ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

Digital Watermarking: Data Hiding Techniques using DCT-DWT Algorithm

Kunal D Megha[1], Nimesh P Vaidya[2], Asst. Prof Ketan Patel[3]

Student of C.S.E. Dept, Govt. Engineering College, Sector-28, Gandhinagar, Gujarat, India[1]

Student of M. Tech, Computer Science Dept. Mewar University, Chittorgarh, Rajasthan, India[2]

Grow More Faculty of Engineering, Udaipur-Himmatnagar Highway, Himmatnagar, Gujarat, India[3]

Abstract: Digital watermarking is the technique used by researchers to conceal user-defined information along with important information that may be visible or invisible depending on user requirements. Now the digital watermark refers to the proprietary information. The absence of digital watermarks in the results of information lost revenue. The full digital watermark information to be inseparable. In this work we present here the topography of the digital watermark

Keywords: Watermarking, Spatial Domain technology, Discrete Cosine transform (DCT), Discrete Wave late transform (DWT) and Frequency Domain technology

I. INTRODUCTION

Digital watermarking is to insert a watermark message hidden in a hot object such that the hidden message is inseparable. Earlier watermark is applied only in the text [1]. Today watermark applies to all media types. Digital watermarking is applied to video as well to stop piracy resulting in lost revenue. There should be no perceptible difference between the watermarked signal and the original and the watermark should be difficult to remove without damaging or altering the host object. The technology of digital watermark is an emerging field in computer science, cryptography, signal processing and communications [2].

II. GENERAL FRAMEWORK OF DIGITAL WATERMARKING

Watermarking is the process that incorporates data called a watermark or digital signature or tag or label into a multimedia object; watermark can be detected or extracted later to make an assertion about the object [3]. The object may be an image or audio or video. A simple example of a digital watermark would be a "seal" placed over an image visible to identify copyright. However the watermark might contain additional information including the identity of the purchaser of a particular copy of the material.

In general, any watermarking scheme (algorithm) consists of three parts [4].

- The watermark.
- The encoder (insertion algorithm).
- The decoder and comparator (verification or extraction or detection algorithm).

Each owner has a unique watermark or an owner can also put different watermarks in different objects the marking algorithm incorporates the watermark into the object. The verification algorithm authenticates the object determining both the owner and the integrity of the object.

A. *Encoding Process [4]*

Let us denote an image by *I'*, a signature by S = S1, S2, and watermarked image by I'. E is an encoder function, it takes an image I and a Signature S, and it generates a new image which is called watermarked image I. Mathematically,

$$E(I, S) = I' \quad (1)$$

It should be noted that the signature S may be dependent on image I. In such cases, the encoding process described by Eqn. 1 still holds. Following figure illustrates the encoding process.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

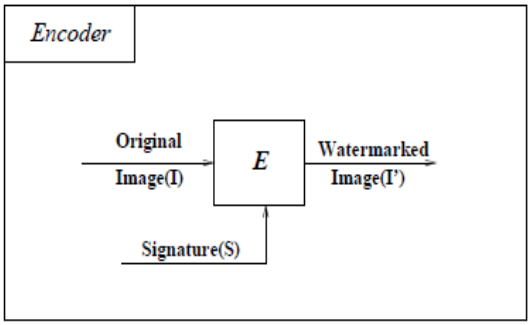

Figure-1: Encoder

B. *Decoding Process[4]*

A decoder function D takes an image J (J can be a watermarked or un-watermarked image, and possibly corrupted) whose ownership is to be determined and recovers a signature S' from the image. In this process an additional image I can also be included which is often the original and un-watermarked version of J. This is due to the fact that some encoding schemes may make use of the original images in the watermarking process to provide extra robustness against intentional and unintentional corruption of pixels

