International Journal of Advances in Image Processing Techniques– IJIPT
Volume 2: Issue 1 [ISSN : 2372-3998]
Publication Date : 30 April, 2015

Image watermarking technique in MDCT domain exploiting the properties of the JND model

[Maha Bellaaj, Kais Ouni]

***Abstract*—View the development of the internet in the 90s and the orientation of the world to an era when digital is playing an increasingly important have found ourselves faced with serious problems of copyright. Where digital watermarking as an effective solution does faces to these problems and whose basic idea is to insert a mark in digital media.**

In this paper, we will present a watermarking technique for image. Our proposed technique operates in the frequency domain. We will apply the MDCT (Modified Discrete Cosine Transform) on the original image to pass from temporal domain to frequency domain. We exploited the proprieties of the JND (Just Noticeable Difference) model to search the places for insertion of the watermark to optimize the imperceptibility criterion of the mark at the insertion phase of the proposed technique. To ensure maximum capacity of insertion, we will duplicate the bits of the brand N times and then each bit is inserted in the LSB (Least Significant Bit) of the components sought by JND model. In order to increase the detection rates, we used Hamming code as error correction code. We evaluated the invisibility of the technique by calculating the PSNR, the Structural Similarity Metric (SSIM). We studied the robustness of this technique against the different attacks given by checkmark. Finally, to highlight our results, we compared the proposed technique with some other existing techniques.

***Keywords*—watermarking, MDCT, JND, LSB, Hamming, impercebtibility, PSNR, SSIM, checkmark, robustness**

I. Introduction

This new era where digital takes a place increasingly important poses serious problems of copyright. In this context, digital watermarking [1] has been introduced in the early 90s as an additional mechanism of security to encryption. Its basic idea is to protect a digital document (audio, video, picture ...) by embedding a signal in robust and imperceptible way [2]. However, there are several domain of insertion. We can distinguish three main categories: the spatial domain (time domain), the frequency domain and the multi resolution domain. The selection of the domain of integration and detection is an important stage in the design of the watermarking scheme.

In addition, a good marking system must meet the following specifications: imperceptibility, robustness against attacks and high insertion capacity (ratio). Or, in case of digital images, the embedded information can be either visible or invisible from the user. In this work, we will concentrate on invisible watermarking. In this paper we propose a watermarking technique for digital image based on spectral approach of insertion of the mark combined with the proprieties of a JND model to improve the robustness of the techniques.

This paper is organized as follows: in section 2 we will detail the process of insertion and detection for the proposed technique. Section 3 will present the experimental results. In section 4, we compare the results obtained by the proposed technique with other existing in the literature

In the last section we give a conclusion for this work.

Maha Bellaaj/U.R. Signals and Mechatronic Systems UR 13ES49
Higher School of Technology and Computer Science Carthage University

Kaïs Ouni/U.R. Signals and Mechatronic Systems UR 13ES49
Higher School of Technology and Computer Science Carthage University
Tunis

II. Presentation of the proposed technique

This section describes in detail the process of integration and detection of the mark of the proposed technique. In general, Image watermarking consists to insert in a manner robust a signal (watermark) in the original image in order to protect it against illegal manipulations.

A. *MDCT*

The majority of existing watermarking techniques for images and video use block transformations that introduce blocking artifacts causing perceptible distortions. For this reason, the proprieties of MDCT [10] are helpful in eliminating the blocking artefacts. In addition, the MDCT is a lapped transform, where the coefficients are separated into "Low-Frequency" part and "High-Frequency" part. The major interest of this transform is that the coefficients are real and there are also robust to manipulations changing their values. The MDCT for two dimensional arrays is defined as:

$$X(k,l) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} s(i,j)\cos\left(\frac{\pi}{N}(2k+1)(i+n)\right)\cos\left(\frac{\pi}{N}(2l+1)(j+n)\right) \quad (1)$$

With:

- $n = \frac{1}{2}\left(\frac{N}{2}+1\right)$

When it is implemented effectively with FFT algorithm and the coefficients are symmetrical.

$$x(k,l) = x(N-k-1, N-l-1) = -x(k, N-l-1) = -x(N-k-1, l) \quad (2)$$

This reduces the spectrum size from N^2 to $\left(\frac{n}{2}\right)^2$.

