An Efficient Image Watermarking Approach based on Fourier Transform

Methaq T. Gaata, PhD
Computer Science Department,
University of Mustansiriyah,
Baghdad, Iraq

ABSTRACT
Currently, inserting of the watermarking information into various multimedia files represent important research area. The objective is to insert the watermark with less perceived distortions in order to achieve copyright protection and authenticity. This paper presents a new image watermarking approach based on Fourier transform and characteristics of vision system. In fact, the proposed approach exploits the areas that produce after applied the Fourier transform on the images in order to select of appropriate coefficients to store the watermark bits. The original image is partitioned into the non-overlapping blocks. Watermark bits are inserted within the selected coefficients of each block depending on certain condition. The performance of the proposed watermarking approach is evaluated in terms of quality and robustness with many of statistical measures. Experimental results illustrate that the proposed approach can be optimal compromise to solve conflict problem between quality and robustness. In addition, the proposed approach exhibit good robustness against different types of attacks such as Gaussian noise, Gamma noise, blurring filtering, and sharpness.

Keywords
Digital watermarking, Fourier transform, Color Image.

1. INTRODUCTION
The increasingly easy access to digital multimedia content via public networks as well as the available of many powerful editing techniques provides good chances for creativity, but also for illegal manipulation, reproduce and distributions. Digital watermarking approach represented optimal solution to the pre-defined problem. A watermark is sequence of bits added into text files, digital image, speech signals or video frames that identifies the owner data (author, rights, etc.). The term "watermark" is original from the indistinctly visible labels imprinted on products. The watermarking system can be classified for two main classes are visible and invisible. Visible watermarks are mainly applied to images, for example, to visibly mark preview images available in image databases or on the World Wide Web in order to prevent people from commercial use of such images [1].
The drawbacks of visible watermarks are degrading the quality of image and detect by visual means only. Invisible watermarks are hidden information in digital contents. An authorized person can detect them only [2]. However, this work, will concentrate on invisible image watermarking.
Invisible color image watermarking is the process of inserting information inside a color image where the watermark should not be visible neither should it degrade the visual quality of the image. In general, three basic watermarking procedures are required in digital watermarking and these procedures are watermark insertion, watermark detection and watermark extraction. Watermark insertion requires an original image *(I)*, a watermark *(W)*, and public or secret key *(K)*. The output is the watermarked image *($\bar{I}$)*. The watermark can be of any nature such as a number, text, or an image etc. The key may be used to enforce security that is the prevention of unauthorized parties from recovering and manipulating the watermark. All practical systems may employ at least one key, or even a combination of several keys. In combination with a secret or a public key the watermarking techniques are usually referred to as secret and public watermarking techniques, respectively [3, 4].
In [5] *C. Pun*. proposed a novel system for image watermarking based on DFT. At started, the digital image is transformed into DFT domain using a fast Fourier transform in order to reduce the impact on the image fidelity, the watermark data are embedded into DFT coefficients with highest magnitudes. But, watermark robustness is not take in account for all attacks types.
In [6] *A. Poljicak et al.* developed a watermarking strategy that chooses the optimal radius of the implementation to minimize quality degradation. It employ Fourier transform in order to embedded watermark in magnitudes of the original image. The performance of the proposed strategy was evaluated for quality and robustness with many of reference images. Detection rates and receiver operating characteristic performance confirmed acceptable robustness against the many common attacks which are found in the popular StirMark benchmark platform.
In [7] *X. Wanga et al.*, proposed a robust blind color image watermarking based on quaternion Fourier transform and least squares support vector machine (LS-SVM), which has good visual quality. In [8] *R. Jain et al.*, developed algorithm to implemented digital image watermarking using hybrid 3-level DWT-FFT technique via image compression for better results compared with others.
The paper is structured as follows. The proposed approach for design of image watermarking is presented in Section 2. Section 3 shows obtained experimental results. Finally, Section 4 provides conclusions.

