MATLAB R2013a.




(i) Original Image (ii) Histogram




(iii) Discrete Wavelet Transformation using and (iv) Watermarked Image

**Figure 4: (i) Original Image (ii) Histogram of the image (iii) Discrete Wavelet Transform (Lower Bound and Upper Bound) and (iv) Watermarked Image**

In this figure shows that the upload the original image from the database and histogram creates i.e used for find the maximum and minimum intensity of the image. Discrete wavelet transformation creates the wavelet of the upper and lower bounds of the image. In this procedure is any wavelet transform for which the wavelets are separately sampled. With other wavelet transformation, a key advantage it has over FFT is temporal resolution. It considers both frequency and position information.


**Figure 5: (i) Embedding Image and (ii) Extracted Image**

In this figure represents that the embed image refers to any type of multimedia file that you might insert, or embed into the Web page. This includes files like graphics and sound files and image represented that the extracted image.

**Table I**
**Proposed Parameters (PSNR and BER)**

| *IMAGE NO.* | *PSNR* | *BER* |
|---|---|---|
|  | 48.1308 | 0.66852 |
|  | 49.56 | 0.568 |
|  | 48.09 | 0.478 |

| | | |
|---|---|---|
|  | 49.80 | 0.345 |
|  | 50.0 | 0.234 |
|  | 47.56 | 0.76 |
|  | 49.78 | 0.67 |

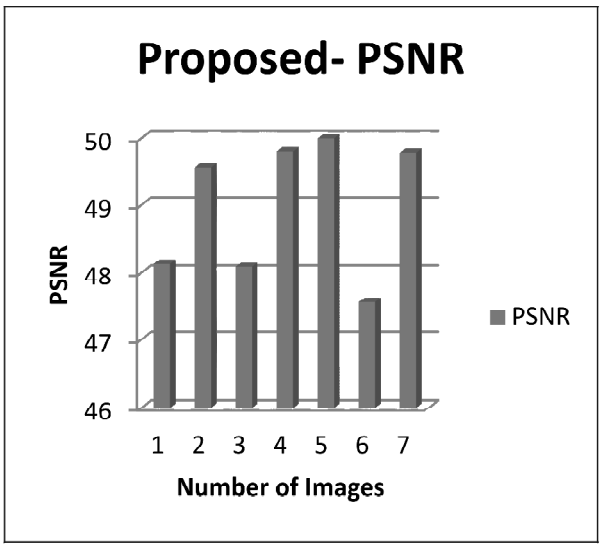



**Figure 6: Proposed-Peak Signal to Noise Ratio**

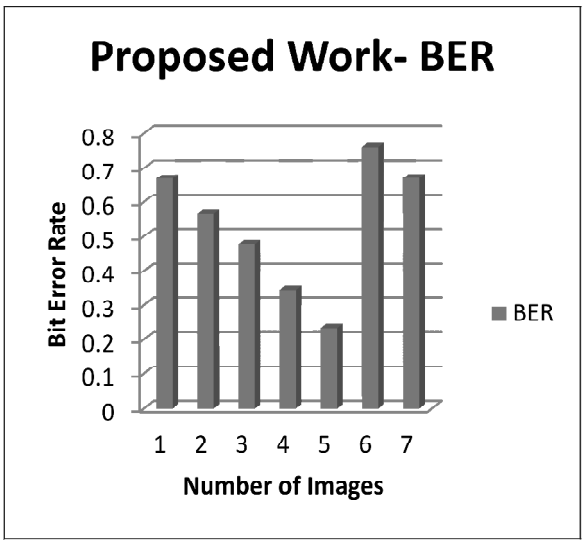



**Figure 7: Proposed–Bit Error Rate**

Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is most easily defined via the mean squared error (MSE).

Bit error rate means the rate at which errors occur in the transmission of digital data.

