Implementation of Digital Watermarking For Image Security with EBCOT Algorithm and Error Correcting Codes

Keta Raval, Rajni Bhoomarker, Sameena Zafar

Abstract-In the cutting edge of technology, secured communication media becomes the essential need of multimedia broadcasting. In the reference of multimedia broadcasting, digital audio, video, internet data needs copyright authentication to prevent unauthorized access of data. Digital Watermarking by DWT-DCT with secrete key provides robustness as well as securing information. Digital Watermarking is processed by some way before it reaches to the receiver. The uncompressed digital image has lots of problems related to bandwidth. We can do effective image compression by EBCOT Algorithm. Error correcting codes reduces the effect of noises and attacks on communication channel. Digital watermarking provides cost effective solution for image security and communication.

Index Terms—Discrete Cosine Transform, Discrete Wavelet Transform, Embedded Block Coding With Optimal Truncation.

I. INTRODUCTION

Digital Watermarking is become essential need of multimedia communication. Digital Watermarking is an embedding technique which inserts the hidden information in the form of image, audio, video and text. After embedding the watermark specific algorithm is applied. Here we apply DCT-DWT joint transform robust algorithm. After inserting the watermark the original image slightly modified. This watermark image transmitted over communication channel. Watermark over communication channel may corrupted by noise. To archive the high reliability of watermark detection, the watermark detection process has to be robust to the alterations in the host image caused from both unintentional and intentional distortions (Called “attacks”) [2].

The aim of attacks is not always completely remove or destroy watermark but usually to disable its detection. The aim of attacks is not always to completely remove or destroy the watermark but usually to disable its detection distortions are limited to those not producing excessive degradations. Otherwise, the transformed watermarked object would be unusable. These distortions could also introduce degradation to the performance of the system.

The use of digitally formatted image and video formation is rapidly increasing with the development of multimedia broadcasting, network databases and electronic publishing. This evolution provides many advantages as easy, fast and inexpensive duplication of products.

However, it also increases the potential for unauthorized distribution of such information, and significantly increases the problems associated with degradations. Otherwise, the transformed watermarked object would be unusable. These distortions could also introduce degradation to the performance of the system. The use of digitally formatted image and video formation is rapidly increasing with the development of multimedia broadcasting, network databases and electronic publishing. This evolution provides many advantages such as easy, fast and inexpensive duplication of products. However, it also increases the potential for unauthorized distribution of such information, and significantly increases the problems associated with enforcing copyright protection. The rapid evolution of digital technology makes the development of reliable and robust schemes for protecting digital still images, audio and video from piracy a matter of urgency. Piracy of attacks includes illegal access to transmitted data in networks, data content modification, production and retransmission of illegitimate copies. The impact of such attacks might be very large, both in financial and security terms [2]. Robust image watermarks are watermarks designed to survive attacks including signal processing operations and spatial transformations. To evaluate robust watermarks, we need to evaluate how attacks affect the watermark of an image. The mean square error (MSE) and peak signal to noise ratio (PSNR) are the most popular metric to measure fidelity.

The most important parameter of watermark communication is encryption key. Watermarking requires secrete key for owner. A secret key is use during the embedding and the extraction process in order to prevent illegal access to the watermark.

A digital watermark is a distinguishing piece of information that is assign to the data to be protect. One important requirement by this is that the watermark cannot easily extract or removed from the watermarked object. Watermarks and watermarking techniques can classify into several categories taking into account by this various criteria). As it can note, one of the criteria is embedding domain in which the watermarking is implement [3].

Manuscript published on 28 February 2013.
***** Correspondence Author (s)

Ms Keta Raval , Dept. of Electronics and Communication ,Patel Institute of Engineering and Science, RGPV, Bhopal, M.P., India.
Mrs. Rajni Bhoomarker , Dept. of Electronics and Communication Patel College of Science and Technology, RGPV, Bhopal, M.P., India.
Mrs Sameena Zafar, HOD, Department of Electronics communication, Patel College of Science and Technology,, RGVP, Bhopal, M.P, India.

