J Inf Process Syst
https://doi.org/10.3745/JIPS.00.0000

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Copyright Protection for Digital Image by Watermarking Technique

Suhad A. Ali*, Majid Jabbar Jawad*, and Mohammed Abdullah Naser*

Abstract

Due to the rapid growth and expansion of the Internet, the digital multimedia such as image, audio and video are available for everyone. Anyone can make unauthorized copying for any digital product. Accordingly, the owner of these products cannot protect his ownership. Unfortunately, this situation will restrict any improvement which can be done on the digital media production in the future. Some procedures have been proposed to protect these products such as cryptography and watermarking techniques. Watermarking means embedding a message such as text, the image is called watermark, yet, in a host such as a text, an image, an audio, or a video, it is called a cover. Watermarking can provide and ensure security, data authentication and copyright protection for the digital media. In this paper, a new watermarking method of still image is proposed for the purpose of copyright protection. The procedure of embedding watermark is done in a transform domain. The discrete cosine transform (DCT) is exploited in the proposed method, where the watermark is embedded in the selected coefficients according to several criteria. With this procedure, the deterioration on the image is minimized to achieve high invisibility. Unlike the traditional techniques, in this paper, a new method is suggested for selecting the best blocks of DCT coefficients. After selecting the best DCT coefficients blocks, the best coefficients in the selected blocks are selected as a host in which the watermark bit is embedded. The coefficients selection is done depending on a weighting function method, where this function exploits the values and locations of the selected coefficients for choosing them. The experimental results proved that the proposed method has produced good imperceptibility and robustness for different types of attacks.

Keywords

Digital Watermarking, Discrete Cosine Transform (DCT), Normalized Correlation (NC), PSNR

1. Introduction

The Internet is very useful technique today. All people can do their jobs digitally during this technique with high efficiency and low-cost. Approximately, all digital media such as text, audio, video, maps are available for everyone. This situation affects the owner of these media. For example, a company 'A' has spent high effort to produce a valuable digital product, a company 'B' can illegally make a copy of this product, a company 'A' cannot prove whether this product is theirs or not. This situation will restrict the growth of producing the digital media in the future. In order to prevent the unauthorized operation on the digital media (copying, tampering, etc.), the researchers proposed

Manuscript received September 29, 2016; accepted January 28, 2017.
Corresponding Author: Suhad A. Ali (wsci.suhad.ahmed@uobabylon.edu.iq)
* Dept. of Computer Science, Faculty of Science for Women, Babylon University, Babylon, Iraq ({wsci.majid.jabbar, wsci.mohammed.abud}@uobabylon.edu.iq)

several techniques. One of these techniques is called watermarking techniques. Watermarking means embedding an object within another one in order to prevent future illegal operation on the digital media. Several watermarking methods have been proposed for text, audio, image, video, etc. [1-4]. This paper is an attempt to design and implement a robust watermarking system for copyright protection of the still image.

The rest of the paper is organized as follows. In Section 2, the related works which have been done in the area of watermarking for still image are discussed. The proposed watermarking method is presented in Section 3. Section 4 illustrates the experimental results and Discussions. The suggestions for future works is represented in Section 5.

2. Related Works

Several works have been proposed in the field of watermarking methods. Approximately, all of these methods are applied in two domains, namely, spatial domain and transform domain. Sometimes the watermarking method is applied by mixing the two domains (spatial and transform). Since the proposed method is applied in a transform domain and uses discrete cosine transform (DCT), some previously proposed methods which are applied in the transform domain and used DCT will be illustrated.

In 2013, Ahmed [5] presented a PhD dissertation for digital watermarking of still images for copyright protection. This thesis presented a novel research work on copyright protection of greyscale and color digital images. In this dissertation, eight algorithms were developed based on the DCT using 1D and 2D Walsh coding. These algorithms used the low frequency coefficients of the 8×8 DCT blocks for embedding the watermark. The experimental results showed an optimal trade-off between perceptual distortion caused by embedding and robustness against certain attacks.

In 2014, El Hossaini et al. [6] presented a new robust digital watermarking algorithm for embedding content into the DCT. The watermark is embedded in low and mid-frequency of DCT components. The experimental results illustrated a good visual imperceptibility and resiliency of the proposed scheme against an intentional and un-intentional variety of attacks, such as geometric attacks, JPEG compression attacks, noise attacks, filtering attacks and enhancement attacks.

In 2014, Ali and Kumar [7] presented a new digital watermarking algorithm for embedding content into the DCT. In the proposed method, the binary image is used as a cover for embedding the watermark. As we know, the embedding in binary image is very difficult due to the characteristics of this image. So, in order to do the embedding operation perfectly, a blurring preprocessing and a biased binarization must be done on the image. After blurring the binary image, the watermark is embedded by modifying the DC components of DCT, followed by a biased binarization. According to the experimental results, the proposed method provided degree of robustness against common signal processing and good imperceptibility.

In 2015, Abdullah et al. [8] proposed a robust watermarking algorithm based on DCT for securing Iris images. Because the security of biometric trait is very important, a robust security must be provided. So, this method is used for protecting the integrity of the iris images using a demographic text as a watermark. The watermark text is embedded in the middle band frequency region of the iris image (in the middle band coefficients pairs of the DCT). The experimental results showed that watermark is robust against several attacks. Also, the results showed that the method do not introduce discernible decrease on iris image quality or biometric recognition performance.

