Side-Informed Image Watermarking Scheme Based on Dither Modulation in the Frequency Domain

Osama Hosam*

The City for Scientific Research and Technology Applications, IRI, Alexandria, Egypt

Abstract: Digital communication and media sharing have extensively increased in the last couple of years. Research is focused on protecting digital media through copyright protection. The digital media is secured by watermarking. We have developed an image watermarking technique in the frequency domain to hide secure information in the Discrete Cosine Transform (DCT) coefficients of the carrier image. DCT coefficients are modulated by Dither Modulation (DM). We have increased the modulation step to be able to entirely recover the embedded data (watermark) and increase the robustness of our proposed algorithm to affine transforms and geometrical attacks. Our algorithm showed lower complexity and robustness against different attacks.

Keywords: Watermarking, DCT, side-informed, decoding, encoding, attack, robustness.

1. INTRODUCTION

Steganography is the art of hiding data into digital carriers. Steganography is used mainly in secure communication. Watermarking is a small branch of steganography. The watermark is embedded into the digital carrier to make it robust to different types of attacks. Even if the watermark is visible to some algorithms, it must be robust to the degree that makes it impossible for the attacker to use the digital carrier after successfully removing the watermark.

Watermarking research started in 1990 [1], watermarking is mainly used for copyright protection such as protecting governmental documents [2]. The massive production of communication technologies and the insecurity of transferring digital data in digital channels made it urgent to find a method to protect digital media and secure digital communication. Generally, any watermarking technique must have the following properties:

- Imperceptibility: This means embedding the secure information into the digital channel without detection from Human Visual System (HVS) or statistical methods.
- Robustness: This means the watermarking scheme must be robust mainly to affine transforms such as rotation, translation and scaling. In addition, it must be robust to geometrical attacks such as compression and noise addition.

Spatial domain watermarking techniques such as Least Significant Bit (LSB) are easily detected by Steganalysis tools [3]. Extensive approaches in literature concentrate on embedding the watermark in the frequency domain. Li and Wang [4] presented watermarking approach that modifies the quantization table of JPEG compression and inserts the secure data into the middle frequency coefficients. They paid attention to increases the payload; their new version of quantization table provides 36 coefficients in each 8x8 block. Watermarking based on DCT (Discrete Cosine Transform)of JPEG compression contains several stages, JPEG compression is shown in (Fig. **1**). Watermarking is done in the quantization step to avoid losing the secure data.

In [5], the authors embedded the watermark by applying dual domain transforms into the carrier image. However, such techniques increased capacity but are still more complex to be implemented. Watermarking scheme based on Scalar Costa Scheme (SCS) is presented in [6]. The author changed the random Codebooks of the Costa scheme which is presented in [7] with lattice-structured Codebooks in order to reduce complexity. The author also implemented a scheme independent of the host signal distribution. The author supposed independent and identically distributed(IID) signal and considered only the White-Gaussian-Noise (WGN) attack so that the scheme can be measured only by using Window to Noise Ratio(WNR).

In this paper, we proposed watermarking technique based on Quantization Index Modulation (QIM). QIM is a powerful watermarking technique; attention is paid to QIM as a powerful watermarking technique and adopted by researchers in the past ten years for its simplicity [8]. Dither modulation (DM) – is a type of QIM, it will be used for encoding the watermark. Our approach showed simplicity in implementation (The algorithm is presented in a couple lines of code), it showed also robustness to affine and geometrical attacks.

The paper is organized as follows: in section 2, the proposed watermarking technique will be presented. In section 3, the experimental results will be presented to show the performance of the proposed algorithm.

