COPYRIGHT PROTECTION FOR DIGITAL IMAGES

Thuong Le-Tien, Tuan T. Nguyen

Department of Telecommunications, HCMUT, VietNam
thuongle@hcmut.edu.vn, nguyenthanhtuan@hcmut.edu.vn

ABSTRACT

Nowadays, the copyright protection problem of digital works becomes the urgent and necessary requirement. The paper proposes the method of watermarking approach for copyright protection with still images in DWT (Discrete Wavelet Transform) domain, finds out the optimal parameters for embedding and detecting watermark, and estimates the its robustness in comparison with algorithm using traditional DCT (Discrete Cosine Transform). Unlike some algorithms before, the optimal watermark is added to maximum coefficients of the approximation band in Wavelet domain to enhance the robustness. We also use two keys: one for watermark and another for generating embedded multi-bits to reinforce the security. Besides, lots of various attacks such as compression (JPEG and JPEG2000), filtering (average, median, adaptive, sharpening, Gaussian, etc) and noise are investigated with different type of images. Based on these results, the paper also proposes the solution for verifying on kit DSP TMS320C6711.
Key words: Watermarking, DCT, Wavelets, DWT, JPEG2000.

1. WATERMARKING OVERVIEW

Watermarking is one of the modern data hiding technologies. It is defined as inserting the information on the multimedia without perceptiveness, means that only making the small changes in the original data. Normally, we only discuss about digital watermarking. It is known that a set of the secondary digital data – called the watermark – is embedded in the primary digital media – called the cover data – such as text, image, digital audio and video. The data after embedding is called the watermarked data.

The first publications about watermarking were in turn published by Tanaka (1990), Caroni and Tirkel (1993) [1] but it was not taken care much. Until 1995, this topic became interesting more and since then digital watermarking developed rapid with lots of further research and various methods.

Watermarking is applied in lots of fields such as copyright protection, fingerprinting, copy protection, broadcast monitoring, data authentication, data hiding, indexing, etc [2]. A popular application of watermarking today is to give proof of ownership of digital data by embedding copyright statements. This application requires a very high level of the robustness. Additional issues besides robustness have to be considered. For example, the watermark must be clear and still resolve rightful ownership if other parties embed additional watermarks or attack.

All watermarking methods share the same generic building blocks: a watermark embedded system and a watermark recovery system [3]. The generic watermark embedding process is described in Figure 1. The input to the scheme is the watermark, the cover-data and an optional public or secret key. The output of the watermarking scheme is the watermarked data.

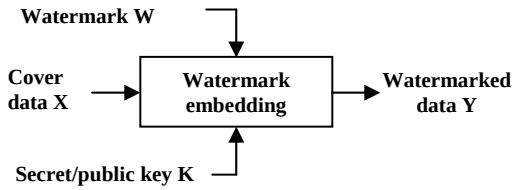


Fig 1. Generic watermark embedding scheme.

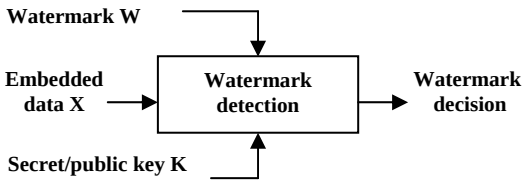


Fig 2. Generic watermark recovery scheme.

Figure 2 shows the generic watermark recovery. Inputs to the scheme are the watermarked data, the secret or public key, and the original data or the original watermark, depending on the method. The output is either the recovered watermark or some

kind of trust measure indicating how likely it is for the given watermark at the input to be existent in the data under examination.

Depending on the watermarking application and purpose, different requirements arise resulting in various design issues. But for real-world efficient watermarking systems, they have some common requirements below.

- Imperceptibility: the modifications caused by watermark embedding should be below the perceptible threshold, which means that the individual samples that are used for watermark embedding are only modified by a small.
- Robustness: robustness of the watermarked data against noise, modifications or malicious attacks is one of the key requirements in watermarking.
- Watermark recovery with or without the original data.
- Watermark extraction or verification of presence for a given watermark.
- Watermark security and keys.

