

# A Blind digital Watermarking Algorithm based on DWT-DCT Transformation

Sukanti B. Mardolkar<sup>1</sup>, Nayana Shenvi<sup>2</sup>

PG Scholar, Department of ETC Engineering, GEC, Farmagudi, Goa, India<sup>1</sup>

Assistant Professor, Department of ETC Engineering, GEC, Farmagudi, Goa, India<sup>2</sup>

**Abstract:** In this paper we propose, a blind digital image watermarking algorithm based on combined DWT-DCT transformation with low frequency watermarking. The watermark embedding is carried out by modifying the wavelets coefficients of carefully selected DWT sub-band of a host image after two levels of DWT decomposition, followed by the application of the block based DCT transform on the selected sub-band. Watermark embedding is done using low frequency coefficients of each selected 4×4 DCT block. The watermarked host image is exposed to several watermark attacks. Experimental results demonstrate that the proposed algorithm is able to withstand a variety of common signal processing and geometric attacks.

**Keywords:** Discrete Cosine Transform, Digital Image Watermarking, Discrete Wavelet Transform, PSNR.

## I. INTRODUCTION

Internet evolution, together with the development of several digital multimedia tools has offered an extremely easy way for duplication, distribution and manipulation of the multimedia data. This has raised a concern for multimedia security. Digital watermarking is an effective way to tackle this situation.

Watermarking is a process that hides some information into the original image imperceptibly. This hidden information is called the watermark. The watermark information can be copyright information, authentication information or controlling information so as to determine the copyright owner of the digital works, certify the authenticity and integrity of multimedia works, control copying according to the embedded control information, achieve the purpose of copyright protection [1].

Watermarking techniques can be categorized in several ways. Depending on the need of the original image, watermarking is classified as non-blind and blind watermarking. The requirement of original image for detecting the watermark is known as non-blind watermarking, while the blind technique does not require the original image [2]. Watermarking is commonly classified based on the domain used for watermarking, that is spatial domain and transform domain. Spatial domain techniques are simple but do not provide good resistance against image compression and other image processing. Transform domain watermarking commonly use Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).

As compared to spatial domain techniques transform domain techniques provide higher degree of imperceptibility and robustness. Discrete wavelet transform has excellent spatial localization and multi-resolution characteristics which are similar to the theoretical model of human visual systems. This is the reason why DWT is employed more frequently in digital image watermarking. The imperceptibility and robustness of DWT-based digital image watermarking algorithms could be boosted if we combine DWT and DCT [2-6]. In this manner the shortcomings of the two transforms could be compensated. As a result of this better watermarking is achieved.

The rest of the paper is divided into four sections and organized in the following manner. We have discussed the watermark embedding procedure in detail in Section II. Section III gives the complete watermark extraction procedure. To demonstrate the performance of this algorithm the experimental results are presented in section IV. Section V gives the conclusion.

## II. THE WATERMARK EMBEDDING PROCEDURE

The entire watermark embedding procedure is performed using the following steps. The block representation of the same is depicted in Fig. 1.

**Step1:** Decompose the original image of size 512×512 into four non-overlapping multi-resolution sub-bands using DWT. This results in sub-bands LL<sub>1</sub>, HL<sub>1</sub>, LH<sub>1</sub>, and HH<sub>1</sub> each of size 256×256.