2. THE PROPOSED WATERMARKING TECHNIQUE

The overall idea of the proposed watermarking solution is to extract a set of features from the image. These features

*Address correspondence to this author at the City for Scientific Research and Technology Applications, IRI, Alexandria, Egypt, Tel: +20125966704; Fax: +20125966704; Email: mohandesosama@yahoo.com

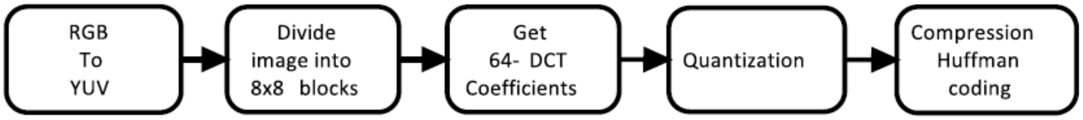

Fig. (1). JPEG compression stages. Watermarking is done in the quantization step of JPEG compression.

are then modulated by DM in the transform domain. The DCT linear transform will be used to extract the coefficients of the image. The description of the two-dimensional DCT [9] for the input image F and output image T is calculated by:

$$T_{pq} = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} F_{mn} cos\frac{\pi(2m+1)p}{2M} cos\frac{\pi(2n+1)q}{2N} \qquad (1)$$

Where

$0 \leq p \leq M-1$
$0 \leq q \leq N-1$

And

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}}, p = 0 \\ \frac{\sqrt{2}}{M}, 1 \leq p \leq M-1 \end{cases} \qquad \alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, q = 0 \\ \frac{\sqrt{2}}{N}, 1 \leq q \leq N-1 \end{cases}$$

Where *M, N* are the dimensions of the input image, *m,n* are the values ranging from 0 to *M-1* and 0 to *N-1* respectively.

DCT coefficients will be modulated by using Dither modulation. The watermarked image will be obtained by getting the inverse of the modulated coefficients. To extract the watermark, we extract the positions of the carrier features from the stego-image. These features are obtained by applying DCT on the watermarked image, the positions which hold the watermark bits will be scanned until the length of the watermark is reached.

The decoding and encoding phases of the proposed algorithm are depicted in (Fig. **2**). In the next subsections we are going to introduce the encoding and the decoding phases in detail.

2.1. The Function for Extracting the Image Features

There are many transforms used to extract the image features in the frequency domain. The most common transform is the DCT linear transform. The main objective of the proposed approach is to slightly change the DCT coefficients by using one of the side-informed image watermarking techniques. Because of the slight change, perturbation will be noticed in the image after watermarking. However, watermarking in the frequency domain is more robust than the traditional spatial domain embedding methods such as LSB. Fig. (**3**) shows the DCT transform of the Lena image. The high frequencies are located in the lower right corner of the image, changing them will dramatically change the quality of the watermarked image. The low frequencies are located in the upper left corner of the image, changing them will not affect the watermarked image.

Our feature extraction procedure is going to sort the coefficients in descending order. The feature vector contains a number of coefficients equal to the size of the watermark.

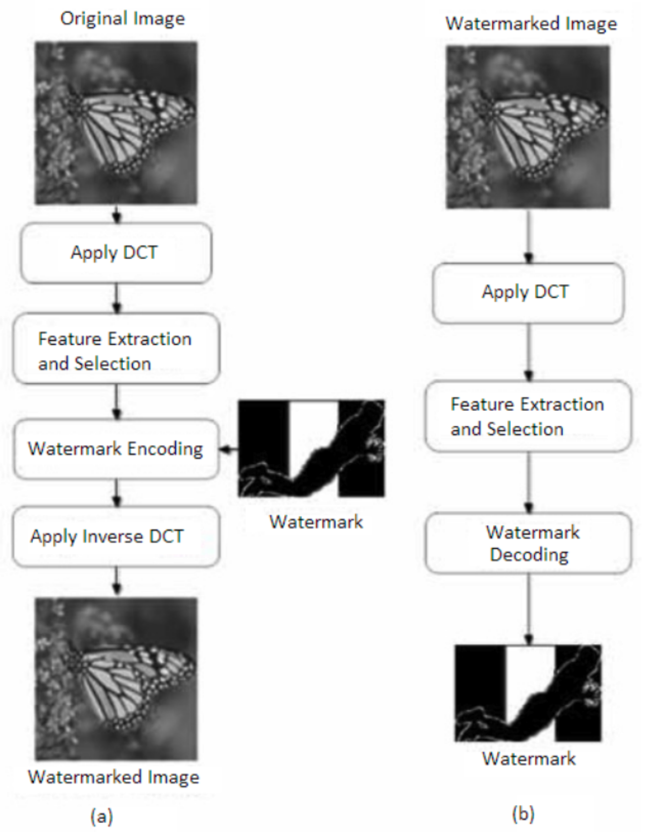

Fig. (2). The proposed Watermark (**a**) Encoding and (**b**) Decoding algorithms.