For example, watermarking can do in the spatial domain. An alternative possibility is the watermarking in the frequency domain. Watermarking techniques can classify into the following four categories according to the type of the multimedia document to watermark. According to the human perception, digital watermarks can classify into three different categories, like Visible, Invisible-Robust watermark, Invisible-Fragile watermark, Dual watermark

An advantage of the spatial techniques discussed above is that they can easily applied to an image; regardless of subsequent processing, (whether they survive this processing however s a different matter entirely). A possible disadvantage of spatial techniques is they do not allow for the exploitation of this subsequent processing in order to increase the robustness of the watermark. A watermarking algorithm using transform (frequency) domain techniques focus on embedding information in the frequency domain of the image as opposed to the spatial domain. The most popular transforms where the frequency domain watermarking algorithms work are Fourier Transform (FT), Discrete Cosine Transform (DCT) and Wavelet Transform (DWT). These are applies to transform an image into the frequency domain where the coefficients of the digital image are separated into different priorities in accordance to the human perception system. The watermark bits embed by modulating the magnitude of these co-efficient.

II. BASIC THEORY OF WATERMARKING

The purpose of digital watermarking is to embed or insert a message into a image in a secure way. The embedded watermark in DCT-DWT algorithm is in the form of two images original image and watermark message. A watermarked image may be distorted before it is available to the watermark detector at receiving side. A block diagram of watermarking system is shown in Figure 1. The watermarked embedded and recover through various schemes. A secret key is use during the embedding and the extraction for copyright authentication. The original image and the desired watermark are embedded using one of the various schemes which are currently available. The obtained watermarked image is passes through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark. The different techniques differ in the way in which it embeds the watermark on to the cover object.

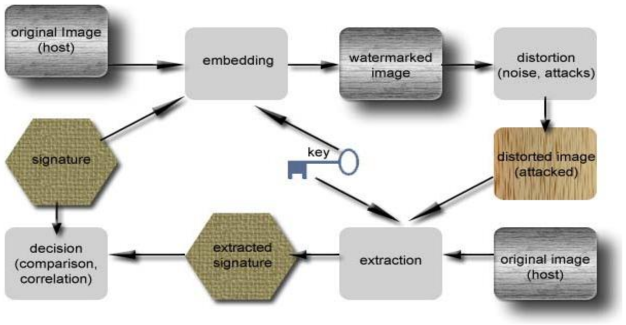

Figure 1 Typical Watermarking block diagram

III. TYPES OF WATERMARKING

A digital watermark is distinguishing way information to be protected. Watermarking techniques can classify into several categories (see in Figure 2 types of watermarking) For example, watermarking can do in the spatial domain and the frequency domain.

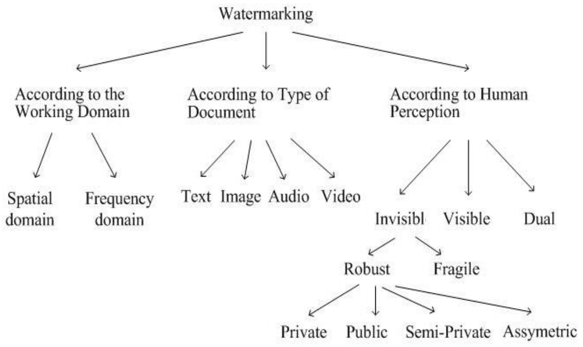

Figure 2 Types of watermarking methods

Watermarking techniques can classify into the following four categories according to the type of the multimedia document to watermark. According to the human perception, digital watermarks can classify into three different categories like - Visible watermark, Invisible Robust watermark, Invisible Fragile watermark, Dual watermark.

