Unified Approach to Secure and Robust Digital Watermarking Scheme for Image Communication

Keta Raval, Rajni Bhoomarker

Abstract: ***Digital Watermarking has become essential and prime need for multimedia industry, internet users and digital data authentication fields. With rapid growth of digital data, we have problems related to security and copyright authentication .These increased use of digital data creates new challenges for document owners and their reliable customers. Digital Watermarking has provided global and cost effective solution for digital image communication. In this paper a robust digital watermarking algorithm based on Joint DWT-DCT Transformation is proposed. A secrete message is scrambled and embedded in DWT-DCT coefficients of host image. Uncompressed digital watermark images need a lot storage capacity and bandwidth. For efficient image transmission needs image compression. Then watermarked data is used for desired application by channel communication.***

Index Terms: Digital Watermarking, Discrete Cosine Transform, Discrete Wavelet Transform

I. INTRODUCTION

Digital Communication has increasing now days. Digital watermarking is an embedding technique, which inserts the hidden information into multimedia data. The hidden information may be in text, image, audio or video form. These watermarked images transmitted over a channel, noise could interrupt. The watermarked image may be corrupted. The watermark detection process has to be robust from both unintentional and intentional distortions. These distortions called attacks [2].

The aim of attacks is not always to remove or destroy the watermark. These distortions could introduce degradation of the system. Solution is providing by Digital Watermarking based on DCT-DWT. This evolution of DCT-DWT 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 digital images, audio, text and video from piracy a matter of urgency. Piracy attacks include illegal access to transmitted data networks, data content modification, production and retransmission of illegitimate copies. The impact of such type attacks might be very large, booth in financial and security terms [2].

The watermarked images transmitted over a channel via communication media like Entertaining Broadcasting World. On communication channel watermarked may be corrupted by noise. A proper encoding and decoding techniques should remove random noise occur over a communication channel. By Error Correcting codes help to remove noise in communication. 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 attacks are divided into mainly two types intentional and unintentional. The embedded watermark unintentionally impaired by such processing like compression and signal enhancement etc. The intentional watermark applied with explicit goal of hindering watermark. The mean square error (MSE) and peak signal to noise ratio (PSNR) are the most popular metric to measure fidelity [4].

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.

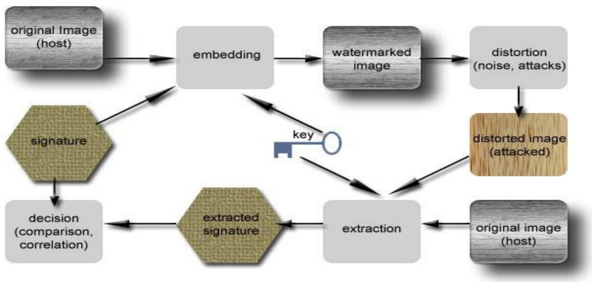

Figure 1 Typical Watermarking block diagram

Revised Manuscript Received on 30 March 2013.
* Correspondence Author
Keta Raval*, Dept. of Electronics and Communication, Patel Institute of Engineering and Science, RGPV, Bhopal, M.P., India.
Rajni Bhoomarker, Dept. of Electronics and Communication Patel College of Science and Technology, RGPV, Bhopal, M.P., India.

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.

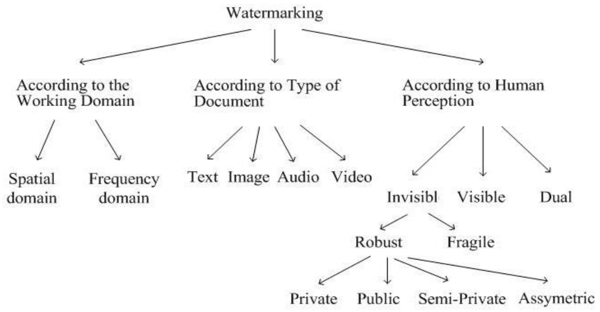

Figure 2 Types of watermarking methods

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. 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.

$$F(jk) = a(j)a(k)\sum_{n=0}^{N-1}\sum_{m=0}^{N-1} f(mn) \cos\frac{(2m+1)j\pi}{2N} + \cos\frac{(2n+1)j\pi}{2N} \quad (1)$$

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

$$f(jk) = \sum_{n=0}^{N-1}\sum_{m=0}^{N-1} a(j)a(k)F(jk) \cos\frac{(2m+1)j\pi}{2N} + \cos\frac{(2n+1)j\pi}{2N} \quad (2)$$

Where m = 0, 1, 2…….M-1

n = 0, 1, 2…….N-1

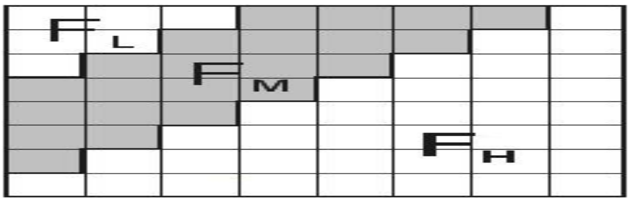

Figure 3 Discrete Cosine Transform regions

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.