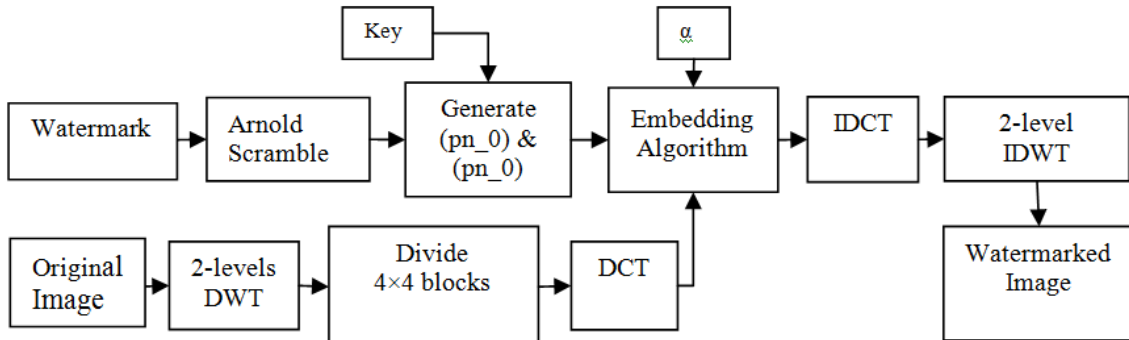


Fig.1 Detailed watermark embedding procedure

**Step2:** Using DWT decompose sub-band HL<sub>1</sub> of size 256×256 to get four smaller sub-bands each of size 128×128. Fig. 2 shows the 2-level decomposition of an image. Select HL<sub>2</sub> sub-band for embedding the watermark bits.

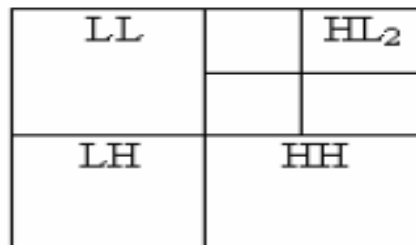


Fig.2 Decomposition of image with two levels DWT

**Step3:** Next divide the sub-band HL<sub>2</sub> into number of blocks equal to watermark bits that is 1024 blocks. Each of the blocks will be of size 4x4.

**Step4:** Now perform DCT on each 4x4 block obtained from the previous step.

**Step5:** Arnold Scramble the watermark to increase the robustness. Arnold transform is given as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{ mod } N ; x, y \in \{0, 1, 2, \dots, N - 1\} \quad (1)$$

Where, x and y are the original watermark pixel coordinate, and x' and y' are the transformed watermark pixels coordinate. The application of Arnold transform will give a scrambled watermark. This scrambled watermark is embedded into the host image.

**Step6:** Use a key and generate two uncorrelated pseudorandom sequences. The first sequence is used to embed the watermark bit 0(p<sub>n\_0</sub>) and the second sequence is used to embed the watermark bit 1(p<sub>n\_1</sub>) .

**Step7:** Using the gain factor 'α' embed the two pseudorandom sequences in the DCT transformed 4x4 blocks of the selected DWT coefficient set (HL<sub>2</sub>) of the host image.

Only low frequency coefficients of each DCT block are used for embedding. Fig. 3 shows the lower frequency coefficients that are used for watermarking embedding.

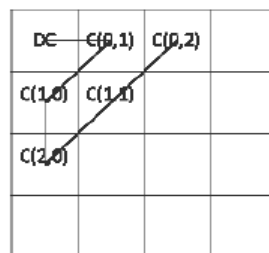


Fig. 3 Low frequency coefficients of a 4x4 DCT block used for watermarking

If we denote Z as the matrix with elements as the low frequency coefficients of the 4x4 DCT transformed block, then embedding is carried out as per the equations (2) and (3).

$$Z' = Z + (\alpha \times pn\_0) ; \text{ watermark bit } = 0 \tag{2}$$

$$Z' = Z + (\alpha \times pn\_1) ; \text{ watermark bit } = 1 \tag{3}$$

**Step8:** Perform the IDCT on each block.

**Step9:** Perform the IDWT on the DCT transformed image to get the final watermarked host image.

### III. THE WATERMARK EXTRACTION PROCEDURE

The entire watermark extraction procedure is performed using the following steps. The block representation of the same is shown in Fig. 4.

**Step1:** Decompose the watermarked image into four non-overlapping multi-resolution sub-bands using DWT. This results in sub-bands LL<sub>1</sub>, HL<sub>1</sub>, LH<sub>1</sub>, and HH<sub>1</sub>.