3. Proposed Watermarking Method

In this section, the proposed method is illustrated as follows:

3.1 Evaluating the DCT Coefficients Weights

Before the embedding procedure, the image is divided into 8×8 blocks. Then 2D DCT equation is applied on these blocks. The 2D DCT equation is defined as follows:

$$c(u, v)=\alpha(v)\ \alpha(u)\sum_{x,y=0}^{N-1}\sum f(x,y)cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right] \tag{1}$$

For u, v=0, 1, 2, 3....., N-1 and $\alpha(u)$ and $\alpha(v)$ defined in the following equation [9]:

$$\alpha(u)=\begin{cases}\sqrt{\frac{1}{N}}, & u=0\\ \sqrt{\frac{1}{N}}, & u\neq 0\end{cases} \tag{2}$$

The 2-D DCT inverse transforms is given by:

$$f(x, y)=\sum_{u,v=0}^{N-1}\sum \alpha(v)\alpha(u)c(u,v)cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right] \tag{3}$$

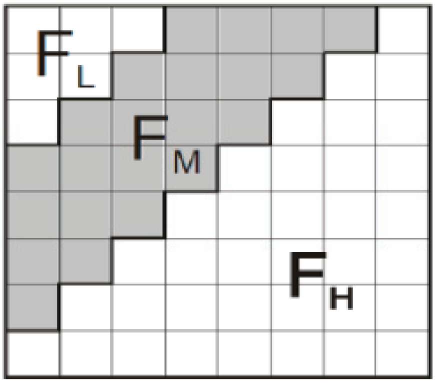


Fig. 1. Low, middle, and high frequency distribution in a DCT block.

As we know, the DCT divides the image into three spectral subbands, each having different importance with respect to the image's visual quality. Fig. 1 shows the DCT bands, namely, low (F_L), middle (F_M), and high (F_H) frequency bands. In most watermarking schermes based on DCT, the researcher selectes one of these three bands for embedding the watermark.

In order to make the watermark more robustness, our method objective is to select the best DCT coefficients for embedding process. These coefficients are found in different bands. It will be selected according to a proposed weighting function, where the coefficients with higher weights will be used for embedding the watermark. In other words, in the embedding process, a best block and best coefficients in this block will be selected.

At first, the standard deviation (σ) of each 8×8 cover image block is computed according to Eq. (4):

$$\sigma_g = \sqrt{\sum_{g=0}^{L-1}(g-\bar{g})^2 p(g)} \tag{4}$$

where *g* is gray value. Only the blocks that satisfy certain condition, where the standard deviation (σ) of cover block that is less than the certain threshold (α), will be selected.

Then the DCT will be applied on the selected blocks (*sb*). The weight evaluation function is implemented on the DCT coefficients of selected blocks, in order to choose the best coefficients (in which the watermark is embedded). The weight evaluation function is illustrated in the following equation.

$$wc(i,j) = 1 - tanh\big(c(i,j)\big) \tag{5}$$

where $c(i, j)$ represents the current DCT coefficient, $c(i, j)$ represents the location of the current DCT coefficient , $wc(i, j)$ represents the weighting value of the current DCT coefficient and then represents the hyperbolic tangent.

After applying the Eq. (5), an array of weights will be obtained. Then *n* of these weights will be used for choosing the best DCT coefficients, (in which the watermark bits will be embedded). The value of n is computed according to the following formula:

$$n = \frac{w*h}{Nsb} \tag{6}$$

where *w*, *h* are the width and height of watermark, and *Nsb* is the number of selected blocks, where the standard deviation (σ) of selected blocks is less than the certain threshold (α).

In order to understand the above procedures, let us take a simple example. Suppose that we have original (spatial) 8×8 block as shown in Fig. 2.

After applying the DCT, the DCT coefficients will be obtained as shown in Fig. 3.

146	144	141	138	135	134	133	133
146	143	140	137	135	134	134	134
144	142	139	136	134	134	134	135
142	140	137	135	133	134	135	136
138	137	136	135	134	134	135	135
133	134	135	136	136	135	135	134
129	131	135	137	138	137	134	132
127	130	135	138	139	137	134	131

Fig. 2. Original (spatial) (8×8 block).

1.0879	0.0122	-0.0003	0.0001	-0.0001	0.0006	0.0003	-0.0000
0.0124	0.0179	0.0139	0.0003	0.0005	-0.0000	0.0002	-0.0005
-0.0002	-0.0001	-0.0079	0.0004	-0.0002	-0.0001	0.0003	0.0003
-0.0004	-0.0001	-0.0000	-0.0002	0.0001	0.0001	-0.0004	0.0001
-0.0001	0.0005	0.0006	-0.0003	-0.0001	0.0003	-0.0001	-0.0003
-0.0001	-0.0002	-0.0002	-0.0000	-0.0002	-0.0003	0.0004	-0.0005
-0.0001	0.0001	-0.0002	-0.0005	-0.0001	-0.0002	-0.0003	-0.0001
-0.0003	0.0003	-0.0006	-0.0001	-0.0002	-0.0002	0.0004	0.0001

Fig. 3. DCT coefficients (8×8 block).

In order to compute the weighting values for above DCT coefficients, Eq. (5) is applied and the following weighting values for each coefficient were obtained. As shown in Fig. 4 illustrates the weight values of each DCT coefficient. Here (as an example), n is set to three. So, three coefficients with highest weights are selected (as shown in bolded form).

0	0.0000	1.2900	0.8674	1.1244	0.4721	0.7466	1.0390
0.0000	0.0000	0.0000	0.7446	0.5639	1.0168	0.8386	**1.4947**
1.419	1.1022	**2.0000**	0.6429	1.1619	1.1423	0.6740	0.6972
1.4115	1.0653	1.0044	1.1802	0.9221	0.8795	1.3466	0.9213
1.1244	0.5477	0.4452	1.2518	1.1244	0.7520	1.1231	1.2576
1.0945	1.1509	1.1642	1.0254	1.2436	1.2545	0.6023	1.4560
1.0675	0.8803	1.1602	1.4921	1.0675	1.1948	1.3134	1.1135
1.2502	0.6984	**1.5237**	1.0564	1.1605	1.1641	0.6500	0.9424

Fig. 4. The weight of DCT coefficients.