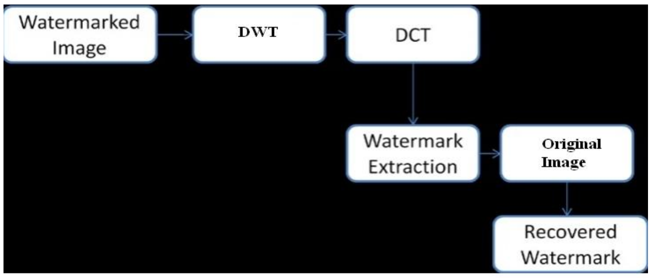

Figure 4 Wavelet Based Transform

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.

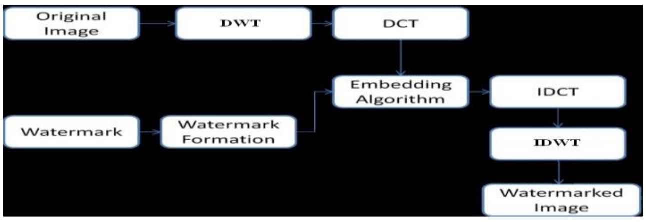

Figure 5 Watermark Embedding using DCT-DWT

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.

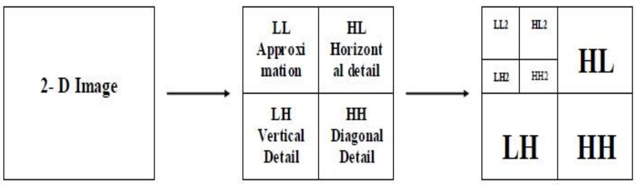

Figure 6 Watermark Recovery

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.

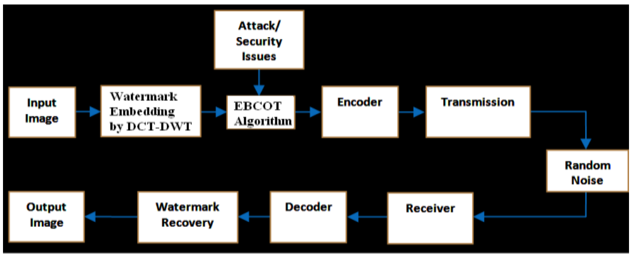

Figure 7 Our System Utilization Approach

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 "Apple" (256*256) is used as host image to embed with watermark message "copyright". 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 rotation attack, laplacian attack blurring attack, salt pepper noise, median filtering and Gaussian white noise with JPEG compression by EBCOT algorithm. Here the watermarked image is tested with rotation, laplacian, blurring, salt pepper noise and median filter 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).

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

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.T
he 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 "Apple" image is shown in Table I.

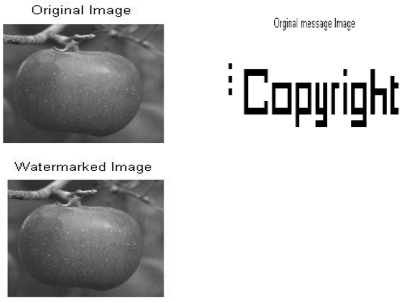

Figure 8(a) Watermarked Embedding by DCT-DWT

Figure 8(b) Watermark Recovery without attack with PSNR = 23.6388 dB and Compression ratio = 62.0949%

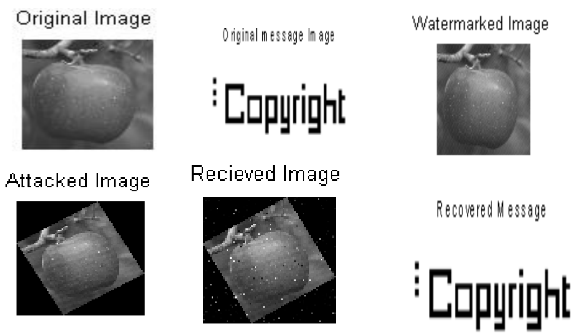

Figure 8(c) Watermarked Image with rotation attack with PSNR = 17.4346 dB and Compression Ratio = 62.0949%

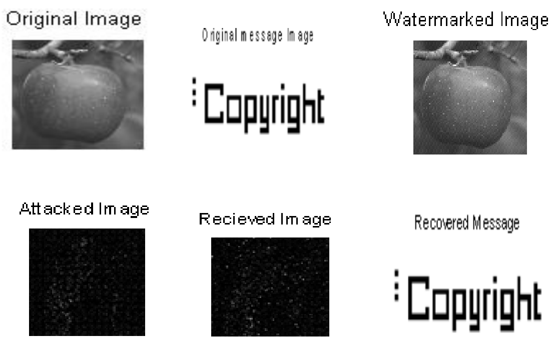

Figure 8(d) Watermarked Image laplacian attack with PSNR = 0.0014 4 dB and Compression Ratio = = 62.0949%