2. THE PROPOSED WATERMARKING APPROACH
In this section, image watermarking approach is proposed based on DFT to hide the watermark information into the color image without degrade the visual quality of the image. The major goal of proposed watermarking approach is insert the watermark information into color image without sensitively degradation and robust against common attacks. Therefore, the hiding coefficients should selected in carefully. The main steps of the proposed watermarking approach is shown in Figure 1.

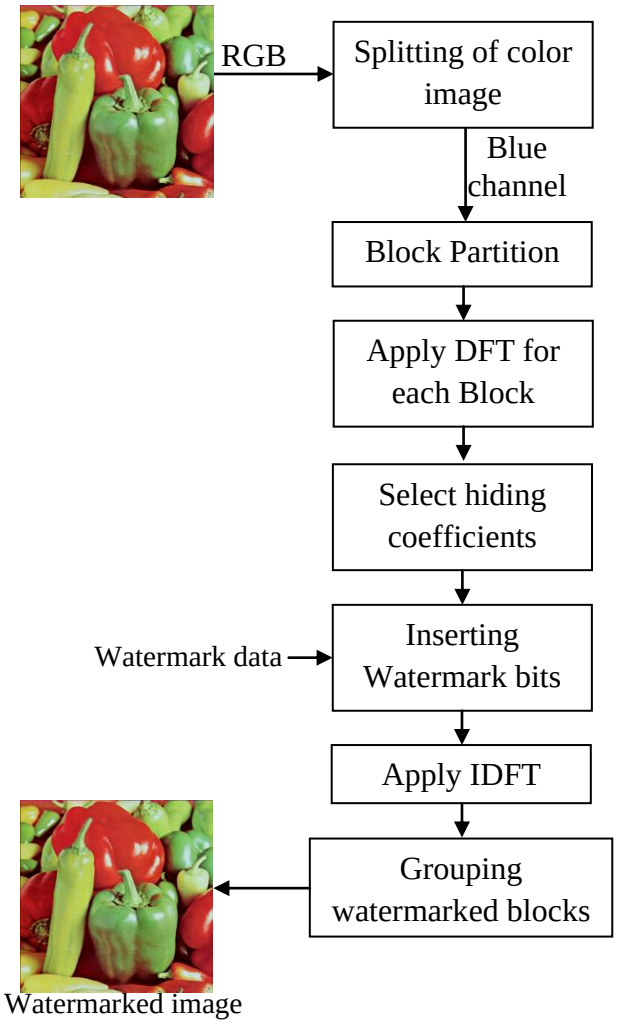


Fig 1: The main steps of proposed color image watermarking approach

2.1 Host Image

The input for the proposed watermarking approach is a 24-bits color image which is got from USC-SIPI image database [9]. In the proposed approach, the color image used during watermark hiding process to store watermark bits. The each host image with size of 256×256 pixels . Figure 2 shows one example of host color image.

Fig 2: Example of host color image 'house'.

2.2 Splitting of Color Image

In this step, the color image channels are separated into three independent channels included Red, Green, and Blue. After that, the blue channel is used for store the watermark bits. Because of the changes in blue color are less sensitive to the human vision system. The data of other channels are saved in the pre-define buffer to used for the reconstruct watermarked image in last step.

2.3 Block Partition

As Known the Fourier transform is mathematically complex when it is applied to the whole image. therefore, the blue channel of color image is partitioned into non-overlapping blocks and the size of each block is 16x16 pixels. All blocks arranging from left to right, top to bottom before assigning labels to each block. In the next steps each block processed as independent sub-image.

2.4 Discrete Fourier Transform

As stated earlier, that our main objective is to hide the watermark in imperceptible and robust manner. To achieve this, it have to hide the watermark bits with frequency domain instead of the spatial domain. So, the strength of the watermark is spread over the whole image after the inverse image data to the spatial domain, which produces the robust watermarking approach with less observed changes.

Here, the 2-D DFT applied on each block B(x,y) of size 16 x 16 pixels. In the DFT image, each pixel is represent a specific frequency which contain complex number that can expressed with two components are magnitude and phase. The watermark bits are hidden in a host image in the selected magnitude coefficients of the DFT.