IV. TRANSFORM DOMAIN WATERMARKING

An advantage of the spatial techniques is that they can easily apply to any image. A disadvantage of spatial techniques is they do not allow for the subsequent processing in order to increase the robustness of watermark. Watermarking algorithm by using transform domain techniques embedding information into the frequency domain .The most popular transforms where the frequency domain watermarking algorithms work are Discrete Fourier Transform (FT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). DFT decompose image in sine and cosine form. DFT gives output in complex value and it's required more frequency rate. DFT is not used now days due to above disadvantages.

A. Discrete Cosine Transform

Discrete Cosine Transformation (DCT) transforms a signal from the spatial into the frequency domain by using the cosine waveform. DCT divide the information energy in the bands with low frequency and DCT popularity in data compression techniques such as JPEG and MPEG.The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of the image. Here the middle frequency bands chosen such that they minimize to avoid the visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies). FL is use to denote the lowest frequency components of the block, while FH is used to denote the higher frequency components.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

FM is Chosen as the embedding region as to provide additional resistance to lossy compression techniques. The DCT and IDCT is calculated by equation 1 and equation 2 respectively. Here (j, k) are transformed basic functions of (m, n) for rows and columns.

$$F(jk) = a(j)a(k)\sum_{n=0}^{N-1}\sum_{m=0}^{N-1} f(mn)$$

$$\cos\frac{(2m+1)\,j\pi}{2N} + \cos\frac{(2n+1)\,j\pi}{2N} \qquad (1)$$

Where a (j) = $\sqrt{\frac{1}{M}}$ for m=0

a (j) = $\sqrt{\frac{2}{M}}$ for m=1,2,3…..M-1

a (k) = $\sqrt{\frac{1}{M}}$ for n=0

a (k) = $\sqrt{\frac{2}{M}}$ for n=1,2,3…….N-1

$$f(jk) = \sum_{n=0}^{N-1}\sum_{m=0}^{N-1} a(j)a(k)F(jk)$$

$$\cos\frac{(2m+1)\,j\pi}{2N} + \cos\frac{(2n+1)\,j\pi}{2N} \qquad (2)$$

Where m = 0, 1, 2…….M-1

n = 0, 1, 2…….N-1

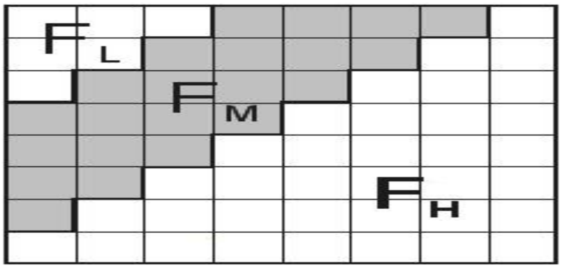

Figure 3 Discrete Cosine Transform regions

B. *Discrete Wavelet Transform*

The wavelet transform has been extensively use in the application of image processing The Figure 4 shows basics of DWT approach for image processing.

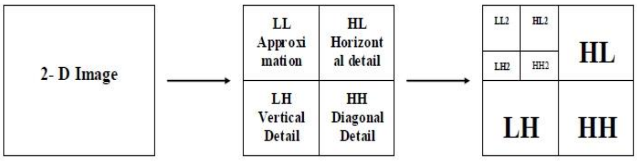

Figure 4 Wavelet Based Transform

To understand the basic idea of the DWT we focus on one dimensional signal. A signal splits into two parts, usually high frequencies and low frequencies. This process is continuing until the signal has been entirely decomposed or stopped before by the application at hand. For compression and watermarking applications, generally no more than four decomposition steps are computing. Furthermore, from the DWT coefficients, the original signal can be reconstructing. The reconstruction process called the inverse DWT (IDWT).