2. THE WAVELET TRANSFORM

Over the past several years, the Wavelet transform has gained widespread acceptance in signal processing in general, and in image compression research in particular. In many applications Wavelet-based schemes (also referred as sub-band coding) outperform other coding schemes like the one based on DCT. Because of their inherent multi-resolution nature, Wavelet coding schemes are especially suitable for applications where scalability and tolerable degradation are important.

Wavelets are functions defined over a finite interval and having an average value of zero. The basic idea of the Wavelet transform is to represent any arbitrary function *f(t)* as a superposition of a set of such wavelets or basis functions. These basis functions or baby wavelets are obtained from a single prototype wavelet called the mother wavelet, by dilations or contractions (scaling) and translations (shifts) [4].

In real calculation, the discrete Wavelet transform (forward and inverse) is often done following equation (1) and (2).

$$\mathrm{DWT_f(m,n)} = a_0^{-m/2} \int_{-\infty}^{+\infty} f(t)\psi^*(a_0^{-m}t - nb_0)dt \qquad (1)$$

$$\mathrm{f(t)} = \sum_{m=-\infty}^{+\infty} \sum_{n=-\infty}^{+\infty} < \psi_{m,n}, f > \tilde{\psi}_{m,n}(t) \qquad (2)$$

Where, $\psi(t)$ is mother wavelet. The condition of $\psi(t)$ being bandpass function ensures the existence of the inverse Wavelet transform. Commonly, choose $a_0=2$ and $b_0=1$.

As discussed above section, watermark can be performed in traditional transform domain such as DFT, DCT, etc. Unlike these transforms, Wavelet transform has the multi-resolution characteristic. So it is used in many applications, and now is becoming a key technique in the ongoing source compression standard JPEG-2000. The positive arguments closely resemble those for advocating DCT for JPEG, which means that preventing watermark removal by JPEG-2000 lossy compression, reusing previous studies on source coding regarding the visibility of image degradations, and offering the possibility of embedding in the compress domain. In addition to these criteria, the multi-resolution aspect of wavelets is helpful in managing a good distribution of the message in the cover in terms of robustness versus visibility. General speaking, the Wavelet transform consists in a multi-scale spatial frequency decomposition of an image. Decomposition of the image generates the coefficients of the approximation and horizontal, vertical and diagonal details, and then the process repeatedly until the last level. The coefficients of the approximation contain information about the lowest frequency band, while coefficient of the details contain information about the high and low horizontal and vertical frequency band.

3. ALGORITHM

Based on Cox's DCT, additive, non-blind image watermarking algorithm [5, 6], this paper implements some improvements and embed the watermark in Wavelet domain according to diagram below [7, 8].

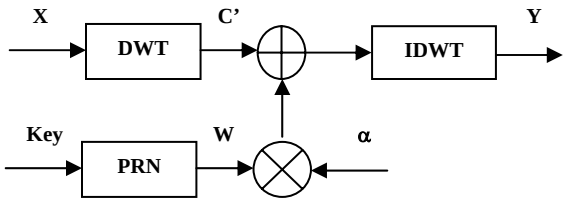


Fig 3. The watermark embedded process.

The watermark is produced by a pseudo- random number generator (PRN) with a secret key. The choice of the watermark length N and the watermark strength α determines to which degree the

watermark is spread out. In most cases the larger the watermark the lesser the embedding strength needs to be. But there is no watermark length N that is suitable for all images.

In the watermark embedding, DWT of an image is computed. A series of coefficients in suitable band which are the largest are extracted and embedded with the watermark by the following formula:

$$C' = C + \alpha * W \quad (3)$$

Where, alpha can vary from 0 to 1 and is the embedded strength of the watermark.

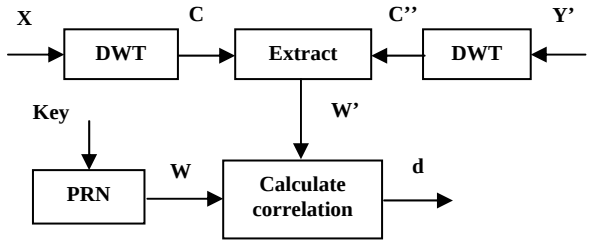


Fig 4. The watermark extracted process.