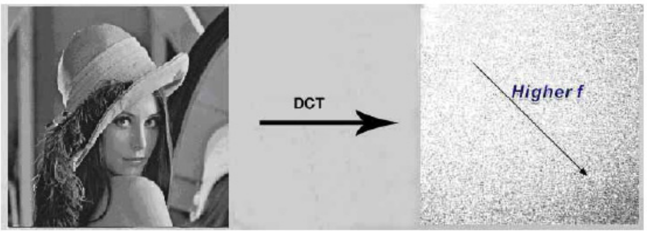

Fig. (3). The DCT transform of the Lena image showing that the absolute values of the coefficients corresponding to the low frequencies are higher and appear in the up-left corner of the square, while high frequency coefficients appear in down-right with lower absolute values.

2.2. Watermark Encoding by Using a Side-Informed Watermarking Scheme

QIM (Quantization Index Modulation) is selected as a side-informed watermarking scheme. The main idea of QIM is to move x to the centroid of the nearest decision region. In case of noise addition, the embedded watermark will not be affected since the change will sway x around the center of the region, probably x will not move to another region after attack. Dither modulation is the shifted version of the basic quantizer.

- If c is the centroid for logic 1 then c + d is the centroid of logic 0.

The basic quantizer will be uniform with quantization step S = 2d and d is the dither value.

The watermark encoder is depicted in Algorithm **1**.

Algorithm 1: Watermark Encoder

```
Read the watermark
Calculate watermark size wmsz
Read the host image
Assign quantization step S with suitable value (application dependent)
Get DCT of the host image
Extract X vector containing the largest coefficients, number of f =wmsz
For each feature f in X
    Get the next bit to be embedded Wi
    Calculate the integer quotient Q and the remainder R in the following way [10]
    $Q = \frac{f}{S}$
    R=f%S Where % is the modulo operator
    Make Q%S =Wi Always hold by applying the following equation
    $f' = \begin{cases} Q\times S + \frac{S}{2} & if\ Q\%2 = Wi \\ Q\times S - \frac{S}{2} & if\ Q\%2 = 1 - Wi\ and\ R < \frac{S}{2} \\ Q\times S + \frac{3S}{2} & if\ Q\%2 = 1 - Wi\ and\ R \geq \frac{S}{2} \end{cases}$
    Where f' is then new value of the feature.
end for
Get the watermarked image by DCT inverse.
```

So, to embed one bit value *Wi*, we shifted the centroid position of the feature f so that Q is an even value for the bit value 0, or an odd value for 1.

2.3. Watermark Decoding

The decoding process starts by taking the DCT of the watermarked image. The DCT of the watermarked image will be explored to extract the watermark bits. The decoding algorithm is depicted in Algorithm **2**.

Algorithm 2: Watermark Decoder

```
Read the watermarked image
Get DCT of the watermarked image
Extract X vector containing the coefficients which carried the watermark bits
For each feature f in X
    Get the next bit by the following equation
     Wi=Q%2
end for
```

3. EXPERIMENTAL RESULTS AND DISCUSSION

The experiments and results are tested on the University of California image database [11]. A description of the dataset will be introduced then we will explore the effect of Host to Watermark Ratio (HWR) on the quality of the image. JPEG compression affects the decoding process and decreases the ability of extracting the watermark. JPEG compression will be plotted with respect to WNR and with different capacity. Finally, our algorithm will be tested for robustness against different attacks.