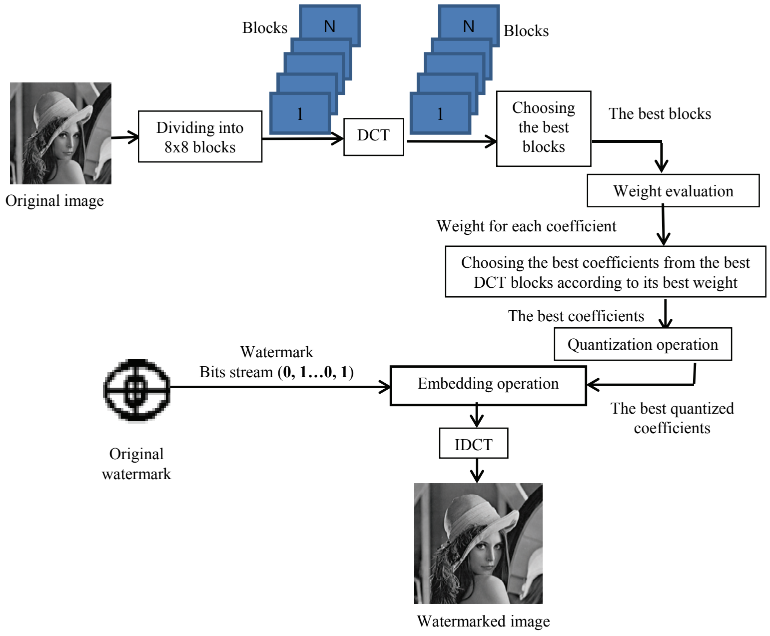


Fig. 5. The embedding process.

Algorithm 1: The embedding algorithm

Input: C, W
(***C***: cover image, ***W*** **:** watermark (*binary image*))
Output: C'
(***C'***: watermarked image)
1: $C_{8\times8(i)} = C$
{subdivide the host image (C) into blocks of 8×8 pixels}
2: $I_{DCT(i)}$ = 2D-DCT ($C_{8\times8(i)}$)
{Compute the 2D-DCT of each 8×8 block of the cover image}
3: Choose the best DCT coefficients blocks
4: apply eq. (5) on all the best DCT coefficients blocks
{***for evaluating the weight for each coefficient within the best blocks***}
5: Choose the best coefficient within all the best DCT coefficients blocks
{ ***coefficient with high weight***}
6: Quantize the best coefficient (qb_s)
{***by applying eq.(7)***}
7: **for** i = 1→size (W) do
{No. of watermark bits}
8: **if** $W_{(i)}$ = 1 then
9: add **v** constant to the DCT coefficient (***which has been chosen as the best according to eq.5 and quantized (qb) according to eq.*** 7) according changing eq. 8
10: **else**
11: subtract **v** constant from the DCT coefficient (***which has been chosen as the best according to eq. 5 and quantized (qb) according to eq.*** *7*) according changing eq.8
12: **end if**
14: **end for**
15: Take inverse DCT to reconstruct C'

3.2 Scaling Factor

The embedding of watermark will be done in selected float of DCT coefficients of higher weights. After that, the DCT block will be converted into spatial domain (IDCT), where each pixel must be in the range [0–255] (gray levels). This conversion from float into integer may affect the watermark. So, scaling factor is used to reserve watermark. Scaling factor is a constant value where all DCT coefficient will divided by it according to the following equation:

$$qb(i,j) = round\left(\frac{c(i,j)}{sf}\right) \tag{7}$$

where $c(i, j)$ represents the DCT coefficient, $qb(i, j)$ represents the DCT quantized coefficient and sf represents scaling factor.

3.3 Embedding Method

The embedding method is shown in the Fig. 5. It is done according to the Eq. (8). The details of the embedding procedure is illustrated in Algorithm 1.

$$c'(i,j) = \begin{cases} qb(i,j) + v & watermark\ bit = 1 \\ qb(i,j) - v & watermark\ bit = 0 \end{cases} \quad (8)$$

where $qb(i, j)$ represents the current quantized DCT coefficient of the original image, $c'(i, j)$ represents the current DCT coefficient of the watermarked image, and v represents constant value.

3.4 Extracting Method

As shown in Fig. 6, the comparison between the watermarked image and the original image is done. If the coefficient of the watermarked image is larger than the coefficient original image, then the watermark bit will be one (1); otherwise the watermark bit will be zero (0). The extracting procedure is done according to the Eq. (9). The detail of the extracting procedure is illustrated in Algorithm 2.

$$w(i,j) = \begin{cases} 1 & c(i,j) > c'(i,j) \\ 0 & c(i,j) < c'(i,j) \end{cases} \quad (9)$$

where $c(i, j)$ represents the current DCT coefficient of the original image, $c'(i, j)$ represents the current DCT coefficient of the watermarked image and $w(i, j)$ represents the watermark bit.