From equation (3) an extraction process can easily be found to be:

$$W' = (C'' - C) / \alpha \quad (4)$$

Where, C'' are N largest extracted coefficients from the watermarked images with attacks DWT domain. From equation (4) we see that the original coefficients C are needed. Therefore we need the original image; this is why this algorithm is non-blind.

When having the extracted watermark W', we can compare it to the original watermark with the following formula:

$$d = \sum_{1}^{N}\sum_{1}^{N}\left(\overline{W_i}' * \overline{W_i}\right) \Big/ \sqrt{\sum_{1}^{N}\left(\overline{W_i}'\right)^2 \sum_{1}^{N}\left(W_i\right)^2} \quad (5)$$

Value of d can range from 1 to –1. The closer the value is to 1 the better the watermark match is. By comparing the correlation d to a pre-defined threshold t, it is possible to determine if the watermark exists or not.

4. RESULTS

Firstly, we investigate to select the watermark. It is a real-value pseudorandom noise pattern with uniform or normal (Gauss) distribution. The length of the watermark in the investigating process is in turn 50, 100, 200, 300, 1000 and 10000. Figure 5 presents the average and maximum correlation values of ten thousands of different watermarks. When two watermarks are same, the correlation value of them equals 1, and when they are different, the correlation value of them is very low (near 0), that means the objectiveness is good. The result in figure 5 shows that the normally distributed random is better than uniformly distributed random, and the larger the length of watermark is, the better the result is. However, when the length of watermark is large, the capacity of embedding multi-bits is low. So the paper proposes to choose the normally distributed random watermark with the length of 1000 in the case of embedding one bit.

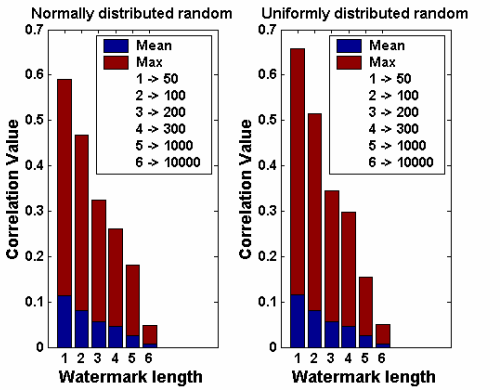


Fig 5. Correlation value of different watermarks.

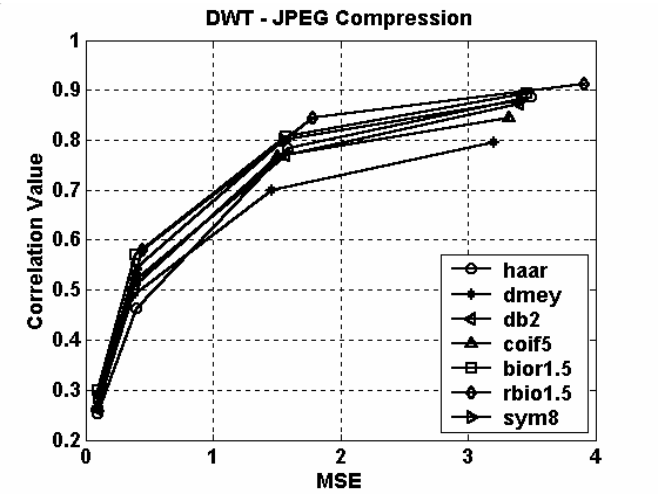


Fig 6. Compare MSE of DCT and DWT with different wavelet families.

Next, the paper compares the perceptivity between DCT and DWT watermarking domain. The result is evaluated by means of objective metrics MSE (Mean Square Error) and PSNR (Peak Signal Noise Ratio). Figure 6 shows that DWT method gives the result better than DCT (about objective aspect), it means that with the same watermark strength α the quality of watermarked image in DWT degrades less.

Besides, it can be seen that wavelet family Bior3.9 gives the best result. However, the perceptual transparence is in inverse proportion to robustness. So after considering subjective perceptivity through HVS (see Figure 7) and some different factors such as executed time and complexity, the paper selects the Haar wavelet in DWT method to compare with DCT.