3.1. Dataset Description

We have used a set of images downloaded from the University of Southern California [11]. The miscellaneous volume of the database consists of 44 images, 16 colors and 28 monochromes. The sizes are fourteen images of size 256x256, twenty six images of size 512x512, and four images of size 1024x1024.We have implemented our algorithm by using MATLAB R2009a, in the algorithm we have resized all the datasets to be 512x512; and for colored images we converted them from RGB to gray-scale images. Each experiment is applied on all the datasets. We have displayed the average results for each experiment. So the curves, tables and figures are not showing the actual result of specific image, they show the average result after applying the algorithm on all images in the dataset.

3.2. The Effect of HWR on the Visibility of the Watermark

Two power ratios are important in the context of watermark embedding [12]. The **HWR** is a measure for the embedding power of the watermark:

$$HWR = \frac{\sigma_s^2}{\sigma_w^2} \quad \text{or} \quad HWR_{dB} = \frac{10\log\left(\sigma_s^2\right)}{\sigma_w^2} dB \tag{2}$$

It should be kept as high as possible to guarantee a negligible perceptibility of the watermark w. The **WNR** characterizes the watermark channel quality

$$WNR = \frac{\sigma_w^2}{\sigma_n^2} \quad \text{or} \quad WNR_{dB} = \frac{10\log\left(\sigma_w^2\right)}{\sigma_n^2} dB \tag{3}$$

We have applied the above function on samples of the dataset after watermarking them with the watermark in (Fig. **2**), we found **HWR** =31 dB.

In Fig. (**4**) if HWR is increased, it will have an effect on increasing the visibility of the watermark in the host image. i.e. decreasing the quality of the host image. So, it is approximately linear relationship.

3.3. The Effect of JPEG Compression with Different Quality Factors on the Watermark

JPEG compression affects the quality of the decoding process. In Fig. (**5a**), for quality factors between 5 and 80 there is little change in WNR. For values more than 80, WNR rapidly increases. All analyse are applied on the images with HWR=15 dB. If we consider capacity in our experiment, as shown in (Fig. **5b**), we notice that, Increasing bit capacity degrades the extracted watermark. For high quality factor and low capacity, the decoding process has less probability of error. However, for high capacity and low JPEG quality factor the extracted watermark is extensively degraded.

3.4. Robustness of the Proposed Encoding Technique Against Different Attacks

Our proposed watermarking scheme is robust to affine transforms such as, rotation, scaling and translation. With

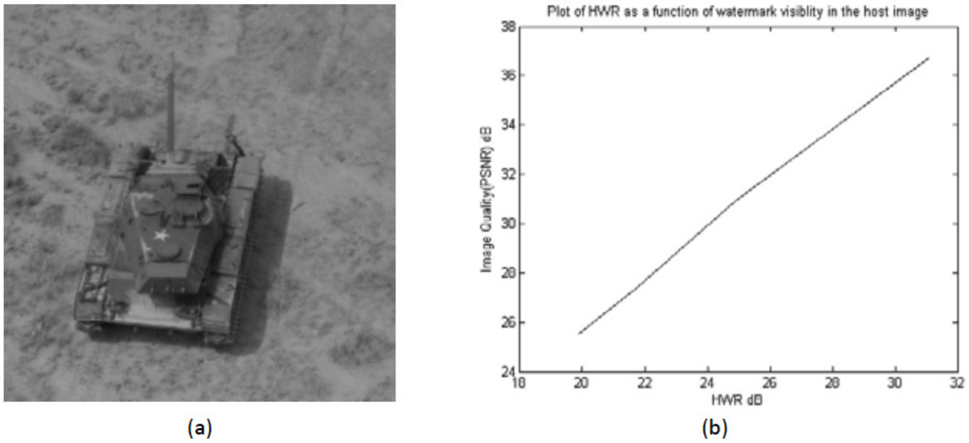

Fig. (4). Visibility of the watermark in the host image as a function of HWR (**a**) The image with embedded watermark HWR=31 db (**b**) The general trend of the changing of HWR with respect to image quality.