2.5 Select Hiding Coefficients

After completed apply DFT on each block in sequential order. Then we require to select which the magnitude coefficients will used to embedding the watermark bits in frequency domain. When we choose the appropriate coefficients to hide the watermark bits some challenges must be facing. If the watermark bits was are hidden into the lowest coefficients, it maybe cause significant annoyance to the watermarked image. But, if it were hidden into the highest coefficients it possible to eliminated by using one of common image processing operations such as filtering, compression, or cropping. For that reason, watermark bits will hide into middles coefficients as optimal trade-off between quality and robustness factors. In addition to that, the secret key will be used to distribute watermark bits among selected coefficients in semi-random way.

2.6 Hiding of Watermark Bits

The main aim of this step is hide a watermark bits into the selected middles coefficients of blue channel from host image. To implement this goal, we require to represent the watermark information to series of binary form (0 and 1). The watermark bits insert to selected coefficients by modify the particular bit of the magnitude coefficients. The algorithm of proposed image watermarking approach as follow:

Input: Color image, watermark information, and secret key. **Output:** Color watermarked image
Begin Step 1: Read color image and keep pixels values to buffer. Step 2: Split color image channels into three independent channels (Red, Green, and Blue). Step 3: Partition the blue channel into the non-overlapping

blocks (16x16).
Step 4: Arranged the blocks in ascending order and assign label for each one.
Step 5: Perform 2D DFT for the each independent block B(x,y).
Step 6: Select hiding coefficients (middles coefficients just) in each block.
Step 7: Read the watermark information and represented it in the binary representation.
Step 8: Hide the watermark bits into coefficients which are selected in step (7), and use secret key to distribute watermark bits in semi-random way.
Step 9: Apply the inverse DFT for each block.
Step 10: Rearranged the blocks to regenerated the blue channel.
Step 11: Concatenates the three channels (Red, Green, and Blue) to construct the color watermarked image.
End.

2.7 Watermark Extraction

The watermark extraction steps taken the same sequence of the watermark hiding steps. The watermark extraction steps are executed as follow: First, the color watermarked image split into three channels. Second, the blue channel of watermarked image partition into non-overlapping blocks. Third, arranged the blocks in ascending order. Forth, Apply the DFT on each block. Last, extract the watermark bits from magnitude coefficients which are determining during steps of watermarking hiding.

3. EXPERIMENTAL RESULTS

The proposed watermarking approach is tested on a variety of reference test images and different attacks. Two important requirements are imperceptibility and robustness which are considered in the performance evaluation of the proposed watermarking approach. Imperceptibility means is not possible to note the presence of the watermark information in the watermarked image and preserve its quality without degraded perceptible. While, the robustness means the strength of the watermark in the to resist the intentionally and unintentionally attacks. About quality evaluation, two quality measures are used to do that. First measure is Peak-Signal-to-Noise-Ratio (PSNR) which usually used to calculate the variation for two images depends on differences of pixel values. For an image with size of N×M pixels, PSNR is calculated as [10]:

$$PSNR(\text{dB}) = 10\log_{10}\left(\frac{255}{RMSE}\right)^2, \quad ...(1)$$

where RMSE is the root mean square error.

The second of objective quality metric is Structural SIMilarity (SSIM) which consistent with HVS. The SSIM is based on a top-down hypothesis that consider HVS is very adapted to structural information which are extracting from the image, and therefore a calculate of structural similarity must be a good estimate of image quality. The SSIM is defined as [11]:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}, \quad ...(2)$$

where μ_x and μ_y are the mean of the original image x and the watermarked image y, σ_x^2 and σ_y^2 represents the variance of the original image x and the watermarked image y, and σ_{xy} is the covariance between x and y. While, c_1 and c_2 are two constants to stabilize the division with weak denominator.

Figure 3 shows the original color images and corresponding watermarked images after insert the watermark information using proposed approach.