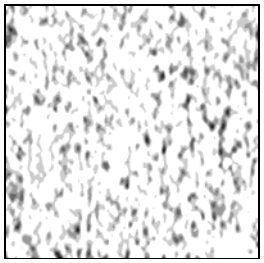
In DWT method, embedding in the approximation band gives less MSE than detail bands, especially in high level. However, when evaluating with HVS the result is not good at this band. This is fully suitable with the characteristic of the wavelet transform. In the wavelet transform, the approximation coefficients contain almost energy of the signal while the detail coefficients contain information of the signal. So embedding in the approximation band will affect to perceptivity more than in the detail bands, focus in the edge of the image. When the level is high, this effect expands then human eyes can not be perceptive. Embedding in the detail bands gives HVS a bit better than the approximation band, but we are easy to find out the robustness of watermarking in these bands is not good, and so it is not effective before popular attacks such as compress JPEG or JPEG2000, noise, … Therefore, the paper selects to embed watermark in the approximation band at level 3 with the Haar wavelet.

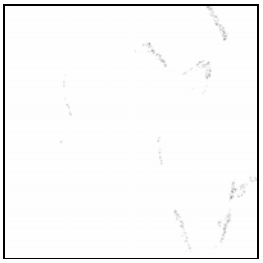
Table 1. Compare MSE of DCT and DWT.

DCT 6.30	DWT appro	DWT hori	DWT vert	DWT diag
Level 1	**6.21**	**6.13**	**6.12**	**6.10**
Level 2	**6.20**	**6.19**	**6.20**	**6.19**
Level 3	**6.28**	**6.28**	**6.29**	**6.28**

Table 2. Compare PSNR of DCT and DWT.

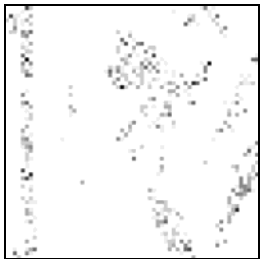
DCT 35.29	DWT appro	DWT hori	DWT vert	DWT diag
Level 1	**35.35**	**35.41**	**35.42**	**35.43**
Level 2	**35.36**	**35.37**	**35.36**	**35.36**
Level 3	**35.30**	**35.30**	**35.30**	**35.30**

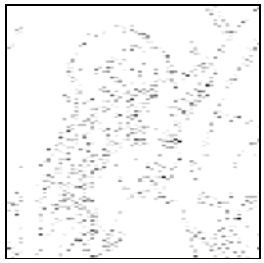




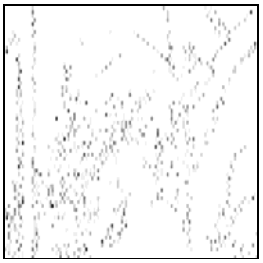
(a) Original image (b) Edged image

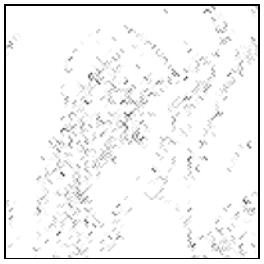
(c) DCT difference image (d) Haar appro.1





(e) Haar appro. 3 (f) Haar vert. 3





(g) Haar hori. 3 (h) Haar diag. 3

(i) DCT watermarked image (j) Haar appro. 3

Fig 7. Illustrated images using DCT and DWT.

Through the results in Table 1, 2 and Figure 6, 7 (the amplitude amplified maximum for view), obviously if evaluating by MSE or PSNR, watermarking in DWT gives perceptivity not much better than DCT. But Figure 7 (i and j) shows that when using HVS, watermarked image with the Haar wavelet level 3 (MSE=9.9390) is almost same with the original image and better than watermarked image using DCT (MSE=10.0379). Since its basis functions have variable length, DWT-based watermarking is more

robust and better matched to the HVS characteristics. Meanwhile, DCT does not have characteristic of multi-resolution as DWT so the effect of watermark presents in whole image.
Following, investigating the effect of compress JPEG and JPEG2000 on the watermarked image. In both case, the results are executed with image Lena.