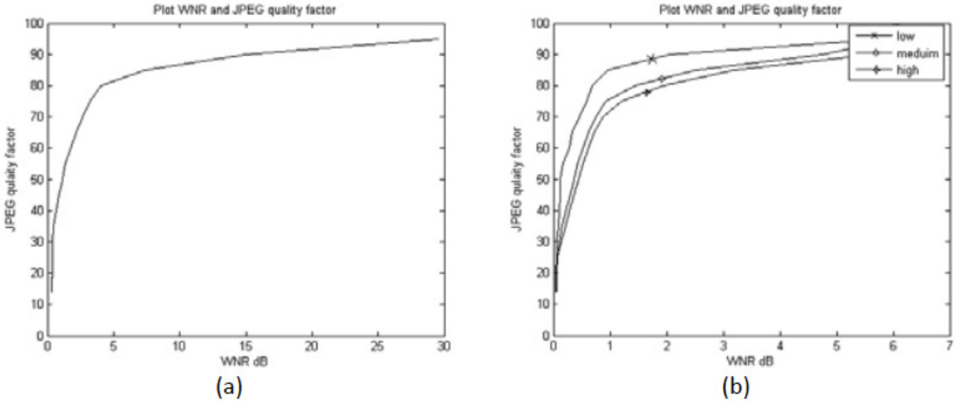

Fig. (5). The effect of JPEG compression, (**a**) with different compression quality factors, (**b**) with different capacity levels.

affine transforms, the image intensity is not changed and hence DCT and inverse DCT feature extraction will not be affected. The only thing we need is to locate the carrier coefficients; this is done in one of two ways, either to make the watermarking non-blind and use the original image in the decoding process, or use extra information embedded in the image about the location of the carrier coefficients. Peak Signal to Noise Ratio (PSNR) is used as a measurement of the image quality after different attacks.

PSNR can be defined by using the mean square error (MSE). Given m×n monochrome image *I* and the image after attack *Is,* MSE is defined as

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - Is(i,j)]^2 \qquad (4)$$

The PSNR is defined as:

$$PSNR = 10.log_{10}\left(\frac{255}{MSE}\right) \qquad (5)$$

Here, 255 is the maximum possible pixel value of the image represented using 8 bits per sample

PSNR can be represented in the compact form as:

$$PSNR = \frac{\sigma_s^2}{\sigma_n^2} \qquad \text{or} \qquad PSNR_{dB} = \frac{10\log\left(\sigma_s^2\right)}{\sigma_n^2}dB \qquad (6)$$

As shown in Table **1**, for scaling attack, the watermark is not affected at all. For cropping attack, the algorithm is not robust, the image intensity will be changed and all its components and features will be different in the DCT and inverse DCT feature extraction. The locations of the carrier features are lost and the quality of the image is also affected. For JPEG compression with quality factor 80% (expressed in the table as attack=0.2 or 20%), most components of the image features are not affected and the decoding process can successfully recover more than 99% of the watermark. As JPEG compression quality decreased the recovered watermark is negatively affected, but still the recovered logo can be distinguished and identified. For noise addition such as adding Salt & Pepper noise and Gaussian noise, the watermarking algorithm is robust, more than 80% of the watermark can be recovered and the watermark can be easily identified.

3.5. Performance Comparison of the Proposed Technique

The authors in [5, 8] proposed a similar technique but with increased levels of embedding. However, they increased the complexity of their approach by watermarking in dual transform domain. We have reduced the complexity of the algorithm by embedding only in DCT domain. The execution time is reduced compared to previous approaches.

Table **2** lists the comparison between the selected previous approaches and the proposed approach. The algorithms

Table 1. The Robustness of the Proposed Algorithm Against Attacks

Attack name	Attack factor	Robust?	Percentage of the extracted watermark	PSNR(dB)
Scale	2	Yes	100	56.23
	0.5		100	56.23
Cropping	0.4	No	12.44	31.34
	0.5		11.30	30.12
	0.6		6.51	18.34
JPEG compression	0.2	Yes	99.89	54.23
	0.5		67.42	50.29
	0.9		61.34	47.98
Noise addition (Salt & Pepper)	0. 2	Yes	72.59	32.53
	0.02		96.29	42.49
	0.002		99.66	52.72
Noise addition (Gaussian)	0.02	Yes	65.13	37. 19
	0.002		81.19	47. 95
	0.0002		92.65	51. 28