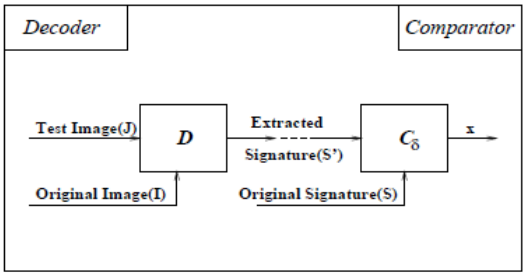

Figure-2: Decoder Process

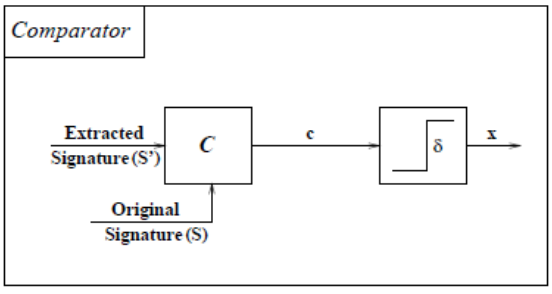

Figure-3: Comparator

A watermark must be detectable or extractable to be useful. Depending on the way the watermark is inserted and depending on the nature of the watermarking algorithm, the method used can involve very distinct approaches. In some watermarking schemes, a watermark can be extracted in its exact form, a procedure we call watermark extraction. In other cases, we can detect only whether a specific given watermarking signal is present in an image, a procedure we call watermark detection. It should be noted that watermark extraction can prove ownership whereas watermark detection can only verify ownership.

III. ATTACKS ON WATERMARKS

A watermarked image is likely to be subjected to certain manipulations, some intentional such as compression and transmission noise and some intentional such as cropping, filtering, etc. They are summarized in Fig.4.

A. *Lossy Compression*

Many compression schemes like JPEG and MPEG can potentially degrade the data's quality through irretrievable loss of data [5].

B. *Geometric Distortions*

Geometric distortions are specific to images videos and include such operations as rotation, translation, scaling and cropping [6].

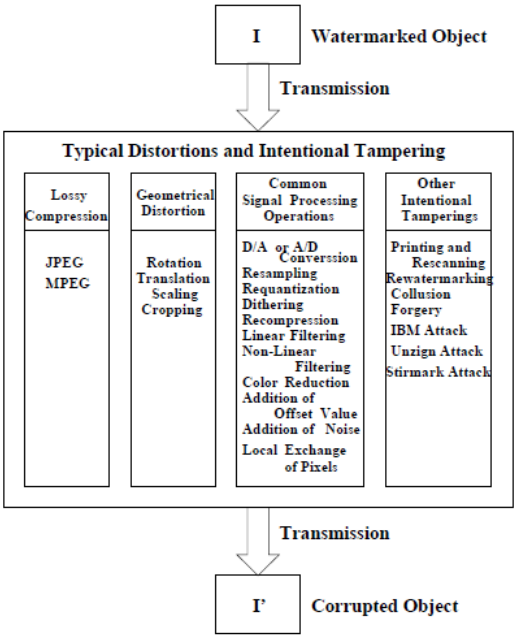

Figure-4: Attacks on Watermarks

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

C. Common Signal Processing Operations

They include the followings:

1. D/A conversion
2. A/D conversion
3. Re sampling
4. Re quantization
5. Dithering distortion
6. Recompression
7. Linear filtering such as high pass and low pass filtering
8. Non-linear filtering such as median filtering
9. Color reduction
10. Addition of a constant offset to the pixel values
11. Addition of Gaussian and Non Gaussian noise
12. Local exchange of pixels

D. Other Intentional Attacks

1. Printing and Rescanning

2. Watermarking of watermarked image (re watermarking) [7, 8, 9]

3. Collusion: A number of authorized recipients of the image should not be able to come together (collude) and like the differently watermarked copies to generate an un-watermarked copy of the image (by averaging all the watermarked images).

4. Forgery: A number of authorized recipients of the image should not be able to collude to form a copy of watermarked image with the valid embedded watermark of a person not in the group with an intention of framing a 3rd party.

5. IBM attack [10, 11, and 12]: It should not be possible to produce a fake original that also performs as well as the original and also results in the extraction of the watermark as claimed by the holder of the fake original.

6. The Unsigned and Stir mark have shown remarkable success in removing data embedded by commercially available programs.

IV. IMPLEMENTATION

A. Watermarking Insertion Steps

Step 1: Take input image.

Step2: Convert RGB image to YIQ image model

Step 3*:* Apply DWT on I- Component. Apply 1 levels DWT. Generate DWT coefficient

Step 4: Take watermark image which you want to hide and which is grayscale

Step5: Apply DCT on watermark image

Step 6: Insert DCT coefficient into DWT coefficient, and generate Watermarked image coefficient.