## VI. CONCLUSION AND FUTURE SCOPE

This thesis work designates the algorithm to use a discrete wavelet transformation, Des encryption and back propagation neural network with an included benefits of hiding the trained network weights with the original main image. The watermarked image has a better healthiness and the stillness of the real image is also upper preserved. For the extraction, only main image is required and no external weights records need to be supplied with the watermarked picture. Thus, this work leads to successful watermarking structure. The watermarks bits are embedded into the mid frequency band of the DWT coefficients such that the host image is not partial and yields a better PSNR value. In the inserting process the back propagation neural network is used to remember the original un-watermarked sub image coefficients, this network is used at the withdrawal process to get back the watermark bits. Experimental consequences show that the proposed algorithm is robust to many image processing attacks and for inaudibility it yields good PSNR value. In future Scope, we will use the hybrid techniques (dwt and dct) and hybrid optimization (GA+BFO) technique used and to improve the PSNR and BER.

## REFERENCES

[1] Zhang, Yanqun. "Digital watermarking technology: A review." In Future Computer and Communication, 2009. FCC'09. International Conference on, vol 9, pp. 250-252. IEEE, 2009.

[2] Vybornova, Olga, and Benoit Macq. "Natural language watermarking and robust hashing based on presuppositional analysis." In 2007 IEEE International Conference on Information Reuse and Integration, vol 7,pp. 177-182. IEEE, 2007.

[3] I. Cox and M. L. Miller, "A review of watermarking and the importance of perceptual modeling", Proceedings of SPIE, Human Vision and Electronic Imaging II, vol. 3016, pp. 92–99, 1997.

[4] I. J. Cox and J.-P. Linnartz, "Some general methods for tampering with watermarks", IEEE Transactions on Selected Areas of Communications, vol. 16, no. 2, pp. 587–593, 1998.

[5] F. A. P. Petitcolas, R. Anderson, and M. G. Kuhn, "Information hiding - A survey", Proceedings of the IEEE, vol. 87, no. 7, pp.1062– 1077, 1999.

[6] Li, Qing-Cheng, and Zhen-Hua Dong. "Novel text watermarking algorithm based on Chinese characters structure." In Computer Science and Computational Technology, 2008. ISCSCT'08. International Symposium on, vol. 2, pp. 348-351. IEEE, 2008.

[7] "ZuneraJaliI, Hamza Aziz Saad Bin Sahib\ Muhammad Arif "A Zero Text Watermarking Algorithm based on Non-Vowel ASCII Characters 978-1-4244-8035-71101$26.00 © vol. 10,pp- 250-256, IEEE, 2010.

[8] Mali, Makarand L., Nitin N. Patil, and J. B. Patil. "Implementation of text watermarking technique using natural language watermarks." In*Communication Systems and Network Technologies (CSNT), 2013 International Conference on*,vol.13, pp. 482-486. IEEE, 2013.

[9] Divecha, Nidhi, and N. N. Jani. "Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color images." In*Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on*, vol.13,pp. 204-208. IEEE, 2013.

[10] Alam, Fahim Irfan, and Md Mohaiminul Islam. "An investigation into image hiding steganography with digital signature framework." In *Informatics, Electronics & Vision (ICIEV), 2013 International Conference on*, vol.13,pp. 1-6. IEEE, 2013.

[11] Juan R. Hernández," DCT-Domain Watermarking Techniques for Still pictures: Detector Performance Analysis and a New Structure". *IEEE TRANSACTIONS ON PICTURE PROCESSING*, Vol. 9, no. 1,pp-1-6, JANUARY 2000.

[12] V. Santhi, "DWT-SVD Combined Full Band Robust Watermarking Technique for Color pictures in YUV Color Space", *International Journal of Computer Theory and Engineering,* Vol. 1, No. 4, pp. 1793-8201, October 2009.

[13] Cheema, Prabhjot Kaur, and Kamaljit Kaur. "Comparison of Text Watermarking Approaches with the Proposed Approach Based on Encryption Techniques used for Creating Watermarks." *International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 7,pp-203-208, 2014.*

[14] Saha, Bidyut Jyoti, Kunal Kumar Kabi, and Chittaranjan Pradhan. "A robust digital watermarking algorithm using DES and ECC in DCT domain for color images." In *Circuit, Power and Computing Technologies (ICCPCT), 2014 International Conference on*,vol.14 pp. 1378-1385. IEEE, 2014.

[15] Ye, Ruisong. "A novel image scrambling and watermarking scheme based on orbits of Arnold transform." In *Circuits, Communications and Systems, 2009. PACCS'09. Pacific-Asia Conference on*, vol.9, pp. 485-488. IEEE, 2009.