The inverse MDCT is defined as:

$$Y(k,l) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\frac{4}{N}s(i,j)\cos\left(\frac{\pi}{N}(2k+1)(i+n)\right)\cos\left(\frac{\pi}{N}(2l+1)(j+n)\right) \quad (3)$$

B. *JND model*

Just Noticeable Difference (JND) [13] accounts for the smallest detectable difference between a starting and a secondary level of a particular sensory stimulus in psychophysics, which is also known as the difference limen or differential threshold.

JND model has given a promising way to model the properties of the Human Visual System (HVS) accurately and efficiently in many image/video processing research fields, such as perceptual image/ video compression, image / video perceptual quality evaluation, watermarking…

JND models generated in the transform domain, namely the sub band based JND, takes into account three characteristics of the HVS: the Contrast Sensitivity Function (CSF), luminance masking and contrast masking.

C. *Insertion process of the mark*

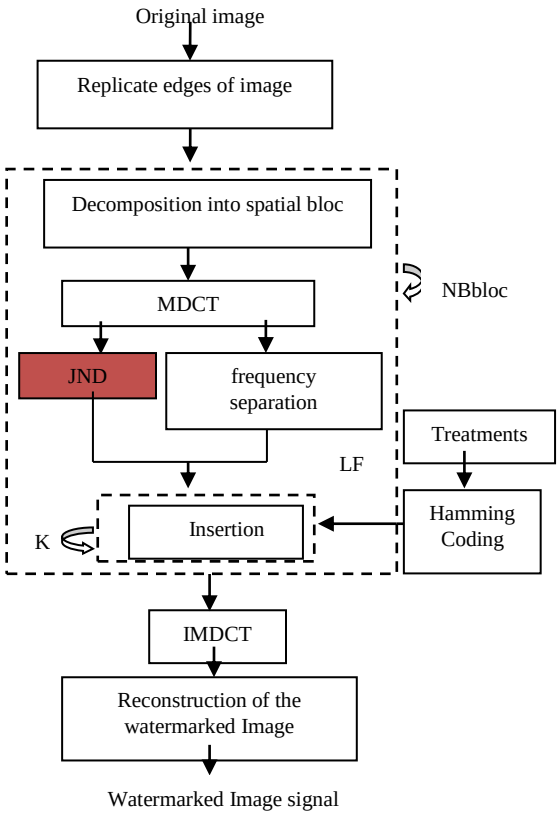


Figure 1: Insertion schema of the mark.

A detailed bibliographical study on the watermarking ([3, 4, 5] led us to choose the frequency domain as an insertion domain of the brand point of view robustness and invisibility, from where the idea of using MDCT to go from the time domain to the frequency domain [6, 7, 8, 9]. Parallel with this spectro-temporal processing, substitutive methods offer the possibility of using an error correcting code to reduce the error rate. For this, we have added to the proposed technique an error correcting code: Hamming code [11]. To reduce the visibility of the brand when inserting the bits of the brand, we have exploited the properties of the JND model in the search for insertions positions. In the final step, we duplicated the bits of the brand to enhance the robustness of the proposed method. The general scheme of the insertion of the mark is shown by Figure 1.

- ✓ The original image can be a color or grayscale image. The first step of the proposed technique is to fix the size of the blocks on which we will work. We have chosen to work on blocks of 8x8 pixels (blocksize=8). The choice of this size is inspired by the JPEG standard since it works on blocks of this size. And as we work on any image size (N × N or N × M) the size of these may not be a multiple of 8. For this, we proceed to replicate edges of image to make its dimensions a multiple of blocksize.