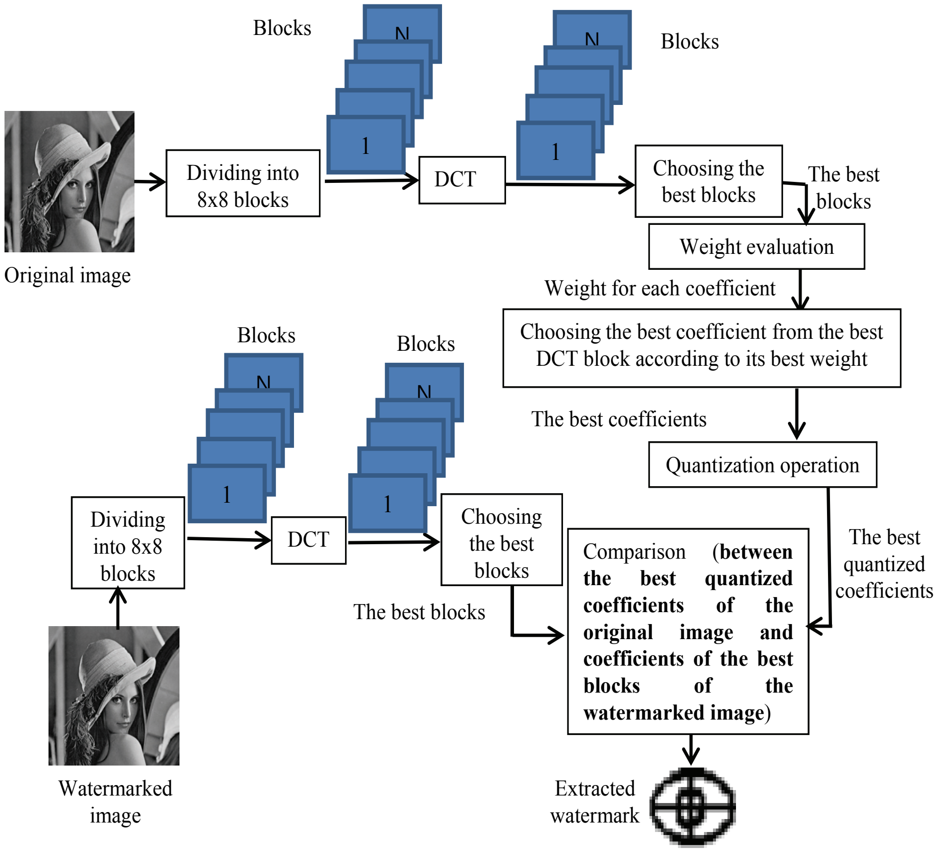


Fig. 6. The extracting process.

Algorithm 2: The extracting algorithm

Input: C′, C
(***C′***: watermarked image, ***C***: original cover image)
Output: W
(***W***: binary text image (watermark))
1: $C_{8\times8(i)} = C$
{subdivide the original cover image (***C***) into blocks of 8×8 pixel}
2: $I_{DCT\,(i)}$ = 2D-DCT ($C_{8\times8(i)}$)
{Compute the 2D-DCT of each 8×8 block of the original cover image}
3: Choose the best DCT coefficients blocks
4: apply eq. (5) on all the best DCT coefficients blocks
{***for evaluating the weight for each coefficient within the best blocks***}
5: Choose the best coefficient within all the best DCT coefficients blocks
{ ***coefficient with high weight***}
6: Quantize the best coefficient
{***by applying eq.(7)***}
7: $C'_{8\times8(i)} = C'$;
{subdivide the watermarked image (*C′*) into blocks of 8×8 pixel}
8: $C'_{DCT\,(i)}$ = 2D-DCT ($C'_{8\times8(i)}$)
{Compute the 2D-DCT of each 8×8 block of the watermarked image}
9: Choose the best DCT coefficients block
10: **for** *i* = 1→size (W) do
11: **if** $\text{DCT}_C >= \text{DCT}_{C'}$
{if the current DCT coefficient of the current block of the original image is greater than the current best DCT coefficient of current best block of watermarked image }
12: $W_{(i)}$ **=1**
13: **else**
14: $W_{(i)}$ **=0**
15: **end if**
16: **end for**
17: reconstruct the watermark image ***W*** from $W_{(i)}$

3.5 Benchmarking Criteria

In order to test the performance of the proposed scheme, several benchmarking criteria have been used. These criteria are listed as follows:

3.5.1 Peak Signal-to-Noise Ratio

The peak signal-to-noise ratio (PSNR) measures the quality of the watermarked image in comparison to the original image (host). It is a standard way of measuring image fidelity [10]. The PSNR is defined as follows:

$$\text{PSNR}=10log_{10}\left[\frac{(I_{MAX})^2}{MSE}\right] \tag{10}$$

where I_{MAX} is the maximum grey level of the image. In this case, I_{MAX} can have a maximum value of 255. MSE is mean square error which is defined as follows:

$$\text{MSE}=\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left(p_1(i,j)-p_2(i,j)\right)^2 \tag{11}$$

where $p_1(i, j)$ and $p_2(i, j)$ represent two images, m, n represent the dimensions of two images.

3.5.2 Structural similarity index measure

The structural similarity index measure (SSIM) is used for evaluate the difference of measured error between the original and the watermarked image. The evaluation of the difference consists of comparisons, viz., the luminance of each image is compared, the contrast of each image is compared and the structure is to be compared. So, SSIM algorithm deals with three components: luminance, contrast, and structure, independently. The value of SSIM function is computed according to the Eq. (12) which proposed by Wang et al. [11] in 2004.

$$\text{SSIM} =\frac{(2\mu_x u_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \tag{12}$$

where μ, σ and σ_{xy} are mean, variance, and covariance of the images, and c_1, c_2 are the stabilizing constants. SSIM has a value between 0-1. Similar images have SSIM near to 1. Then mean of MSSIM is computed according to the following equation [11,12]:

$$\text{MSSIM} = \frac{1}{m}\sum_{i=1}^{m} SSIM(x_i, y_i) \tag{13}$$

where x and y represent the original and the watermarked image respectively; x_i, y_i represent the images contents at the i^{th} local window.

3.5.3 Normalization correlation

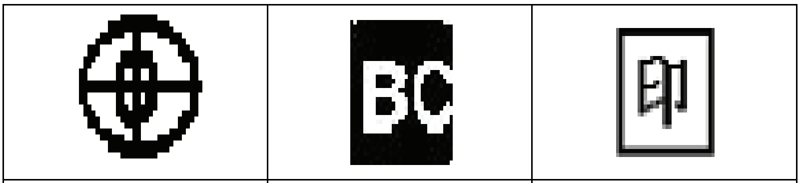
Normalization correlation (NC) is a standard method used as a benchmark to evaluate the degree of correlation between two series, and can be defined in the following equation [12,13]:

$$\text{NC} =\frac{\sum_{i=1}^{M} w_i w'_i}{\sqrt{\sum_{i=1}^{M} w_i^2}\sqrt{\sum_{i=1}^{M} w'^2_i}} \tag{14}$$

where w is the original image and w' is the extracted image.