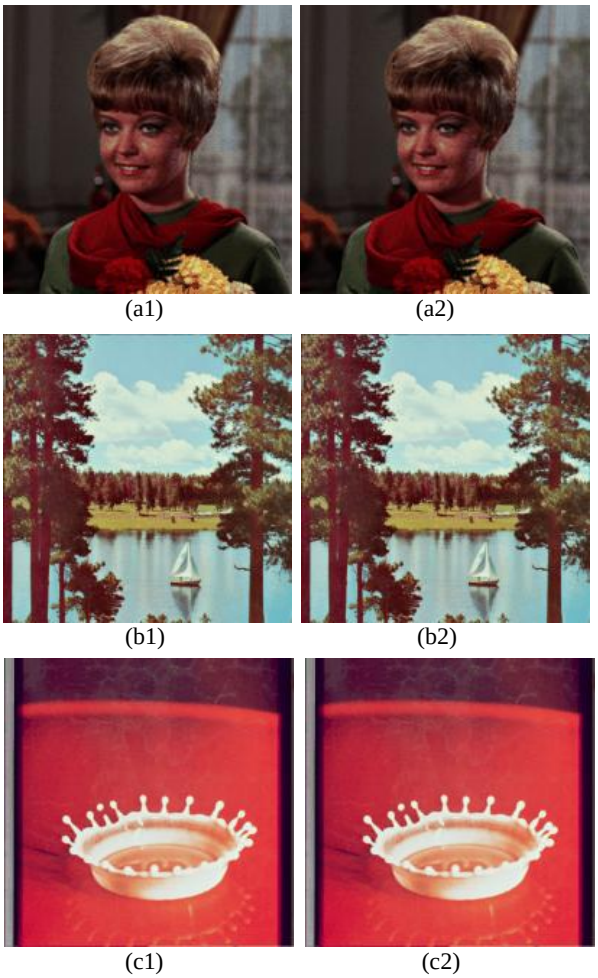


Fig 3: (a1, b1, c1) Original images, (a1, b2, c2) Watermarked images

As noted in Figure 3, the watermarked images that produced after hide the watermark bits in selected coefficients have high degree of image quality and can be hardly distinguished from the original version. The results of quality evaluation based on watermarking approach by using two measures PSNR and SSIM presents in Table 1.

Table 1: Quality evaluation

Watermarked images	Quality Measure	
	PSNR (dB)	SSIM
a2	48.445	0.923
b2	51.34	0.940
c2	43.428	0.853

It can noted in Table 1, the watermarked image (b2) has high quality degree than other images due to this image consist of texture details more than two other images. This means the hiding watermark bits in smooth images give quality degree with low level.
On the other hand, different attacks which available in Checkmark and Stirmark benchmarks have been used in order

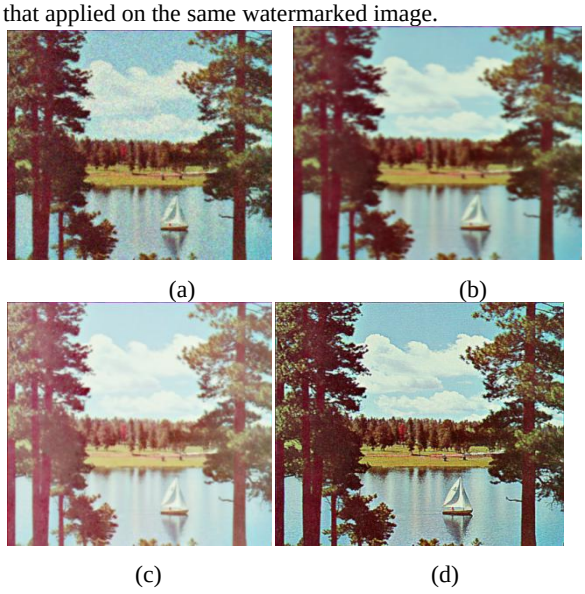
to evaluate robustness of the proposed watermarking approach. After apply each attack, the watermark information which extracted from attacked image are comparing with watermark information which inserted in original version. In this experiment, the Hamming distance computed between of the extracted and the referenced watermarks in binary form. The dissimilarity index represent the number of different bits between two sequences, the formula which computes dissimilarity is defined as [12]:

$$DH(x,y) = \frac{\sum_{i=1}^{n} S(x_i, y_i)}{L}, \quad \ldots(3)$$

where

$$S(x_i, y_i) = \begin{cases} 0 & \text{if } S(x_i = y_i) \\ 1 & \text{if } S(x_i \neq y_i) \end{cases}$$