- ✓ The next step consists in the decomposition of the image into blocks of 8x8 pixels.

$$decomp = \sum_{i=1}^{N}\sum_{j=1}^{M} I(i:i+bloksize-1, j:j+bloksize-1) \quad (4)$$

With :
i = 1 ... N and j = 1... M with a step equal to blocksize = 8.

- ✓ To do the time frequency mapping, we will apply the MDCT.
$MDCTdecomp = MDCT(decomp)$ (5).
We will apply the MDCT on each block of 8x8 pixels.

- ✓ Subsequently, the frequency separation module intervenes which will ensure the separation of the frequency bands. At the output of this module, we get all the low frequencies (LF) where we will insert bits of the brand. The choice of the Low Frequency band is due to the fact that the latter is much less sensitive against the attacks than the high frequency band and the watermark hidden in the higher frequency band might be discarded after a lossy compression (JPEG compression for example). And as the human eyes are more sensitive to noise in lower-frequency band than higher frequency, the energy of natural image is concentrated in the lower frequency range. For this, we use a perceptual mask JND to look up

for the less sensitive and visible insertion places to the human eyes.

- ✓ This approach provides a good compromise between robustness and invisibility.
- ✓ In parallel, we will apply several treatments: binarization of the brand, decomposition into portions of 8 bits each) and Hamming coding (12, 8) to ensure the correction bits if necessary, since the bits of the signature can undergo changes during the insertion and detection. The inserted mark can be an image, a text, or a beep sound.
- ✓ To increase the capacity insertion, each bit is duplicated K times where K is calculated based on number of components that are given by the JND model and the size of the brand. Next, we will make a substitutive insertion of each bit of the mark in the least significant bit (LSB) of the searched components.
- ✓ All the steps already described previously will be repeated NB block times (number of blocks in the original image) and the insertion is done on all the blocks of the image.
- ✓ Thereafter, we apply the IMDCT on the frequency watermarked blocks to obtain watermarked blocks in the spatial domain.
- ✓ The final step consists in the reconstruction of the watermarked image.

D. *Detection process of the mark*

From figure 2, we notice that the detection scheme of the brand is the inverse of the insertion. It is a blind detection that does not require the original image or the presence of the mark originally inserted. Only the secret key (all the positions sought by the JND model in the insertion phase and the number of duplication K) is required. The output of the detection process is the final mark decoded and formatting.

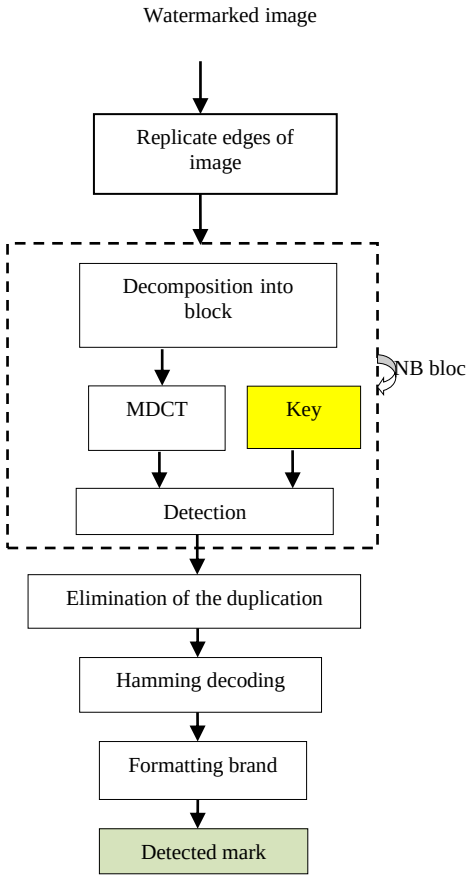


Figure 2: Detection schema of the mark.

