A New Approach for Copyright Authentication for Image Communication

Ms. Poornamma
Dept,of ECE
Mangalore Instution Of Technology & Engineering
Moodbidri,Mangalore,India

Mr. Ajay Pinto
Asst prof. Dept of E&C
Mangalore Instution Of Technology&Engineering
Moodbidri,Mangalore,India

Abstract—**The expansion of digital multimedia communication the uses of data such as image audio and video has been increased. In this type communication there are some security issues. For secure communication digital watermarking has been adapted. In other watermarking algorithms first the host image to be transformed after that embedding the watermark takes place. Digital images which are uncompressed take lot of storage and bandwidth for transmission, so it requires compression for transmission. These methods are complex. Here we are proposing a digital watermarking by transform based DCT-DWT algorithm .**

Keywords: ***Digital Watermarking Discrete Cosine Transform, Discrete Wavelet Transform, Communication Channel***

I. INTRODUCTION

Since, Computer and Internet make the world become digitization because the security issues arise for the secure communication. Digital watermarking is a technique to embed the data for communication. After embedding the watermark the specific algorithm is applied. Here we applied proposed transform based on DCT-DWT watermarking technique. Once the watermark being inserted into original image; the quality of original image would be changed. The watermark may be in text, image, audio or video form. This watermark inserted image to be transmitted over any communication channel. The noise of the channel can affect the watermarked image, so the watermark extraction process has to be robust for all type of attacks [2]. Attack doesn't mean to destroy the watermark but system performance can be degraded because of attacks. To enhance the system performance we proposed DCT-DWT based watermarking.

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.

The technology of digital communication is growing very fast so the technology should be reliable and robust for protecting the data in digital communication like digital images, audio, text and video from piracy. If the illegal data is transmitted over a network, content modification, production of illegal copies of data and retransmission of illegal copies of data is piracy which effects in terms of financial and security issues.[2] In the transmission of watermarked image over a communication channel the watermarked image may be corrupted or degraded because of channel noise.

So to remove noise the encoding and decoding algorithm should be selected properly. To survive the different type of attacks including signal processing operation robust image watermarks are designed. For the evaluation of robust watermark, the evaluation of attacks on an image is required. The attacks are divided into mainly two types intentional and unintentional. Unintentional attacks are used by such processing like compression and signal enhancement etc. The intentional watermark are used for hindering watermark. The measurement of image quality is done by mean square error(MSE) and peak signal to noise ratio(PSNR)[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.

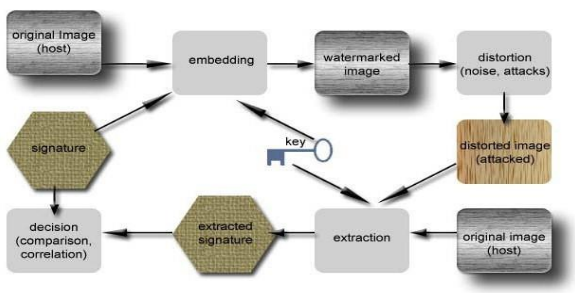

Fig.1. Typical Watermarking block diagram

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.

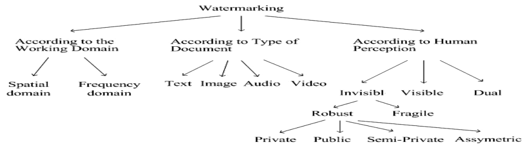

Fig. 2. Types of watermarking methods

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. 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.

A. *Discrete Cosine Transformation (DCT)*

The Discrete cosine transform (DCT) is most popular due to several reasons. One of the reasons is that most of the compression techniques developed in the DCT domain (JPEG, MPEG, MPEG1, and MPEG2) & therefore image processing is more familiar with it. DCT is one of the most common linear transformations in digital signal process technology. Two-dimensional discrete cosine transform (2D-DCT) is defined as

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

The corresponding inverse transformation (Whether 2DIDCT) is defined as

$$F(nm)=\sum_{M=0}^{N-1}\sum_{N=0}^{N-1} a(j)a(k)F(jk)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right] \quad (2)$$

The 2D-DCT can not only concentrate the main information of original image into the smallest low frequency coefficient, but also it can cause the image blocking effect being the smallest, which can realize the good compromise between the information centralizing and the computing complication.

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 an image. In order to invisibly embed the watermark that can survive lossy data compressions, a reasonable tradeoff is to embed the watermark into the middle-frequency range of the image.

The middle frequency bands are chosen such that they have minimized that they avoid the most visual important parts of the image (low frequency) without over-exposing themselves to removal through compression and noise attacks. DCT domain watermarking can survive against the attacks such as noising, compression, sharpening, and filtering.