The wavelet transform is given by equation 3.In the wavelet Domain where W_i denotes the coefficient of the transformed image. Xi denotes the bit of the watermark to be embedded. Here α is a scaling factor. And (u, v) represents basic transformed functions

$$I_{Wu,v} = Wi + \alpha\,|Wi|\,Xi \qquad where\ u,v \in LL \qquad (3)$$

V. PROPOSED DCT-DWT COMBINED ALGORITHM

The wavelet transform based watermarking technique divides the two dimensional image into four sidebands - a low resolution approximation of the tile component (LL), the horizontal component (HL), vertical (LH) and diagonal frequency (HH) characteristics. The process can then be repeated iteratively to produce N scale transform. This allows us to use higher energy watermarks in regions that the HVS known to be less sensitive to, such as the high resolution detail bands (LH, HL, and HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark at little to no additional impact on image quality.

Discrete cosine transform achieves good robustness against compression and other signal processing attacks due to the selection of perceptually significant transform domain coefficients

According to properties and advantages of both DCT and DWT, an algorithm can be made to have advantages of both DCT as well as DWT. A proposed block diagram of image watermarking embedding technique using both DCT and DWT and watermark recovery are shown below in Fig. 5 and Fig. 6 respectively.

In watermark embedding procedure, first watermarked image is decomposed through DWT transform and choosing the appropriate frequency band in which watermark is embedded. Then DCT transform is applied for watermarked message for reformatting and reshaping in its original form. The watermarking information is embedding into the selected position. Then make the whole image IDCT and IDWT transformed and get the watermarked image.

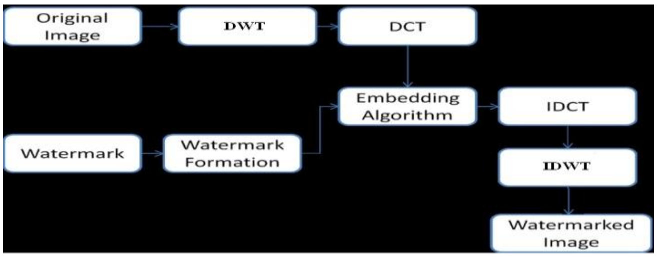

Figure 5 Watermark Embedding using DCT-DWT

In watermark recovery procedure, the host image is decompose through DWT transform and select the appreciate wavelet modulus in the frequency level. The watermarked image will be Discrete Cosine Transformed. Because the DCT modulus contain the low frequency information of watermarking image, as long as these information do not lose or lose little then the watermarking image can be renewed well. This enhances the robustness and concealment.

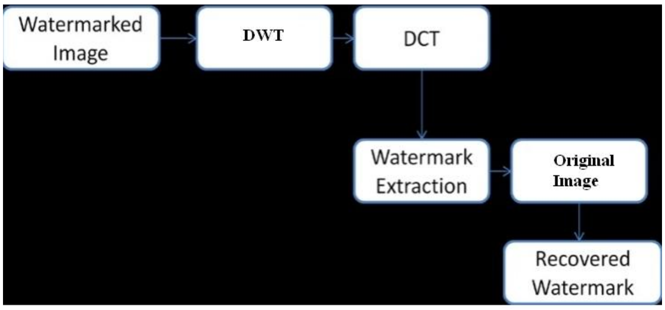

Figure 6 Watermark Recovery

VI. OUR UTILIZATION APPROACH

In most watermarking applications, the watermarked data is likely to be processed in some way before the data reaches to the receiver.

An embedded watermark may unintentionally or inadvertently be impaired by attacks As mentioned above generally there are mainly two types of attacks intentional and un-intentional Attacks. EBCOT (Embedded block coding optimal truncatation) Algorithm helps us to store the information by JPEG compression. Encoding is done by Huffman coding. Similarly decoding is made at receiver side.

Error-correcting codes allow us to receive a piece of information, identify the errors, locate them, and correct them. Hamming codes and cyclic codes are especially useful kind of error-correcting code. The hamming code can only detect the errors but cannot correct it. The cyclic codes can detect and correct the errors.

Here watermarked image transmitted on AWGN (Additive White Gaussian Noise) channel is shown in Figure 7.The quality of received image enhances by performance parameter like bit error rate and signal to noise ratio.