In order to test the robustness of proposed watermarking approach many kinds of common attacks have been used. After, the watermarked image pass through one kind of attacks then the attacked image is produced. Both watermarked image and its attacked version are taken in account to make a decision about the robustness of watermark. Evaluation of proposed watermarking approach is done with several color images which are play the role of host image. Images were selected randomly from the USC-SIPI image database. Figure 4 presents the four kinds of attacks that applied on the same watermarked image.



(a) (b)

(c) (d)

Fig 4: The attacked images. a) Gaussian noise, b) Blurring filtering, c) Sharpness, d) Gamma noise

As noted in Figure 4, the four types of attacks has been applied on the watermarked image including: Gaussian noise, blurring filtering, sharpness, gamma noise. The result of robustness evaluation is stated in Table 2.

Table 2: robustness evaluation

Attack Types	Hamming distance
Gaussian noise	0.314
Blurring filtering	0.185
Sharpness	0.091
Gamma noise	0.263

Evaluation results illustrate that the effect of the Gaussian noise is more annoying attack than other types.

4. CONCLUSIONS

In this paper, image watermarking approach based on Fourier transform have been proposed. This approach can be used for protection of image copyright. Experimental results explain that the amount of distortion due to inserting the watermark information is very little and difficult to be recognize. So, the proposed image watermarking approach can provide a good adjustment between the both quality and robustness. Also, the robustness of proposed approach is strong against some common attacks such as: Blurring filtering, sharpness, gamma noise. In Future work, the focus is placed on add high degree of robustness against other types of attacks and enhancing the quality level.

5. REFERENCES

[1] M. Swanson, K. MEI, A. Tefik," Multimedia Data-Embedding and Watermarking Technologies," Proceeding of IEEE, VOL. 86, NO. 6, June 1998.

[2] K. Rawat and D. Tomar, "Digital Watermarking Schemes for Authorization Against Copying of Piracy of Color Images, Indian Journal of Computer Science and Engineering, Vol. 1 No. 4 295-300, 2009.

[3] Vipula Singh ,"Digital Watermarking: A Tutorial,"Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), January Edition, 2011.

[4] Ali Benoraira*, Khier Benmahammed and Noureddine Boucenna, "Blind image watermarking technique based on differential embedding in DWT and DCT domains" EURASIP Journal on Advances in Signal Processing 2015.

[5] Chi-Man Pun, "A Novel DFT-based Digital Watermarking System for Images",8th International Conference on Signal Processing, vol.2, 2006.

[6] Ante Poljicak, Lidija Mandic, Darko Agic, "Discrete Fourier transform–based watermarking method with an optimal implementation radius", Journal of Electronic Imaging v0l. 20 no.3, 2011.

[7] Xiang-yang Wanga, Chun-peng Wanga, Hong-ying Yanga, Pan-pan Niua , "A robust blind color image watermarking in quaternion Fourier transform domain," Journal of Systems and Software, Volume 86, Issue 2, February 2013, Pages 255–277.

[8] Reema Jain and Manish Jain,"Digital Image Watermarking using 3-Level DWT and FFT via Image Compression," International Journal of Computer Applications (0975 – 8887) Volume 124 – No.16, August 2015.

[9] The USC-SIPI image database, Allan Weber, database editor. http://sipi.usc.edu/database/

[10] H. Sheikh, M. Sabir and C. Bovik, "A Statistical Evaluation of Recent Full Reference Image Quality Assessment Algorithms," IEEE Trans. on Image Processing, 2006, 15, (11), pp. 3441–3451.

[11] Z. Wang, A. Bovik, H. Sheikh and E.Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," IEEE Transactions on Image Processing, vol. 13, no.4, pp. 600-612, April 2004.

[12] Eric Blais, Joshua Brody, and Badih Ghazi, "The Information Complexity of Hamming Distance", Workshop on Randomization and Computation (RANDOM'2014).