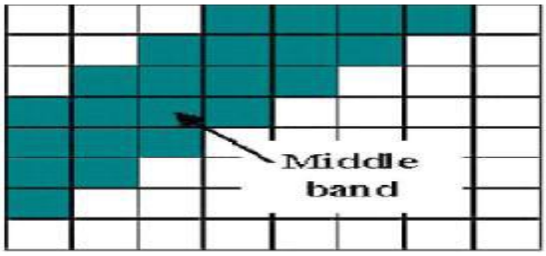

Fig. 3. Middle Band Frequencies In 8x8 DCT Block

B. *Discrete Wavelet Transform*

The DWT decomposition input image into four level components namely LL, LH, HL, and HH where the first letter corresponds to applying either low pass frequency operation or High pass frequency operation to the rows, and second letter refer to the filter applied to the columns which is shown in figure 4. The lowest resolution level LL consists of the approximation part of the original image. The remaining three resolution level consist of the detail parts and give the vertical high (LH) and horizontal high (HL) and high (HH) frequencies. In the proposed algorithm, watermark is embedded into host image by modifying the coefficients of high frequency bands i.e. HH subband.

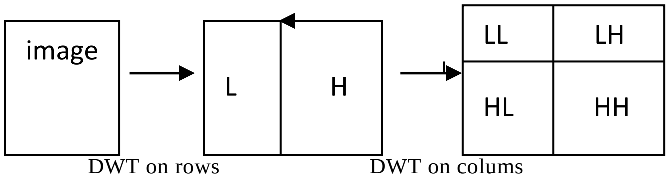

Fig.4. DWT decomposition of image.

The reconstruction process called the inverse DWT (IDWT). The wavelet transform is given by equation 3.In the wavelet

Domain where Wi denotes the coefficient of the transformed image. Xi denotes the bit of the watermark to be embedded. Here is a scaling factor. And (u, v) represents basic transformed functions

Iwu,v=Wi+a$|Wi|Xi$ where u,v $\in HL, LH$ (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.

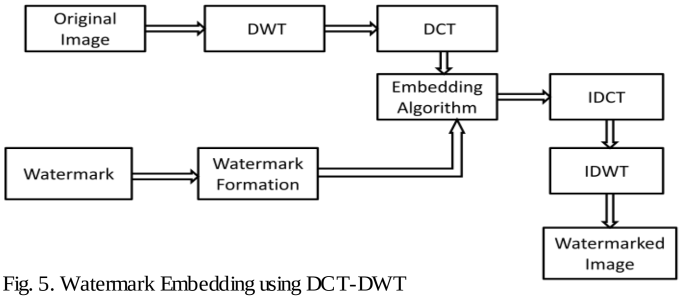

Fig. 5. Watermark Embedding using DCT-DWT

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.

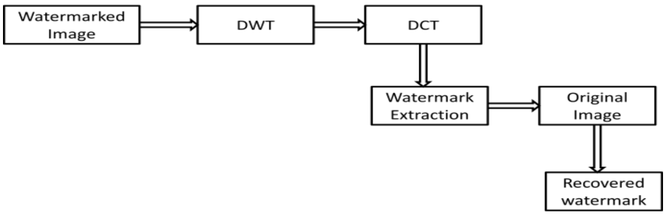

Fig. 6. Watermark Recovery

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.

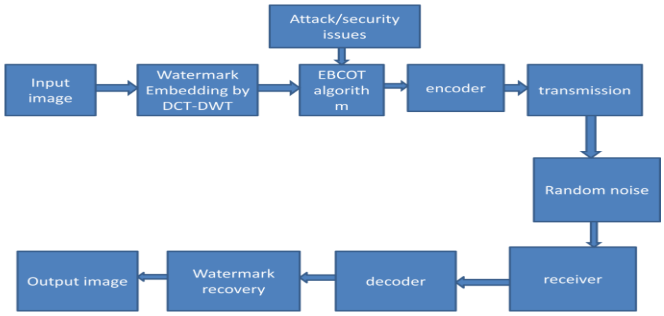

Fig.7. Our System Utilization Approach

I.. EXPERIMENTAL EVALUATION RESULTS

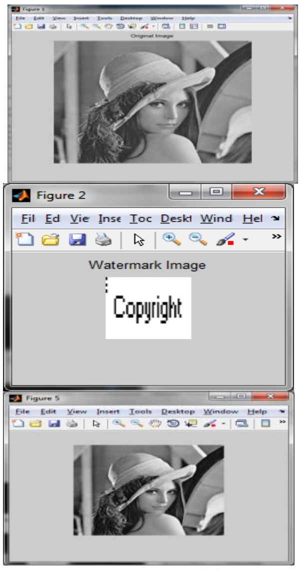

Fig. 8(a). Watermarked Embedding by DCT-DWT

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 "Lena" (512*512) is used as host image to embed with watermark message "copyright" (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 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 media filter attacks with PSNR and JPEG compression results are shown in Figure 8(d), 8(e), 8(f) 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 (g). 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-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 "Lena" image is shown in Table I.