4. Experimental Results

To test the suggested method, the standard grey-levels images Lena, baboon and pepper of size 256×256 are used as host (cover) images. Binary images of size (32×32) are used as watermarks. The constant value (v) is set to 2. Fig. 7 shows the original watermarks images.



(a) (b) (c)

Fig. 7. Original watermarks. (a) (b) (c).

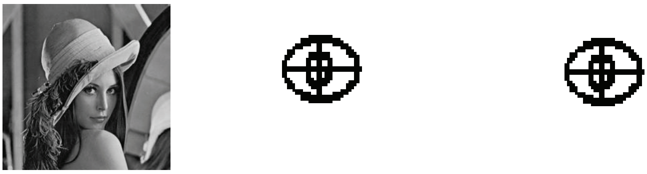
The effect of scaling factors on the perceptual invisibility is tested by using the PSNR and SSIM. Table 1 shows the effect of scaling factors on the perceptual invisibility of the watermarked images, where the chosen values are 4, 8 and 12.

Table 1. The PSNR and SSIM with different scaling factors and different standard images

	Scaling factor	PSNR	SSIM
Lena image	4	49.6590	0.9956
	8	43.7317	0.9818
	12	40.0260	0.9697
Peppers image	4	49.6590	0.9949
	8	42.8182	0.9816
	12	39.2079	0.9599
Baboon image	4	49.0171	0.9979
	8	42.6793	0.9913
	12	39.3456	0.9818

Table 1 shows that the PSNR values ranged from 39.2079 dB to 49.6590 dB, while the SSIM values are ranged from 0.9599 to 0.9979. Table 1 illustrates that the increasing the value of scaling factor affects the quality of the watermarked image.

Before any attack, the NC between the original watermark and extracted watermark is (1) with all scaling factors (4, 8 and 12). Fig. 8 shows extracted watermark from watermarked image (with NC=1 and SF=4) before any attack.



(a) (b) (c)

Fig. 8. Original and extracted watermarks before any attack. (a) Watermarked, (b) original wartermark, and (c) extracted.

Fig. 9 shows that the distortion produced by the new watermarking scheme is undetectable in all tested images with scaling factors (4, 8 and 12). Visually, the watermarked image is relatively close to the original image.

In order to test the performance of the proposed scheme against attacks, different signal attacks are applied on the watermarked image. These attacks can be listed as follows:

4.1 Mean &median & Average Filter Attack

Watermarked image was filtered with a low pass filtering (average filter) and a median filter with window size 3×3 and 5×5]. The experimental results show that watermark is robust to these filters attacks.

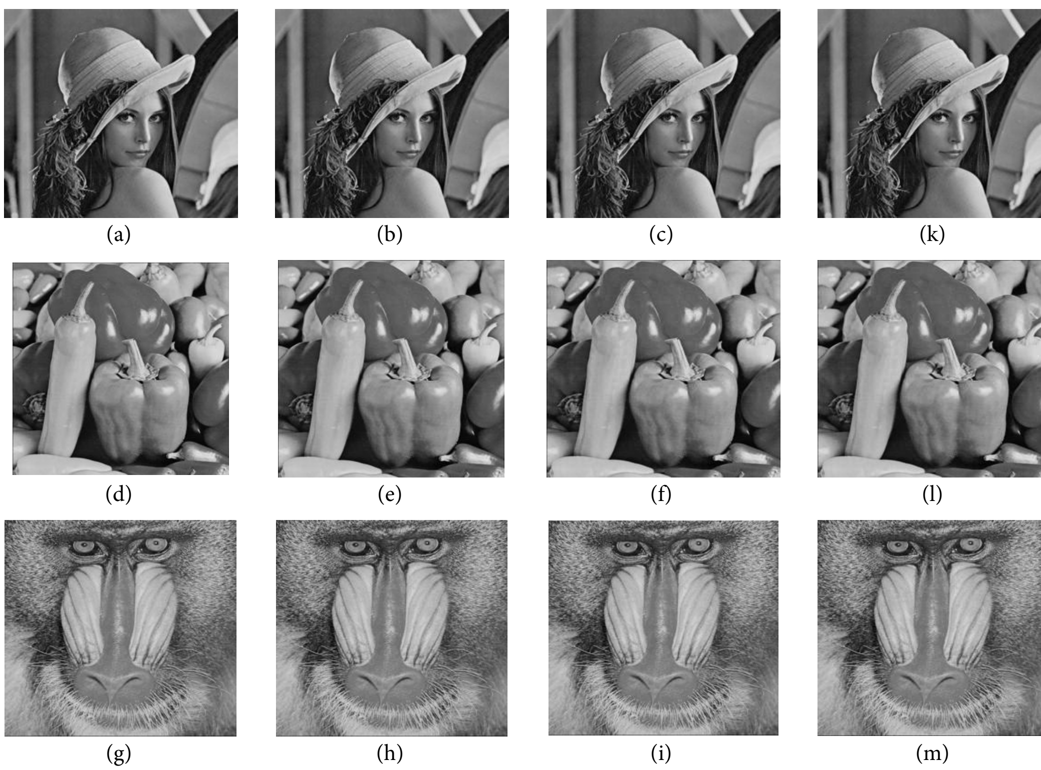


Fig. 9. Different test images and their watermarked versions" (a,d,g) original images; (b,e,h) watermarked images with scale factor of 4; (c,f,i) watermarked images with scale factor 8; (k,l,m) watermarked images with scale 12.