Table 3. Correlation coefficient of DCT and DWT with JPEG compress.

α	DCT	DCT 1	DCT 2	DCT 3
3	0.2030	0.2494	0.2207	0.2614
5	0.3649	0.3791	0.3283	0.4774
10	0.5825	0.5315	0.5361	0.7101
20	0.7859	0.6276	0.7228	0.8843

In the case of JPEG compress, DWT watermarking in the details bands is completely fail. But performing in approximation band is better than DCT, especially in level 3 and with small watermark strength α.

Table 4. Correlation coefficient of DCT and DWT at different levels with JPEG2000 compress.

Compress level	DCT	DWT 1	DWT 2	DWT 3
1 (37.6%)	0.74	0.96	0.92	0.76
2 (44.7%)	0.45	0.60	0.90	0.76
3 (45.6%)	0.29	0.51	0.60	0.76

Table 5. Correlation coefficient of DCT and DWT at different bands with JPEG2000 compress.

DCT 0.773	DWT appro	DWT hori	DWT vert	DWT diag
Level 1	0.775	0.774	0.778	0.787
Level 2	0.783	0.782	0.774	0.773
Level 3	0.783	0.767	0.762	0.769

In the case of JPEG2000 compress, DWT watermarking predominates over DCT, especially within the same of watermarking and compress level. The higher the compress level is, the larger compress ratio is. The results in Table 4 and 5 are investigated with α=10.

Table 6. Correlation coefficient of DCT and DWT with Gauss noise.

P_{noise}	0.0005	0.001	0.005	0.01
DCT	0.8740	0.7736	0.4729	0.3553
DWT	0.8483	0.7833	0.5006	0.4707

After that, the paper continues to consider the effect of the noise. The result is in Table 6. Obviously, DWT only detect watermark better than DCT when embedding in the approximation band with high level. Because Gauss noise can be considered high frequency signal, so it affects not much to the approximation band (low frequency), especially in the high level. Table 6 shows that the larger the power of the noise is, the better the robustness of watermarking in DWT is, but not much. However, if using de-noise tool before detecting watermark, DWT can give better result.
Another factor to evaluate the reliability of watermarking system is BER (Bit Error Rate). In the process of watermark recovery, there are two types of faults: positive fault (undetected watermark) and negative fault (detect incorrectly). Obviously, when the threshold is small, the positive fault decreases but the negative fault increases and on the contrary. So depending on the requirement we can select the suitable threshold.
In the case of embedding multi-bits, the watermark length is selected to equal 100. The BER graph is determined in the case of whole bit 1 with α = 5, DWT in the approximation band level 3 and threshold 0.3 (for the negative fault is the smallest). The attacks include in compress JPEG and JPEG2000, Gauss noise, median, average and adaptive filter. If the requirement of the objective reliability is smaller, we can select the threshold smaller to increase the reliability of whole system.
The result in Figure 8 and 9 shows that watermarking in DWT gives BER smaller than DCT, it means watermarking in DWT is more robust before attacks.

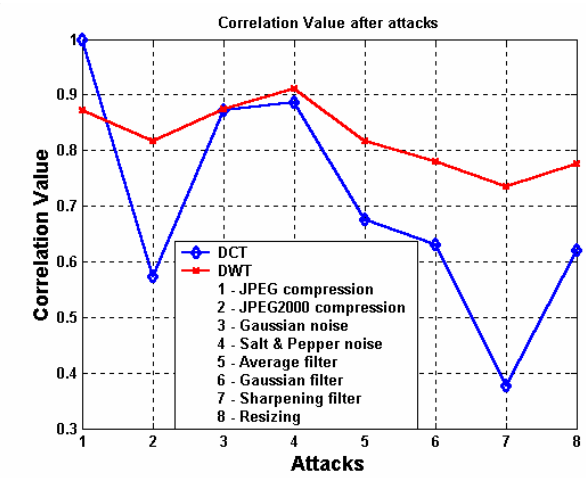


Fig 8. Correlation value of DCT and DWT.