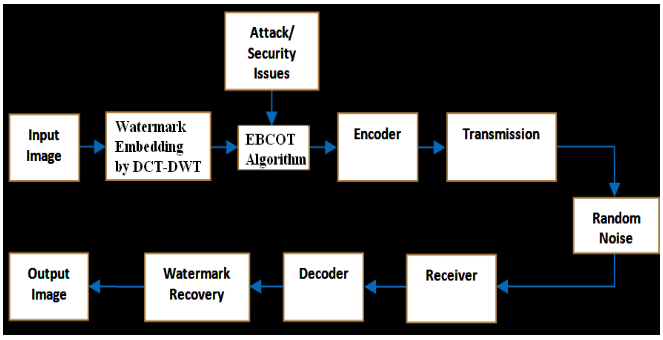

Figure 7 Our System Utilization Approach

VII. EXPERIMENTAL EVALUATION RESULTS

For testing performance of this DCT-DWT proposed algorithm, the experiments result is simulated with the software MATLAB (R2009a). In the following experiments, the gray-level image with size of “Car” (128*128) is used as host image to embed with watermark message “RIGHT OF” (50*20). The original host image, embedded watermark image and extracted watermark image are shown in Fig. 8 (a) and 8 (b) respectively. Then the watermarked image is tested with some typical attacks such as blurring attack, laplacian attack, median filtering, rotation attack, salt pepper noise, and Gaussian white noise with JPEG compression by EBCOT algorithm. Here the watermarked image is tested with blurring, laplacian , median filter ,rotation and salt pepper noise attacks with PSNR and JPEG compression results are shown in Figure 8 (c), 8(d), 8(e), 8(f) and 8(g) respectively. Gaussian noise is generated in AWGN (Additive White Gaussian noise) communication channel.

Information is passes every day in our society. It is essential that interference in the communication channel has been reduced by error correcting codes. The Error correcting codes help us to detect and correct the errors. The results of watermarked image without and with error correcting codes are shown in Figure 8 (h) and Fig.8 (l) respectively.

To determine the degradation of the original image, we use the peak signal to noise ratio (PSNR). PSNR represents the distortion caused by the watermarking. PSNR is defined using the following equation: PSNR=20*log10 (255 / mseval) (Where mseval = mean2 (aa-bb) ^2; aa = original image and bb = received image after AWGN channel communication). The compression ratio is calculated by cr2 = image ratio (c2, f2) (Where c2 = original to JPEG image and f2 = JPEG to original image) Compression ratio in percentage is given by: cr = cr2*100.The execution time in seconds is defined by execution time = (starting time – ending time).The watermarked image after AWGN channel communication is quite close to original image in human perception vision. There is no distinct difference between these two images which can detect with eyes. The graph of bit error rate versus signal to noise ratio of original image and received image after channel communication is shown in Figure 9. This graph shows that DCT-DWT provide more robustness on communication channel against attacks and noise. The comparative analysis of above attacks with “Car” image is shown in Table I.

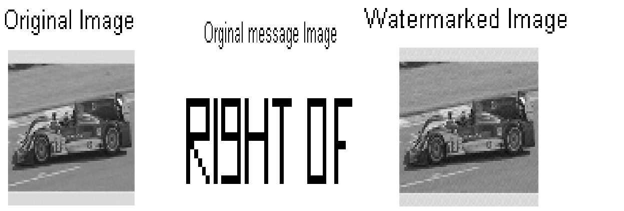

Figure 8(a) Watermarked Embedding by DCT-DWT with PSNR = 23.9841

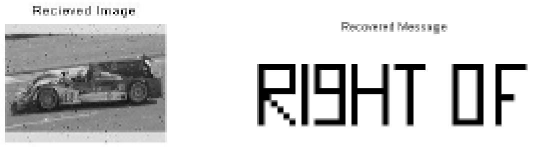

Figure 8(b) Watermark Recovery without attack with PSNR= 20.7656 dB and Compression ratio = 66.6176