III. Experimental results

In this section, we will present the various experimental results obtained by this technique. It was tested on five images whose characteristics are shown in the following table:

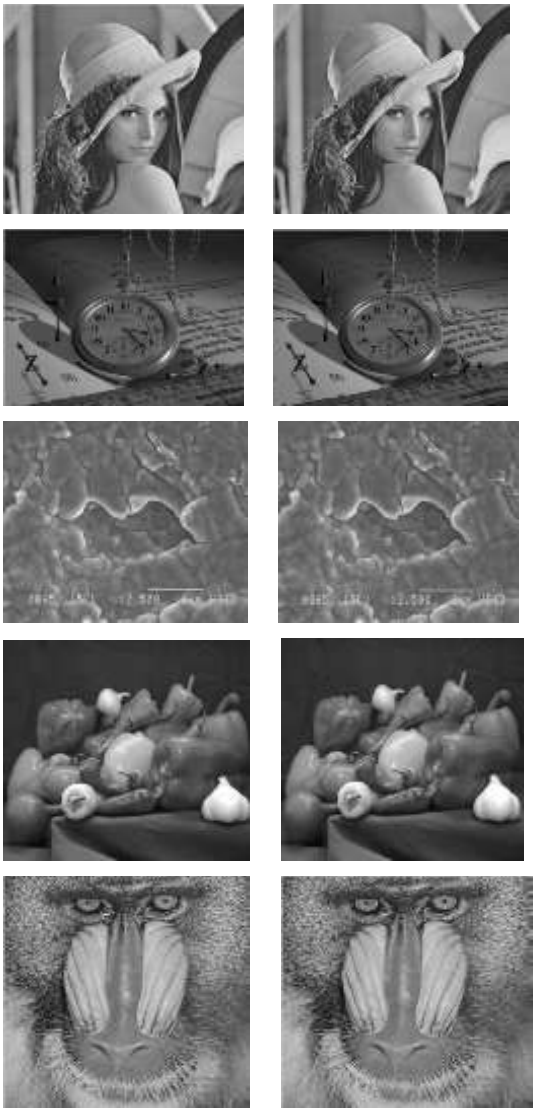
TABLE I. TEST IMAGES

Image	Size
Lena.jpg	512 x 512
Montre.jpg	375 x 500
Medical.jpg	413 x 500
peppers.jpg	512 x 512
Baboon.jpg	512 x 512

We inserted the mark image "logo.bmp" that size is 32 x 32 pixels. After treatment and hamming code we have 1536-bit. Then we insert N x 1536 bits. On after the tests we have made, we have detected the original mark without error and the watermarked image remains faithful to the original picture. The inserted mark is imperceptible.

Figure3: logo.bmp.

The following figure shows the image before and after watermarking:



(a) Originals images (b) Watermarked images

Figure 4: Watermarked images using the proposed technique.

A. *Evaluation of the imperceptibility*

- By calculating PSNR

PSNR (Peak Signal acronym to Noise Ratio) is a distortion measure used in digital image, especially in image compression. It is to quantify the performance of the encoder by measuring the quality of reconstruction of the compressed image compared to the original image. In particular, we used the PSNR to evaluate the invisible characteristic of our watermarking system. It is most easily defined via the mean squared error (MSE) which for two M × N monochrome images I and I' where one of the images is considered a noisy approximation of the other is defined as:

$$MSE = \frac{1}{M * N}\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j) - I'(i,j)]^2 \quad (6)$$

The PSNR is defined as:

$$PSNR = 10 * \log_{10}\frac{{MAX_I}^2}{MSE} \quad (7)$$

$$= 20 * \log_{10}\frac{MAX_I}{\sqrt{MSE}}$$

With, MAX_I is the maximum possible pixel value of the image. The following table gives the different PSNR values obtained by the proposed method for each image.