Step 7: Apply inverse DWT

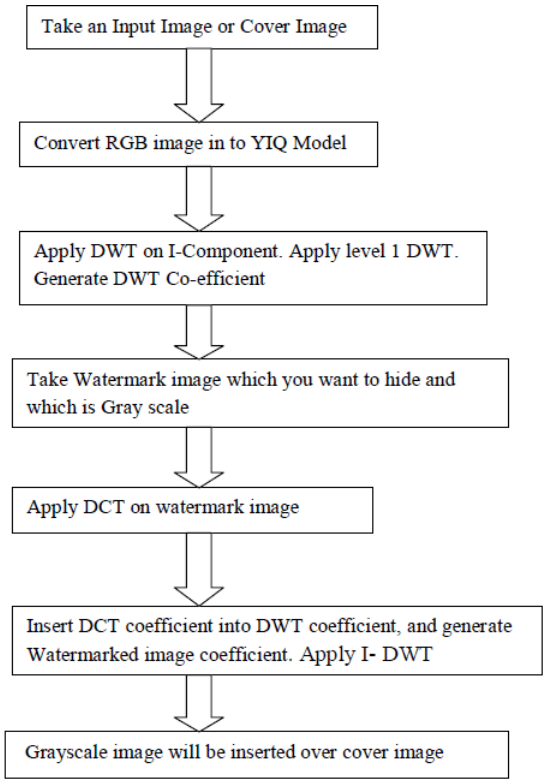

Figure-5: Insertion Method

B. Watermarking Extraction Steps

Step 1: Take an image which you want to extract

Step2: Convert RGB image to YIQ image model

Step 3: Apply DWT on I-Component. Apply Level 1 DWT. Generate DWT Co-efficient

Step 4: Take the Difference of Both the image

Step 5: Apply I-DWT on difference of both the image

Step 6: Get Watermark image

In Extraction Method, here we have to take an image, which we have to extract. After insert your original image into cover image then we have to apply inverse method for

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

extracting the original image. As above steps, we apply that method for extracting the image.

We also then measure the quality of extracted image and robustness of the image by measuring PSNR and NC value.

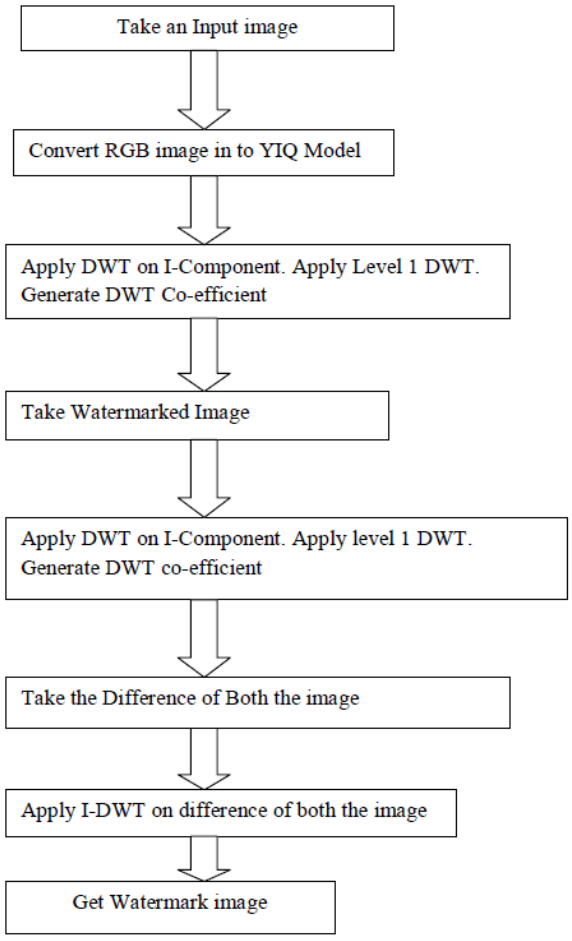

Figure-6: Extraction Method

After performing these techniques, we will get original image and measure the PSNR and NC value and check the robustness of the extracted image and the robust embedded watermark in data that has the ability of surviving after a variety of processing operation and attacks. Then, the watermark must be robust for general signal processing operation, geometric transformation and malicious attack. The watermark for copyright protection does need strongest robustness and can resist malicious attacks, while fragile watermarking; annotation watermarking do not need resist malicious attacks.