4.2 Rotation Attack

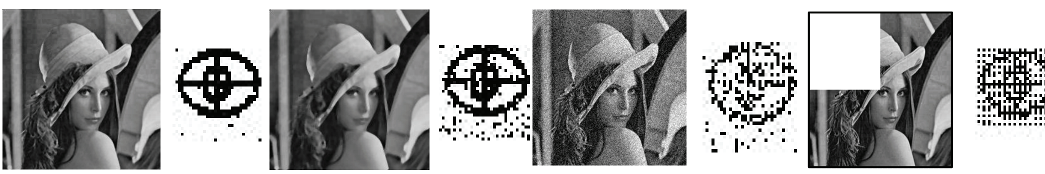
The rotation is a very hard attack. The effect of this geometric attack is not removing the watermark from watermarked image, but destroying the synchronization of the watermark detector. In the image watermarking field, it is very hard to find an algorithm which can easily pass the rotation attack. So, most of the watermarking algorithms are robust to conventional signal processing attacks while neglecting this attack. Experimental results show that the proposed method is robust against this attack.

4.3 Adding Noise (Salt & Pepper, Gaussian) Attack

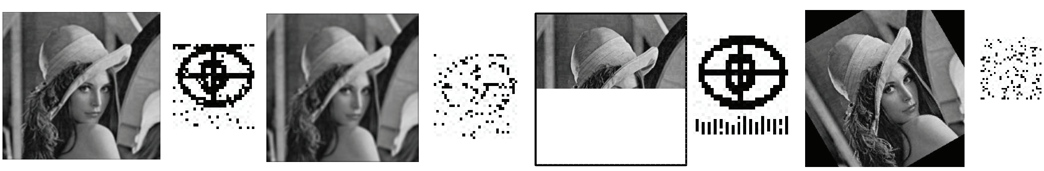
The watermarked is attacked with several noise attacks. Fig. 10 shows that Lena image was corrupted by the addition of (Gaussian or salt & pepper) noise. The Fig. Illustrates that the watermarked image is degraded, but the watermark is extracted easily.

4.4 Cropping Attack

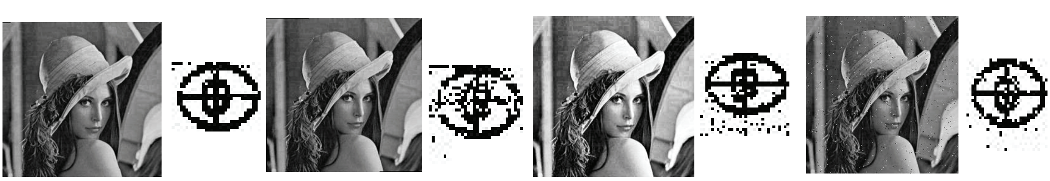
Cropping attack is one of hard attack, where part of watermarked image may be cropped. In the proposed method, the watermark is extracted after cropping off 50% of the watermarked image size.



3×3 median filter 5×5 median filter Gaussian noise v=0.01 Cropping 25% of image



3×3 average filter 5×5 average filter Cropping 50% of image Rotate 30



Rotate 0.25 Rotate 0.5 Histogram equalization Salt & pepper noise v=0.01

Fig. 10. The extracted watermark from Lena image after different types of attacks.

Table 2. NC with different scaling factors

Attack type	NC with SF=4	NC with SF=8	NC with SF=12
Median filter 3×3	0.8996	0.9225	0.9495
Median filter 5×5	0.8474	0.8589	0.8707
Average filter 3×3	0.8551	0.8856	0.8935
Average filter 5×5	0.7907	0.8151	0.8319
Rotation 0.25	0.9549	0.9585	0.9641
Rotation 0. 5	0.8504	0.8734	0.8814
Rotation 30	0.7607	0.7594	0.7577
Salt & pepper noise variance (v) =0.01	0.8907	0.9309	0.9619
Gaussian noise variance (v) =0.01	0.7233	0.8094	0.8894
Cropping ¼ of watermark image	0.8874	0.8874	0.8874
Cropping ½ of watermark image	0.9145	0.9173	0.9185
Histogram equalization	0.7729	0.9007	0.9495

4.5 Histogram Equalization Attack

Histogram equalization is an attack that tries to modify histogram of an image. The experimental results show that the watermark can be recovered after applying this attack.

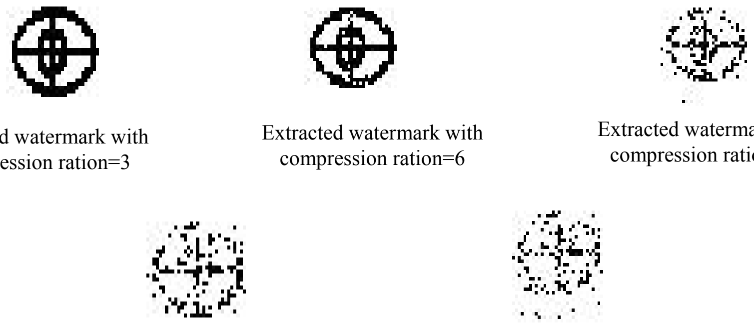
Table 2 shows NC values after applying several attacks on Lena standard image. The Table illustrates that the proposed scheme robust against popular attacks. Fig. 10 shows extracted watermarks from Lena standard image after applying different types of attacks.

4.6 Compression Attack

Compression attack is one of the most important attacks. As we know that, when the compression is applied on the watermark image, its quality will be decreased and it became difficult to recover the embedding watermark. The proposed method has high robustness against the JPEG compression attack. Table 3 shows the NC values at different compression ratio under JPEG 2000 lossy method. Fig. 11 shows the extracted watermark with different compression ratio.

Table 3. The NC values under JPEG 2000 lossy compression with different compression ratio (scale factor =12, test image is Lena)

Compression ratio	NC
3	1
4	1
5	0.9993
6	0.9971
10	0.9435
12	0.9203
16	0.8948
20	0.8627



Extracted watermark with compression ration=3

Extracted watermark with compression ration=6

Extracted watermark with compression ration=12

Extracted watermark with compression ration=16

Extracted watermark with compression ration=20

Fig. 11. The extracted watermarks under different compression ratio.