TABLE II. PSNR VALUES

Image	PSNR (db)
Lena.jpg	58,9915
Montre.jpg	57,5412
Medical.jpg	57,7869
peppers.jpg	58, 0081
Baboon.jpg	58, 0700

According to the results shown in the table, we note that the proposed technique gives interesting results point of view invisibility. We also note that the PSNR values vary between 58, 9915 db and 57, 5412 db which are prefect values. We obtain an average value of PSNR equal to 58.0795 db for the watermarking system.

- By SSIM measures

Structural Similarity or SSIM [15] is a measure of similarity between two digital images. It was developed for measuring the visual quality of a compressed image compared to the original image. The idea of SSIM is to measure the structural similarity between the two images, rather than pixel-to-pixel difference as does, for example, the PSNR. It's a human visual system based (HVS) image quality

metrics. The following table gives the different SSIM values obtained by the proposed method for each image.

TABLE III. SSIM INDEX

Image	SSIM
Lena.jpg	0.9997
Montre.jpg	0.9856
Medical.jpg	0.9887
peppers.jpg	0,9965
Baboon.jpg	0,9861

From the results presented in the table above, we obtained a value of SSIM between 0.9997 ~= 1 for lena.tif and 0.9856 for montre.jpg, which are very interesting values and this means that the degradation caused by the step of insertion is invisible, and show that our watermarking system degrades very little the image quality and proves that the proposed technique provides a good criterion for invisibility of the brand during the insertion process.

We obtain an average value of SSIM equal to 0.99132 db for the watermarking system.

B. *Robustness against attacks*

To test the robustness, we choose to apply all of the attacks proposed by checkmark [14], it's a second generation benchmarking for image watermarking which includes attacks which take into account powerful prior information about the watermark and the watermarking algorithms. this benchmark follow the model of the Stirmark benchmark and propose the 8 following categories of tests: denoising (ML and MAP), wavelet compression, watermark copy attack, active desynchronization, denoising, geometrical attacks, and denoising followed by perceptual remodulation.

Concerning the detection, we calculate the correlation between the inserted mark "bin" and the detected mark "bin ' " by the formula of the normalized intercorrelation [16].

$$NC = \frac{\sum_{i,j=1}^{n} bin(i,j) * bin'(i,j)}{\sqrt{\sum_{i,j=1}^{n} bin'(i,j)^2} * \sum_{i,j=1}^{n} bin(i,j)^2} \qquad (8)$$

More than the value of NC is near 1, more than the detected binary mark 'bin' "is faithful to the inserted binary brand "bin ". Our technique guarantee detection without errors (NC = 1) in the case of an ideal exchange (exchange without manipulations or attacks on the watermarked signal).

In the sequel, we donated some pictures for the picture lena_watermarked.jpg attacked by some checkmark attack.

Lena_watermarked after attack: collage

Lena_watermarked after attack: copy

Cropped image 10%

Cropped image 20%

Cropped image 50%

Cropped image 75%

Lena_watermarked after attach: projective rotation angle = 30

Lena_watermarked after attach: rotationscale rotation angle = 45

Lena_watermarked after attack: linear

lena_watermarked after attack: gaussian

Lena_watermarked After attack: wavletcompression Bitrate=0.1

Figure 5: Example of attacks.

In the following image, we summarize all the values of NC for each attack applied by checkmark.