The Peak signal-to-noise ratio (PSNR) is most commonly employed to check quality of image. Typically, PSNR values which lies between 80 to 90 represents good quality of image. In which higher PSNR value is better. The Correlation Coefficient of two identical size images tells how much similar two images. NC (Normalized Coefficient) is used to evaluate the robustness of the watermarking image.

Watermark should be able to provide full and reliable evidence for the ownership of copyright-protected information products. It can be used to determine whether the object is to be protected and monitor the spread of the data being protected, identify the authenticity, and control illegal copying.

We also applying some attacks like image adding white noise, Gaussian low pass filter and measure the PSNR and NC value and check the result, which will show the our proposed techniques is how much robust.

V. RESULT OF OUR WORK

This scheme is implemented in Mat lab. Results are tested, analyzed for all channels in RGB and YIQ color spaces. Here, two performance parameters are applied to measure the performance of watermarking scheme: 'Perceptual Transparency' and 'Robustness'.'Perceptual Transparency' is measured in terms of 'Peak Signal to Noise Ratio'. Bigger is PSNR, better is quality of image. PSNR for image with size M x N is given by:

$$PSNR(db) = 10log_{10}\frac{(Max_I)^2}{\frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j)-f'(i,j)]^2}$$

Where, f (i, j) is pixel of original image. f'(i, j) is pixel values of watermarked image. Maxis the maximum pixel value of image. Robustness is measured in terms of Normalized Correlation (NC).The correlation factor (Normalized Correlation) measures the similarity and difference between original 'watermark and extracted watermark. Its values are ideally 1, but the value more than 0.75 is highly accepted. Normalized Correlation (NC) is given by:

$$NC = \frac{\sum_{i=1}^{N} w_i w_i'}{\sqrt{\sum_{i=1}^{N} w_i}\sqrt{\sum_{i=1}^{N} w_i'}}$$

Where, N is number of pixels in watermark, wi is original watermark, wi' is extracted watermark. The standard color

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

Lena image of 512X512 sizes and grey scale watermark of 64x64 is used for testing. The flexing factor is varied for 10 different values.

Cover Image	PSNR(dB) After Bit Insertion	NC After Bit Insertion
Football.jpg	92.72	1.0000
Fabric.png	92.59	0.9999
Autumn.jpg	92.76	1.0000

Table-1: Experimental Result

Now we will apply some attacks and then measure the PSNR and NC values and also check the robustness of our work's techniques.

We are adding white Noise to our watermarked image and then extract the original image. Then we measure the PSNR and NC value of our image, which we are comparing with the existing system's result.

We also apply Gaussian low pass filter and check the robustness and image quality of our proposed techniques.

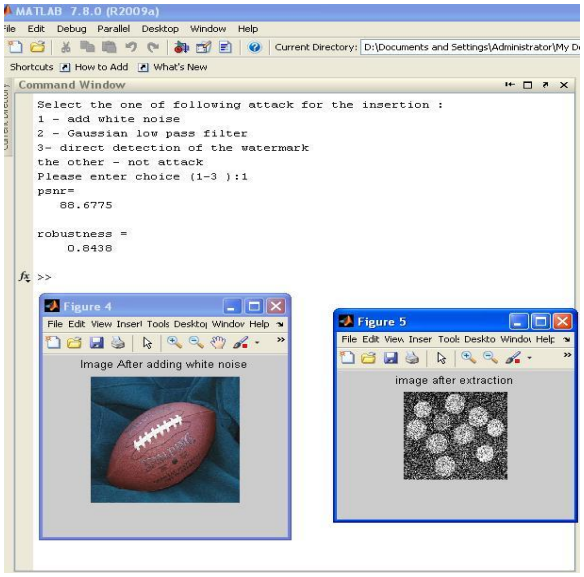

Figure-7: Image after adding White Noise with result

Now we will apply Gaussian low pass filter attack and measure the PSNR value and NC value. In our system we will have to select the one of the choice which we will have to apply attack. If we will have to apply white noise then select choice 1 and if we will have to apply Gaussian low pass filter then select the choice no 2 and if we will have to detect watermark then select the choice no 3 and check the result.