**Step2:** Further decompose the sub-band HL<sub>1</sub> using DWT to get four smaller sub-bands.

**Step3:** Next divide sub-band HL<sub>2</sub> into 4 × 4 blocks.

**Step4:** Perform DCT on each 4 × 4 block in the chosen sub-band (HL<sub>2</sub>).

**Step6:** With the help of the same key that was used in the watermark embedding procedure regenerate the two pseudorandom sequences pn<sub>0</sub> and pn<sub>1</sub>.

**Step7:** Beginning with the first block till the last block, calculate correlation between the low-band coefficients of the block and the two generated pseudorandom sequences.

If the correlation of the low-band coefficients with the pn<sub>0</sub> is higher as compared to the correlation with pn<sub>1</sub>, then the extracted watermark bit is taken as 0, otherwise the extracted watermark bit is taken as a 1.

**Step8:** Using the watermark bits that are extracted using the previous step, reconstruct the scrambled watermark.

**Step9:** Finally scramble the reconstructed watermark with arnold transform with the same key times.

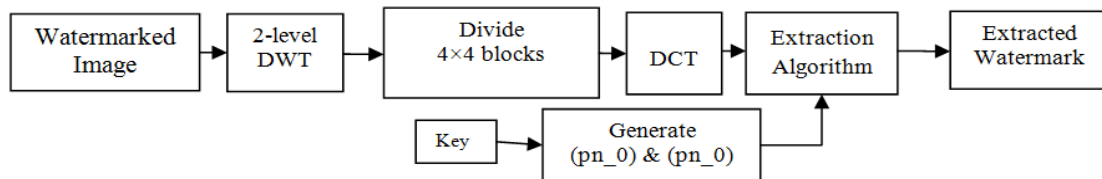


Fig.4 Watermark extraction procedure using combined DWT-DCT

### IV. EXPERIMENTAL RESULTS

For this experiment a standard image “Lena” of size 512×512 is used as the host image and binary image of size 32×32 with text “ECI” is used as the watermark. The watermarking algorithm is implemented using MATLAB. We evaluated the performance of the algorithm in terms of imperceptibility and robustness.

**Imperceptibility:** It means that the perceived quality of the host image should not be distorted by the presence of the watermark [6]. Peak signal to noise ratio (PSNR) is commonly used to measure the imperceptibility. It is defined by the following equation.

$$PSNR(dB) = 10 \log_{10} \left( \frac{255^2}{MSE} \right) \tag{4}$$

PSNR is obtained by first computing the Mean Squared Error (MSE) between the original image and the watermarked image.

$$MSE = \frac{\sum_{i=0}^{N-1} \sum_{j=0}^{N-1} [I_1(i, j) - I_2(i, j)]^2}{N \times N} \tag{5}$$

Where I<sub>1</sub>(i,j) and I<sub>2</sub>(i,j) represent original and watermarked images respectively with dimensions N×N.

**Robustness:** Several attacks may try to remove the watermark; the ability of the watermark to withstand these attacks is robustness. To measure robustness, the extracted watermark from the attacked image is tested for similarity with the original watermark. Normalized Correlation (NC) factor is used for testing the similarity.

$$NC = \frac{\sum_{j=0}^{J-1} \sum_{k=0}^{K-1} W_1(j, k) W_2(j, k)}{\sum_{j=0}^{J-1} \sum_{k=0}^{K-1} W_1(j, k)^2} \tag{6}$$

where W<sub>1</sub> and W<sub>2</sub> are respectively the original and extracted watermarks.

Fig.5 shows the standard “Lena” test image which is used as the host image, the watermarked image with no attack, original watermark image and the extracted watermark with no attack.

The watermarked image does not show any visible distortions and has a PSNR value of 37.3950 dB. This high value of PSNR indicates that the watermarking algorithm has achieved high imperceptibility. For no attack case the extracted watermark is exactly same as original watermark with NC=1.



Fig.5( a) Host image (512×512), (b) Watermarked image, (c) Original watermark, (d) Extracted watermark without attack (NC=1)

To test the robustness of the watermarking, several image manipulation techniques such as JPEG compression, salt & pepper noise, speckle noise, gaussian noise, image cropping , and median filtering were introduced to distort the watermarked image. Fig.6 shows the watermarked “Lena” image distorted by different attacks.