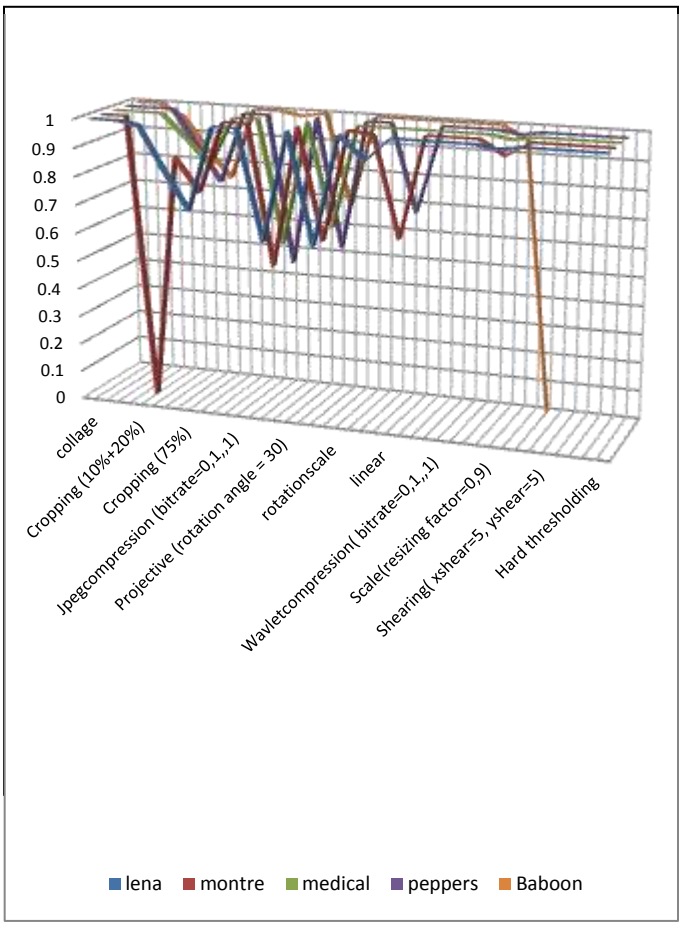


Figure 6: NC/ attacks.

Based on the results presented in the image above, we can conclude that the proposed technique is robust to several manipulations. For example, for attacks collage, copy, JPEGCompression (bitrate=0.1 …1), wavletcompression projective with a rotation angle equal to 30, shearing, rotationscale... The watermarking scheme is still robust (NC value always equal to 1). We could detect without error the inserted mark. These results still very interesting for cropping attacks (NC values vary between 0.7030 and 0.9871), rotation (NC values vary between 0.9181 and 1), scale (NC values vary between 0.9540 and 1).

We can therefore conclude that our technique has a remarkable features ensuring robustness to an important set of attacks and manipulations can be applied to the watermarked image.

IV. Comparison with the existing techniques

To highlight our results, we will compare in this section the detailed above technique with other technique existing in the literature [17, 18, 19, 20, 21]. We will present in the next table the values of PSNR for each technique.

TABLE IV. PSNR VALUES OF EACH TECHNIQUES

	COX method1	**COX method2**	**Xia method**	**Jong method**	**Method proposed in [21]**	**Proposed technique**
PSNR	51,36	42,43	50,12	52,46	56,01	58,0795

Table 5 will illustrate the values of SSIM for the technique presented in [21] and our developed technique.

TABLE V. PSNR VALUES OF EACH TECHNIQUES

Image	**SSIM**	
	Method proposed in (Noore , 2004)	***Proposed technique***
lena	0.8760	0.9997
baboon	0.8259	0,9861
peppers	0.9031	0,9965

The presented results show that the proposed technique gives better results in terms of the invisibility than the others techniques.

In addition, the calculation of the similarity between the original mark and the detected mark after attacks for the techniques presented in [17, 18, 19, 20, 21] and the proposed method shows that our technique is more robust against Gaussian attacks JPEGCompression, wavletcompression since we reaches a similarity value equal to 1.

v. Conclusion

In this paper, we proposed watermarking technique for image (. Jpg, .tif, .gif, .bmp) and which operates in the frequency domain. The time-frequency mapping is done by MDCT transformation. The invisibility of the mark is favored by inserting bits in the LSB of components sought by the JND model. In addition, the 50% overlap in the block size of the MDCT approach has eliminated the blocking artifacts and the quality of the watermarked image is greatly improved. The duplication of bits of the mark throughout the image increases the robustness of the technique against attacks and allows also having a high capacity of insertion. This important capability of insertion does not affect the quality of the image. In addition, the original brand is well identified in the detection phase (we reached a similarity value NC equal to 1). This detection is improved by using of Hamming coding.