Table 2. Time Complexity Comparison with Previous Approaches

	The algorithm in [8]		**The algorithm in [5]**		**The proposed algorithm**	
	Watermark encoding	Watermark decoding	Watermark encoding	Watermark decoding	Watermark encoding	Watermark decoding
Time in mSeconds	0.0931	0.0244	0.1378	0.0656	0.0114	0.0023

are tested on a Personal Computer with Pentium IV processor. We noticed that normally decoding phase takes less time than encoding phase. And our approach has time complexity less than that of previous approaches.

4. CONCLUSION

A side informed image watermarking technique in the frequency domain is presented. The DCT coefficients are perturbed by DM modulation to embed the watermark. The algorithm is simply implemented (its decoding phase is a single line). In addition, the algorithm is robust to affine transforms such as, rotation and scaling, also it is robust to JPEG compression and noise addition (Salt and Pepper, Gaussian Noise). The algorithm is not robust to cropping attack since the locations of the carrier coefficients are lost and the image is totally degraded after extracting the DCT features. In future work we are planning to improve our algorithm to be robust against cropping attack.

CONFLICT OF INTEREST

The author(s) confirm that this article content has no conflicts of interest.

ACKNOWLEDGEMENT

Thanks to Dr. Sameh Dakroury for his effort in explaining the mathematics related to the paper, also many thanks to my wife for her everlasting support.

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", *IBM. Syst. J.,* vol. 35, pp. 313-335, 1996.

[2] D. Rosiyadi, S. Horng, P. Fan, X. Wang, M.K. Khan, and Y. Pan, “Copyright protection for e-government document images”, *IEEE Multi Media.*, vol. 19, no. 3, pp. 62-73, 2012.

[3] O. Hosam, and A.S. Alraddadi, "Novel image watermarking technique based on adjacent pixel position switch", *JNI.T*, vol. 4, no. 3, pp. 81-88, 2013.

[4] X. Li, and J. Wang, “A steganographic method based upon JPEG and particle swarm optimization algorithm”, *Inform. Sci.*, vol. 177, no. 15, pp. 3099-31091, 2007.

[5] S. Wang, X. Zhang, and T. Ma, “Image watermarking using dither modulation in dual-transform domain”, *J. Image Soc. Jpn.*, vol. 41, no. 4, pp. 398-402, 2002.

[6] J.J. Eggers, J.K. Su, and B. Girod, "A blind watermarking scheme based on structured codebooks," IEE Colloquium on secure images and image authentication, London, UK, April 2000, pp. 20-26.

[7] M. H. M. Costa, “Writing on dirty paper*”, IEEE Trans. Inform. Theor.,* vol. 29, no. 3, pp. 439-441, 1983.

[8] F. Bartolini, M. Barni, and A. Piva, "Performance analysis of ST-DM watermarking in presence of non-additive attacks", *IEEE Trans. Signal Process.,* vol. 52, no. 10, pp. 2965-2974, 2004.

[9] A. Cheddad, J. Condell, K. Curran, P. McKevitt, "Digital image steganography: Survey and analysis of the current methods", *Signal Process.,* vol. 90, pp. 727-752, 2010.

[10] H. Wu, Y. Cheung, "A fragile watermarking scheme for 3D meshes" Proceedings of the 7th workshop on Multimedia & Security, New York, NY, USA 2005 pp. 43-47.

[11] University of southern California, (SIPI) Signal and Image processing Institute, Ming Hsieh Department of Electrical Engineering, Miscellaneous images Database, http://sipi.usc.edu /database /?volume =misc&image=12,updated May 2013.

[12] B. Geiser, P. Jax, P. Vary, "Artificial bandwidth extension of speech supported by watermark-transmitted side information". In the proceeding of INTERSPEECH September 2005, pp. 1497-1500.

Received: September 24, 2013 Revised: October 22, 2013 Accepted: November 29, 2013