Fig. 8(b). Watermark Recovery without attack with PSNR= 24.9179 dB and Compression ratio=71.1594%

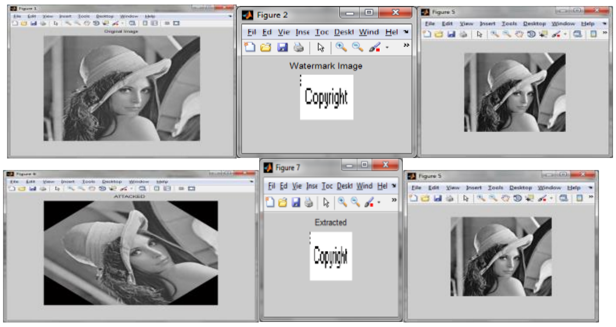

Fig: 8(c). Watermark image with rotational attack with PSNR= 24.9179 dB and Compression ratio=71.1594

Fig. 8(d). Watermarked Image with median filter with PSNR = 21.0429 and Compression Ratio = 71.1594%

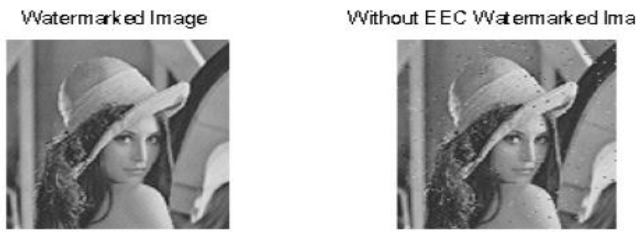

Fig .8(e). Watermark image without Error Correcting code with PSNR = 37.1826 dB and Compression Ratio = 71.1594 %

bb) ^2; aa = original image and bb=received image

Fig. 8(f). Watermarked Image with blurring attack with PSNR = 20.1630 and Compression Ratio = 71.15%

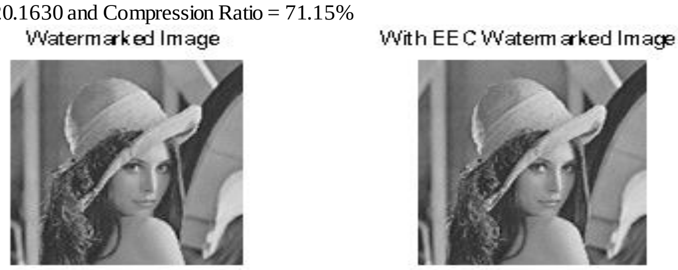

Fig. 8(g). Watermarked image with Error Correcting code (Cyclic Code) with PSNR = 58.5615 dB and Compression Ratio = 71.1594%

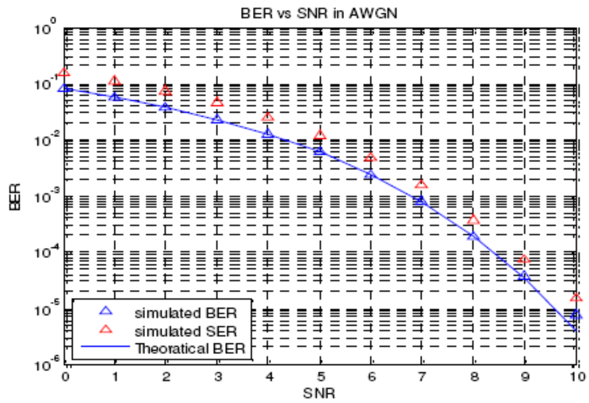

Fig. 9. Graph of Bit Error Rate vs. Signal to Noise Ratio using DCT-DWT (original image and received image after channel communication).

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

REFERENCES

[1] K. J. Raval & S.Zafar, "Digital Watermarking with Copyright Authentication for Image Communication'' 2013 International Conference on Intelligent Systems and Signal Processing (ISSP)

[2] I. J. Cox, M. L. Miller, J. A. Bloom, "Digital Watermarking", Morgan Kaufmann Publishers, 2001.

[3] 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.

[4] K. J. Raval & S.Zafar, "Image Communication For Digital Watermarking '',Published in International Journal of Engineering & Research,IJESR,2012

[5] 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.

[6] 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.

[7] S. AI Zahir & W.Islam ,"A New Wavelet Based Image Watermarking Technique" International Conference on Consumer Electronics, IEEE, 2011

[8] Feng Liu & Yongtao Qian , "A Novel Robust Watermarking Based On Levels DCT and Two Levels SVD", International Conference On Measuring Technology & Mechatronics Automation, IEEE, 2011