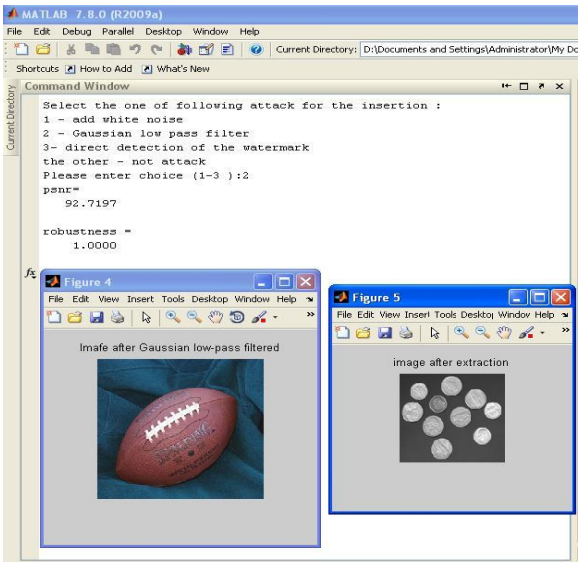

Figure-8: Image after applying Gaussian low pass filter with result

Similarly for fabric and autumn cover image, we will apply attacks and measures the PSNR and NC values of our techniques.

Cover Image	PSNR (db) with White Noise	NC with White Noise	PSNR(db)with Gaussian Low Pass filter	NC with Gaussian Low pass Filter
Football.jpg	88.6775	0.8438	92.7197	1.0000
Fabric.png	89.8472	0.8952	91.9445	0.9999
Autumn.jpg	89.5526	0.9000	92.567	1.0000

Table-2: Experimental Result after applying attack.

VI. CONCLUSION

After implementing my proposed work I am getting PSNR value of extracted watermark image is nearly between 88 to 92 and NC is 1.0000 which is good image quality and shows robust techniques.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

Also, we get the robust watermarked image with high quality. It is more robust then the Spatial technique. It provides better result in case of copyright protection and Ownership identification. In this technique a strongly robust and multilayer security based color image watermarking algorithm in DWT-DCT domain is presented. Since pixel values are highly correlated in RGB color spaces, the use of YIQ color space for watermark embedding is beneficial for improvement in results.

The technique is robust for different attacks like scaling, Gaussian low-pass filtered, rotation etc. This algorithm provides multilayer security by using.DWT domain, DCT domain, and color space conversions. Future Scope of our proposed techniques will be tried to make robust watermarking technique and extract watermarked image with high quality and more secure.

REFERENCES

[1] Sarabjeet Singh, *"Digital Watermarking Trends" International Journal of Research in Computer science*
[2] I. J. Cox, M. L. Miller and J. A. Bloom, *"Digital Watermarking"*, Morgan Kaufman Publishers, 2002.
[3] P. Siva, *"Effectiveness of Still Image Digital Watermarking Algorithms"*, University of Waterloo: Work Term Report, 2002.
[4] Saraju P. Mohnty, *"Digital Watermarking: A tutorial review"*, Dept of Computer Science and Engineering, University of South Florida.
[5] P. Siva, *"Effectiveness of Still Image Digital Watermarking Algorithms"*, University of Waterloo: Work Term Report, 2002.
[6] Lin Liu, *"A Survey of Digital Watermarking technologies"*
[7] Mei Jiansheng and Li Sukang, *"A Digital Watermarking Algorithm based on DCT and DWT"*, International Symposium on Web Information System and Application ISBN 978-952.
[8] GhoutiL, BouridaneA and Ibrahim MK, *"Digital image watermarking using balanced multi wavelets"* , IEEE Transactions on Signal Processing, 54(4), pp. 1519-1536, 2006.
[9] Reddy AA, Chatterji BN, *"A new wavelet based logo watermarking scheme"*, Conf. Pattern Recognition letters, 26(7), pp. 1019-1027, 2005.
[10] S.Craver,*"Can Invisible Watermarks Resolve Rightful Ownership?"* IBM Research Report, RC205209, July25 1996.
[11] S. Craver,*"Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications"*, IEEE Journal, On Selected Areas in Communications, Vol.16, No.4, May 1998, pp.573-586
[12] Kunal Megha, S. M. Shah,*"Study on Digital Watermarking"* International Journal of Engineering Research and Technology, Vol 1, Nov 2012
[12] http://www.digital-watermark.com
[13] http://www.digimarc.com
[14] http://www.altern.org/watermark
[15] http://www.cl.cam.ac.uk/µ fapp2/watermarking
[16] http://nif.www.media.mit.edu/DataHiding
[17] http://www.intertrust.com