Fig.6 Watermarked “Lena” image distorted by different attacks (a) JPEG (Q=50), (b) Salt & pepper noise, (c) Speckle noise, (d) Gaussian noise, (e) Cropping, (f) Median filtering

Table1 shows extracted watermarks under different attacks, and the respective NC values. It is clearly seen that under most of the common attacks the algorithm successively extracts the watermark. Thus the watermarking algorithm has achieved high robustness.

**TABLE.1 EXTRACTED WATERMARKS UNDER DIFFERENT ATTACKS**

| Attack              | Parameter     | PSNR(dB)       | Extracted watermark |
|---------------------|---------------|----------------|---------------------|
| JPEG compression    | Q=70          | 35.6500        | <b>ECI</b>          |
|                     | Q=50          | 32.3004        | <b>ECI</b>          |
| Salt & pepper noise | Strength=0.01 | 24.6427        | <b>ECI</b>          |
|                     | Strength=0.02 | 21.9421        | <b>ECI</b>          |
|                     | Strength=0.05 | 18.1948        | <b>ECI</b>          |
| Speckle noise       | Variance=0.01 | 26.3047        | <b>ECI</b>          |
|                     | Variance=0.05 | 19.4088        | <b>ECI</b>          |
|                     | Variance=0.1  | 16.7225        | <b>ECI</b>          |
| Gaussian noise      | Mean=0        | Variance=0.004 | 23.2628             |
|                     |               | Variance=0.006 | 21.5484             |
|                     |               | Variance=0.01  | 19.5494             |
| Cropping            | 64×64         | 22.7633        | <b>ECI</b>          |
|                     | 128×128       | 16.3638        | <b>ECI</b>          |
|                     | 256×256       | 10.0639        | <b>ECI</b>          |
| Median filtering    | (3×3) window  | 31.2754        | <b>ECI</b>          |

**V. CONCLUSIONS**

We proposed an imperceptible and robust blind digital watermarking algorithm that utilised combined DWT-DCT transformation. Combining the two transforms improved the performance of the watermarking algorithm in terms of imperceptibility and robustness. In the proposed method the host image is decomposed by two levels DWT. Block based DCT is then applied to the selected DWT sub-band and watermark embedding is carried out mainly with the low frequency coefficients of each DCT block. To increase the imperceptibility further, the watermarked image is adjusted by weighted correction in spatial domain. Experimental results show that the watermarking is robust against several common attacks such as JPEG compression, salt & pepper noise, speckle noise, gaussian noise, image cropping, and median filtering.

**REFERENCES**

- [1]. Jiang Xuehua. "Digital Watermarking and its Application in Image Copyright Protection", 2010 International Conference on Intelligent Computation Technology and Automation.
- [2]. Akter Afroja, Nur-E-Tajjina, and Muhammad Ahsan Ullah. "Digital image watermarking based on DWT-DCT: Evaluate for a new embedding algorithm", 2014 International Conference on Informatics Electronics & Vision (ICIEV).
- [3]. Saied Amirgholipour Kasmani, Ahmadreza Naghsh-Nilchi, "A New Robust Digital Image Watermarking Technique Based On Joint DWT-DCT Transformation", IEEE 3<sup>rd</sup> International Conference on Convergence and Hybrid Information Technology Vol. 2 ,year 2008, pages 539-544.
- [4]. Ali Al Haj, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science 3(9):740-746, ISSN 1549-3636, year 2007.
- [5]. Deb K., Al-Seraj M. S., Hoque M. M., Sarkar M. I. H., "Combined DWT-DCT Based Digital Image Watermarking Technique for Copyright Protection", IEEE 7th International Conference on Electrical and Computer Engineering, 20-22 December, year 2012, pages 458-461, Dhaka, Bangladesh.
- [6]. Bhupendra Ram, "Digital Image Watermarking Technique Using Discrete Wavelet Transform And Discrete Cosine Transform", International Journal of Advancements in Research & Technology, Volume 2, Issue4, April-2013, ISSN 2278-7763.