Table 4. The NC values under JPEG lossy compression with different quality factor (Q) (scale factor=12, test image is Lena)

Quality factor (Q)	NC
80	0.9935
70	0.9893
60	0.9886
50	0.9851
40	0.9844
30	0.9782
20	0.9570
10	0.8722

Fig. 12. The extracted watermark from Lena image after different values of quality factor (Q).

Also, the proposed method is tested on JPEG system with different quality factor (Q). Table 4 shows the NC values at different quality factor. The range of quality factor in [0...100], where 0 is lower quality and higher compression, and 100 is higher quality and lower compression [14]. Fig. 12 shows the extracted watermark with different quality factor.

Figs. 13 and 14 illustrate the relation between 'compression ratio and NC' and 'quality factor and NC,' respectively. These figures show that the increasing of the compression ratio will decrease the robustness of watermark and the increasing of the quality factor will increase the robustness of watermark.

Fig. 13. Compression ratio vs. normalization correlation (NC).

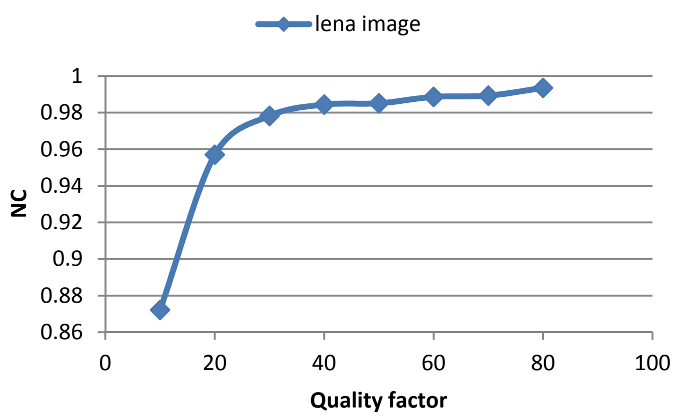


Fig. 14. Quality factor vs. normalization correlation (NC).

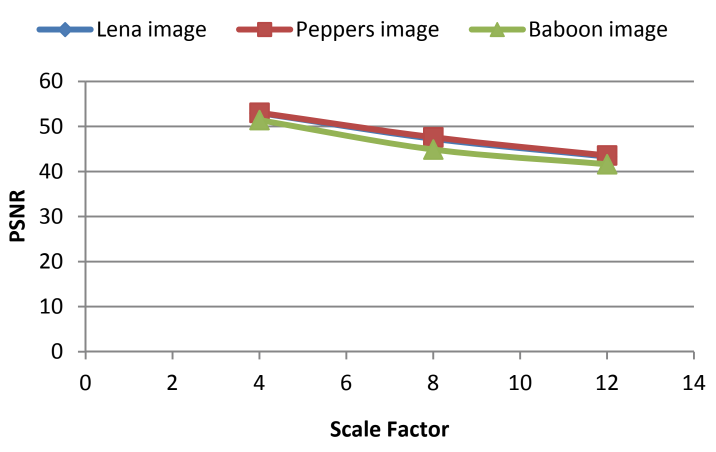


Fig. 15. Scale factor vs. peak signal-to-noise ratio (PSNR).

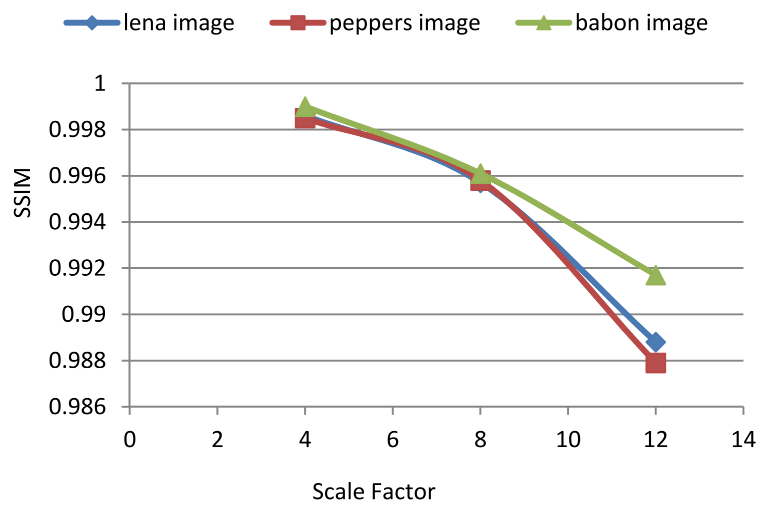


Fig. 16. Scale factor vs. structural similarity index measure (SSIM).

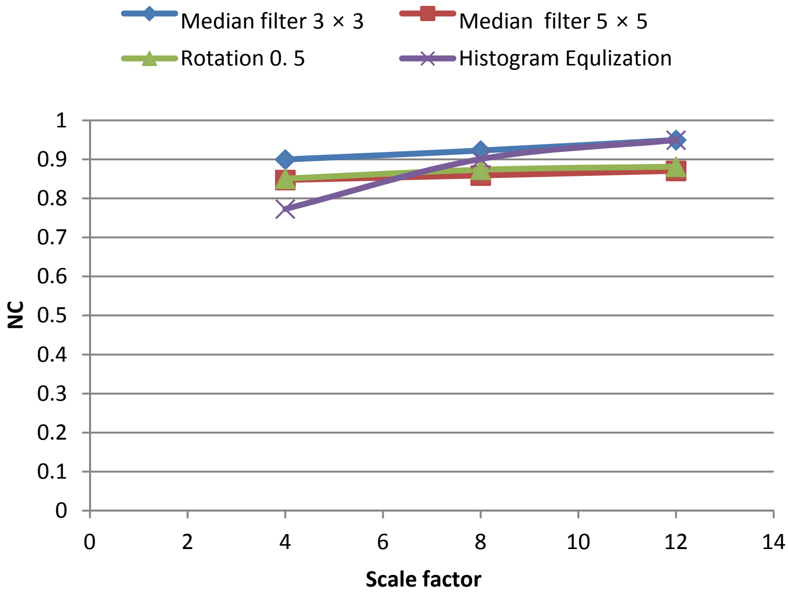


Fig. 17. Scale factor vs. normalization correlation (NC).