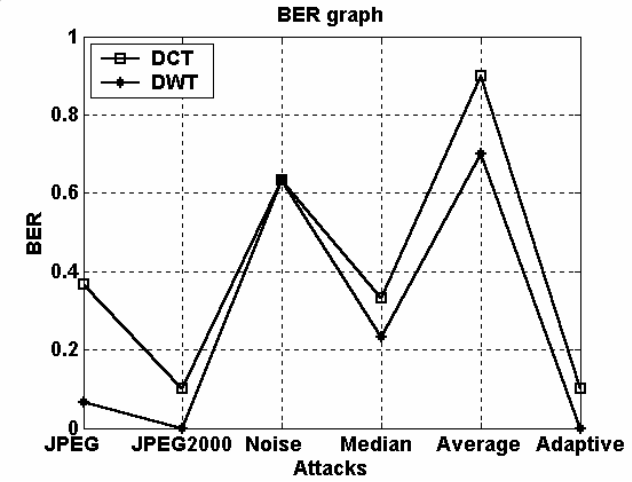


Fig 9. BER graph of DCT and DWT.

We also verified the results on kit DSP TMS320C6711 following the Figure 10. In this figure, the dash block is used to examine the real-time response. The first Sync block identifies the parameters of the embedding and extraction process. The second Sync block (dash) maintains the synchronization of transmitting and receiving process.

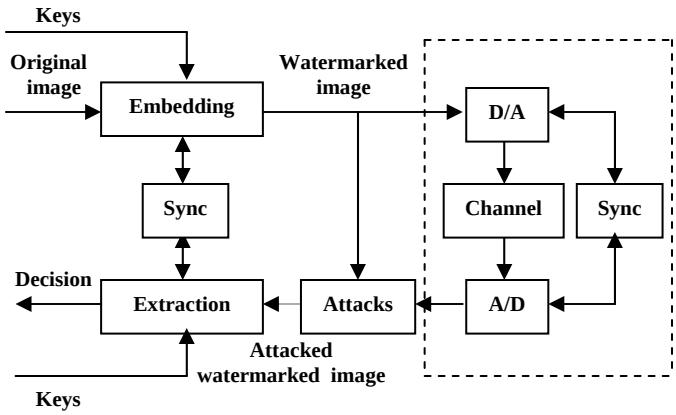


Fig 10. The diagram of verification on DSP.

5. CONCLUSION

Through the process of investigation, we can conclude that watermarking in DWT makes the system become more powerful and robust than in traditional DCT while ensuring the requirement about the perceptivity. Besides, based on these results, we are performing watermarking for audio and video with some suitable modifications to get result better.

REFERENCES

[1] Stefan Katzenbeisser and Fabien A. P. Petitcolas, *Information Hiding techniques for steganography and digital watermarking*, Security Technologies for the World Wide Web, Rolf Oppliger.

[2] Gerhard C. Langelaar, Iwan Setyawan, and Reginald L. Lagendijk, Watermarking Digital Image and Video Data, *IEEE Signal Processing Magazine, Vol. 17*, No. 5, September 2000.

[3] Special issue on signal processing for data hiding in digital media and secure content delivery, *IEEE Transactions on Signal Processing, volume 51*, Number 4, ISSN 1053-587X, 04/2003.

[4] Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal G. Shamoon, Cox's DCT, additive, non-blind Image Watermarking Algorithm, *Proceedings of the IEEE International Conference on Image Processing, ICIP '97, volume 6, page 1673-1687*, Santa Barbara, California, USA, 1997.

[5] I. Cox, J. Bloom and M. Miller, Digital Watermarking, San Francisco, 2001.

[6] Martin Vetterli and Jelena Kovacevic, *Wavelets and Subband Coding*, Prentice Hall 1995, ISBN 0–13–097080–8.

[7] Yiwei Wang, John F. Doherty, and Robert E. Van Dyck, A wavelet-based watermarking algorithm for ownership verification of digital image, *IEEE Transactions on Image Processing, Vol. 51*, No. 4, April 2003.

[8] Chih-Wei Tang and Hsueh-Ming Hang, Fellow, IEEE, A Feature-Based Robust Digital Image Watermarking Scheme, *IEEE Transactions on Signal Processing, Vol. 51*, No. 4, April 2003.