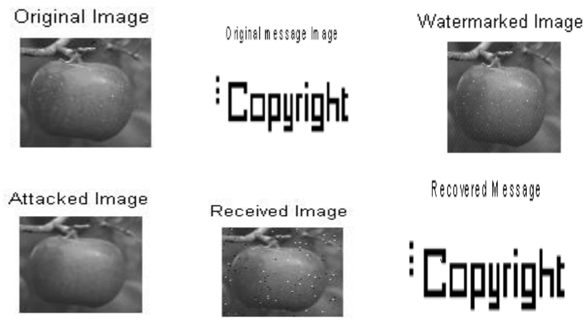

Figure 8 (e) Watermarked Image with blurring attack with PSNR = 30.8930 and Compression Ratio = = 62.0949%

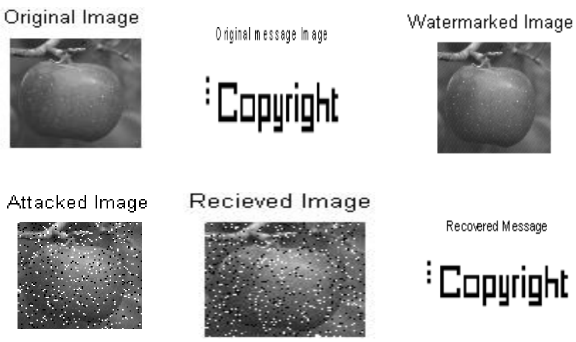

Figure 8 (f) Watermarked Image with salt and pepper noise with PSNRR = 20.8434 and Compression Ratio = = 62.0949%

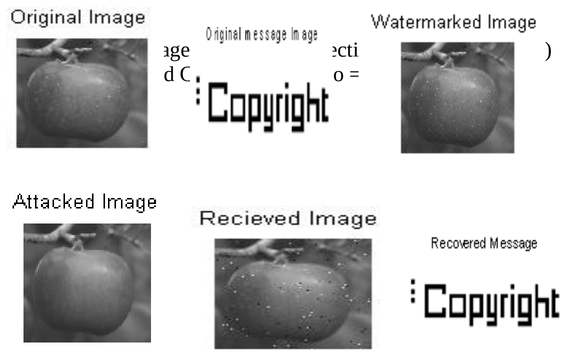

Figure 8 (g) Watermarked Image with median filter with PSNR = 34.2105 and Compression Ratio = = 62.0949%

Figure 8(h) Watermark image without Error Correcting code with PSNR = 37.0814 dB and Compression Ratio = = 62.0949%

Figure 8(l) Watermarked image with Error Correcting code (Cyclic Code) with PSNR = 54.1896 dB and Compression Ratio = = 62.0949%

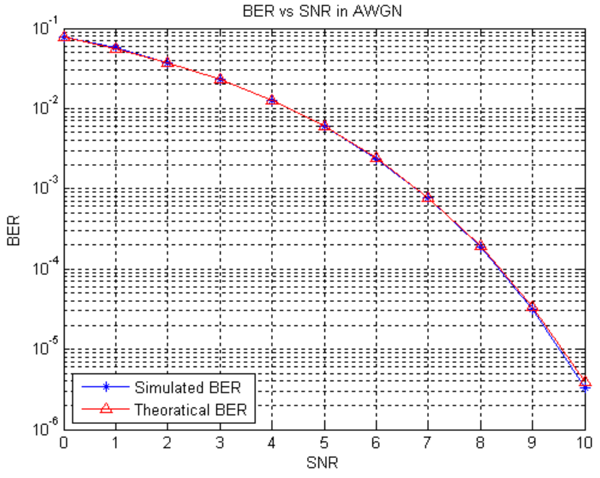

Figure 9 Graph of Bit Error Rate vs. Signal to Noise Ratio using DCT-DWT (original image and received image after channel communication).

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

Process/ Attacks	Proposed Algorithm by DCT-DWT (PSNR : dB)	Execution Time (sec.)
Without Attack	23.6388	68.3125
Rotation	17.4346	69.5938
Laplacian	0.0014	68.3594
Blurring	30.8930	68.3750
Salt Peeper Noise	20.8434	68.5313
Median Filter	34.2105	68.3594
Gaussian noise	23.6388	68.3125
Without Error Correcting Code	37.0814	68.5156
With Error Correcting Code	54.1896	68.5156

VIII. CONCLUSION

Experiment results shows that recombining the DCT-DWT joint transform algorithm improved the performance of the watermarking. From the observation, we can say that proposed algorithm proves its robustness against attacks. EBCOT algorithm helps us store and transmit the watermarked image. Error correcting codes like hamming code and cyclic code reduce almost all random noise or Gaussian noise occur 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.

REFERENCES

1. I. 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 & Research,IJESR,2012
4. Suthar A.C., Patel C.B. and Kulkarni G.R., "Implementation Of Image Security Issues Using Mixed Frequency Domain Scheme" in International Transactions on Electrical, Electronics and Communication Engineering,2011.
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 Technique" International Conference on Consumer Electronics, IEEE, 2011.
7. K. J. Raval & S. Zafar, "Digital Watermarking With Copyright Authentication for Image Communication'', International Conference on Signal and Image Processing, ISSP-2013.

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