References

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems Journal, vol. 35, pp. 313–336, 1996.

[2] G. Doërr and J-L. Dugelay, "Problèmatique de la collusion en Tatouage Vidéo," vol. 22, no.6, pages 563-574, 2005.

[3] W. N. Cheung, "Digital image watermarking in spatial and transform domains," in Proc. TENCON 2000, vol. 3, September 2000, pp. 374 – 378.

[4] P. Bassia and I. Pitas, "Robust audio watermarking in the time domain," In Proceedings EUSIPCO 98, Rodos, Greece, 1998, vol. 1, pp. 25-28,.

[5] T. Liu, Z.-D. Qiu, "The survey of digital watermarking-based image authentication techniques," in Proc. 6th Intl. Conf. on Signal Processing, vol.2, pp. 1556-1559, 2002.

[6] Y. Kelkar, H. Shaikh and M.I. Khan," Analysis of Robustness of Hybrid Digital Image Watermarking Technique under Various Attacks," In nternational Journal of Computer Science and Mobile Computing, IIJCSMC, Vol. 2, Issue. 3,pp.137-143.March 2013

[7] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, "DCT-based watermarking recovering without restoring to the uncorrupted original image," in Proc. IEEE Intl. Conference on Image Processing, vol. 1, 1997, pp.520-523.

[8] Y. Wang, J. F. Doherty and R. E. Van Dyck, "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images", IEEE Transactions on Image Processing, 2002, Vol. 11, Issue 2, pp. 77-88.

[9] J. Hernandez, M. Amado, F. Perez, "DCT Domain Watermarking Techniques for Still Images: Detector Performance analysis and new structure," IEEE Transactions on Image Processing, 2000, Vol. 9, No.1, pp. 55 – 68.

[10] C.Mu-Huo, H .Yu-Hsin," Fast IMDCT and MDCT algorithms— A matrix approach," IEEE Trans Signal Process, 2003,pp. 221-229.

[11] R.W. Hamming. Error detecting and error correcting codes. Bell Syst. Tech. J. 26 (2), pages 147–160, 1950.

[12] L. Man, K.N.Ngan,F. Zhang,S. Li,"AdaptiveBlock-sizeTransformbasedJust-NoticeableDifference model forimages/videos," SignalProcessing: Image Communication, 2011,pp 162-174.

[13] Weber'sLawofJustNoticeableDifferences,/http://www.usd.edu/ psyc301/WebersLaw.htmS.

[14] S. Pereira, S. Voloshynovskiy, M. Madueno, S. Marchand-Maillet and T. Puns,"Second generation benchmarking and application oriented evaluation," IHW '01 Proceedings of the 4th International Workshop on Information Hiding, 2001,pp 340-353.

[15] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: From error measurement to structural similarity," IEEE Trans. Image Processing, 2004, vol. 13, no. 1.

[16] CH. Tung and Ja. Ling, "Digital watermarking for video", 13th International Conference on Digital signal Processing, DSP 97, 2-3 Jul 1997,Vol.1, pp. 217 -220.

[17] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Trans. Image Processing, Dec.1997, vol. 6, no. 12, pp. 1673-1687.

[18] C. T. Hsu and J. L. Wu, "Hidden Digital Watermarks in Images," IEEE Trans.Image Processing, 1999, vol. 8, pp. 58-68.

[19] X. Xia, C. Boncelet, and G. Arce, "Multiresolution Watermark for Digital Images," in Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. 1, pp. 548-551.

[20] J. R. Kim and Y. S. Moon, "A Robust Wavelet-Based Digital Watermark Using Level-Adaptive Thresholding," in Proc. 6th IEEE Intl. Conf. on Image Processing, Kobe, Japan ,Oct. 1999,pp. 202.

[21] A. Noore, " An Improved Method to Watermark Images sensitive to Blocking Artifacts," International Journal of Signal Processing, Vol.1, no. 3, 2004.