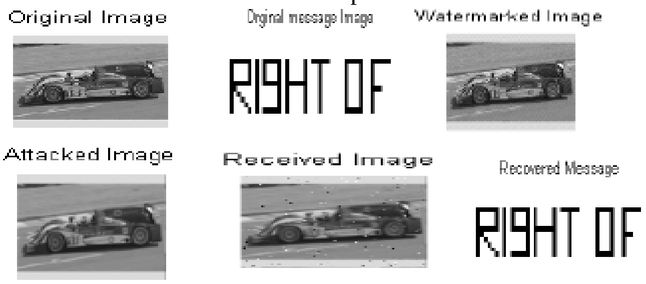

Figure 8(c) Watermarked Image with blurring attack with PSNR = 20.7656 dB and Compression Ratio = 66.6176

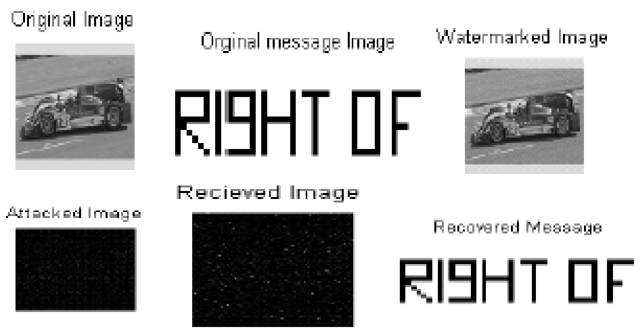

Figure 8(d) Watermarked Image laplacian attack with PSNR = 0.0771 dB and Compression Ratio = 66.6176

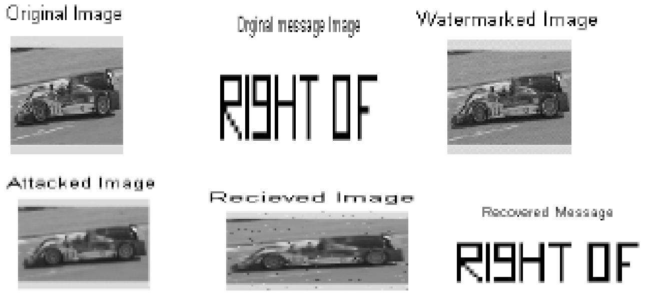

Figure 8(c) Watermarked Image with median attack with PSNR = 21.3140 dB and Compression Ratio = 66.6176

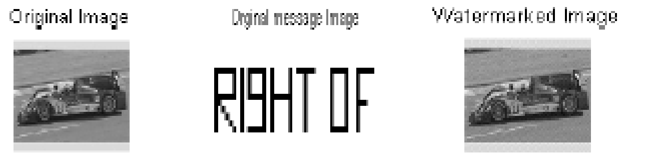

Figure 8(c) Watermarked Image with rotation attack with PSNR = 11.4951 dB and Compression Ratio = 66.6176

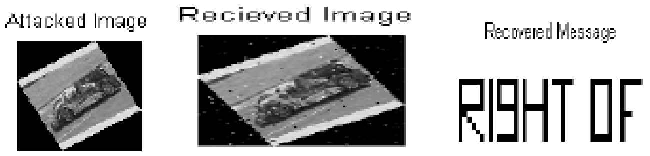

Figure 8(h) Watermark image without Error Correcting code with PSNR = 37.8631 dB and Compression Ratio = 66.6176

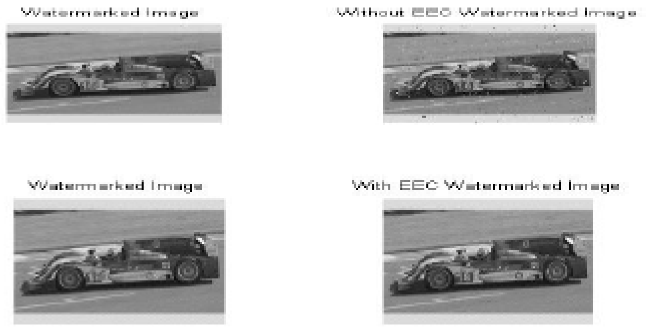

Figure 8(l) Watermarked image with Error Correcting code (Cyclic Code) with PSNR = 62.2016 dB and Compression Ratio = 66.61

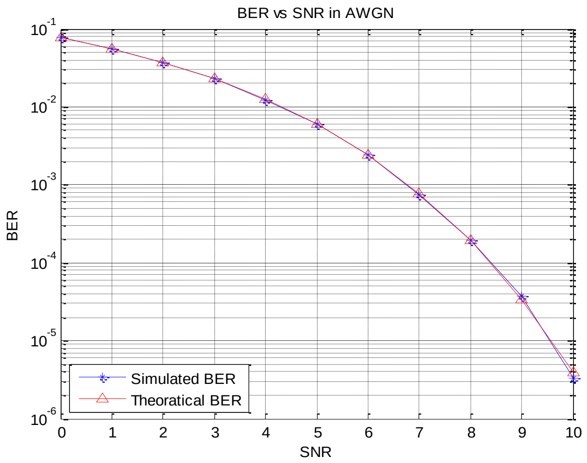

Figure 9 Graph of Bit Error Rate vs. Signal to Noise Ratio using DCT-DWT (original image and received image after channel communication)

Table I
Comparative Analysis of PSNR and Execution Time With Image "Car"

Process/ Attacks	Proposed Algorithm by DCT-DWT (PSNR : dB)	Execution Time (sec.)
Without Attack	23.9841	65.6563
Blurring	20.7656	69.4219
Laplacian	0.0771	66.2344
Median Filter	21.3140	67.4844
Rotation	11.4951	69.4219
Salt Peeper Noise	19.7644	68.0625
Gaussian noise	23.9933	66.6563
Without Error Correcting Code	37.8631	68.2031
With Error Correcting Code	62.2016	68.2031
Without Channel Transmission	23.9841	65.6563

VIII. CONCLUSION

Experiment results shows that recombining the DCT-DWT joint transform algorithm improved the performance of the digital watermarking. From the observation, we can say that proposed algorithm proves its robustness against attacks. EBCOT algorithm helps us store and transmit the digital watermarked image. Error correcting codes like hamming code and cyclic code reduce almost all random noise, errors or Gaussian noise occurs over a communication channel. Overall system designing in this approach tends to reduce noise and gives security to watermarked message image for desired application purposes.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

REFERENCES

1. J. Cox, M. L. Miller, J. A. Bloom, “Digital Watermarking”, Morgan Kaufmann Publishers, 2001.
2. A.M.Kothari, A.C.Suthar, R.S.Gajre. “Performance Analysis of Digital Image Watermarking Technique –Combined DWT–DCT over individual DWT”, Published in International Journal of Advanced Engineering & Applications, Jan. 2010.
3. K. J. Raval & S.Zafar, “Image Communication For Digital Watermarking ’’,Published in International Journal of Engineering and Research,IJESR,2012
4. K. J. Raval & S. Zafar, “Digital Watermarking With Copyright Authentication for Image Communication’’, International Conference On Signal and Image Processing, ISSP-2013.
5. K. J. Raval & S. Zafar, “Implementation of Digital Watermarking by Combined Transform Domain Algorithm for Error Correcting Codes’’, Published in International Journal for Research, Paripex, 2012.
6. S. AI Zahir & W .Islam, ‘‘A New Wavelet Based Image Watermarking Techniques’’, International Conference Consumer Electronics, IEEE, 2010.
7. Feng Liu & Yongtao Qian , “A Novel Robust Watermarking Based on Levels DCT and Two levels SVD”, International Conference On Measuring Technology & Mechatronics, IEEE, 2011.