Figs. 15–17 illustrate the relation between 'scale factor and PSNR,' 'scale factor and SIMM,' and 'scale factor and NC,' respectively. These figures show that the increasing of the scale factor will increase the robustness of watermark against attacks, but will increase the distortion of the watermarked image and the decreasing of the scale factor will decrease the robustness of watermark against attacks, but will decrease the distortion of the watermarked image. Therefore the selection of the scale factor must preserve the balance between robustness and the perceptual invisibility (distortion of watermarked image).

5. Discussions

To prove the robustness of our proposed method (which select DCT coefficients based on weighting function with other methods that select one of DCT spectral bands (low, middle and high) for hiding), different tests will be done in three DCT spectral bands and compare the results with our method. In the low band, the hiding process will be in coefficient (1,2), in the middle band the coefficient (5,2) is selected for hiding and coefficient (2,8) is selected for high band. Table 5 shows this comparison with different type of attacks with SF=12.

Table 5 shows that our proposed method has a high robustness against different types of attacks.

Also, our proposed scheme is compared with other methods that based on DCT watermark. For example, our method is compared with scheme Mei et al. [15] which applied by using Lena image as cover image and the watermark in Fig. 7(c) as secret. Table 6 shows the results using scaling factor (SF=4).

Table 5. Comparison of the weighting function with other DCT spectral bands

Attack type	NC with proposed method	NC with middle band	NC with low band	NC with high band
Median filter 3×3	0.9495	0.2712	0.7460	0.3919
Median filter 5×5	0.8707	0.1666	0.6983	0.2861
Average filter 3×3	0.8935	0.1143	0.6633	0.1728
Rotation 30	0.7577	0.3918	0.4409	0.3610
Salt & pepper noise variance (v)=0.01	0.9619	0.8296	0.8215	0.3718
Gaussian noise variance (v)=0.01	0.8894	0.5868	0.5853	0.5702
Cropping ¼ of watermark image	0.8874	0.8861	0.8869	0.8861
Cropping ½ of watermark image	0.9185	0.6983	0.6994	0.6983
Histogram equalization	0.9495	0.6466	0.5800	0.6511
Compression with quality factor 50	0.9851	0.1429	0.9586	0.1527

Table 6. Comparison of our scheme with Jiansheng scheme [15]

Attack type	NC	
	Proposed method	Method by Mei et al. [15]
Filter	0.9266	0.9132
Noise salt & pepper (v) =0.01	0.9074	0.8643
Cutting 1/4	0.9373	0.7089
Rotation 30	0.8112	0.5034
Compression quality factor 50	0.9791	0.8515

6. Conclusion and Suggestions for Future Works

In this paper, a new watermarking method of still image based on weighting function of frequency coefficients is proposed for the purpose of copyright protection. The embedding operation is done in the transform domain. Different types of attack have been tested. The experimental results proved that the proposed method produced good imperceptibility and high robustness towards these attacks. After designing and implementing the proposed method, the proposed future works can be listed as follows:

1. The proposed scheme can be implemented in other transform domain such as discrete wavelet transform (DWT) or discrete Fourier transform (DFT).
2. The proposed scheme can be implemented in other digital media such as audio and video.
3. Digital watermarking technique can be used in several applications, such as finger print, tamper detection, owner identification, broadcast monitoring, data authentication and others. So, the proposed scheme can be used in the above applications rather than copyright protection application.
4. The proposed method is non-blind watermarking scheme. It is a good idea to suggest a new blind watermarking method depending on the proposed scheme.

References

[1] L. Goyal, M. Raman, P. Diwan, and M. Vijay, "A robust method for integrity protection of digital data in text document watermarking," *International Journal for Innovative Research in Science & Technology*, vol. 1, no. 6, pp. 14-18, 2014.

[2] M. Mulya and Y. Utama, "Implementation of audio watermarking using fast fourier transform for audio digital copyright protection," in *Proceeding of International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, Palembang, Indonesia, 2015.

[3] M. Yesilyurt, Y. Yalman, and A. T. Ozcerit, "A new DCT based watermarking method using luminance component," *Elektronika ir Elektrotechnika*, vol. 19, no. 4, pp. 47-52, 2013.

[4] J. Jeswani and T. Sarode, "A new DCT based color video watermarking using luminance component," *IOSR Journal of Computer Engineering*, vol. 16, no. 2, pp. 83-90, 2014.

[5] K. A. Ahmed, "Digital watermarking of still images," PhD dissertation, School of electrical and Electronic Engineering, University of Manchester, UK, 2013.

[6] A. E. El Hossaini, M. El Aroussi, K. Jamali, S. Mbarki, and M. Wahbi, "A new robust blind watermarking scheme based on steerable pyramid and DCT using Pearson product moment correlation," *Journal of Computers*, vol. 9, no. 10, pp. 2315-2327, 2014.

[7] K. Ali, and V. Kumar, "Robust binary image watermarking using DCT," *International Journal of Advance Foundation and Research in Computer*, vol. 1, no. 6, pp. 50-58, 2014.

[8] M. A. Abdullah, S. S. Dlay, and W. L. Woo, "Securing iris images with a robust watermarking algorithm based on discrete cosine transform," in *Proceedings of 10th International Conference on Computer Vision Theory and Applications*, Berlin, Germany, 2015, pp. 108-114.

[9] S. S. Gonge and J. W. Bakal, "Robust digital watermarking techniques by using DCT and spread spectrum," *International Journal of Electrical, Electronics and Data Communication*, vol. 1, no. 2, pp. 111-124, 2013.

[10] Q. Huynh-Thu and M. Ghanbari, "Scope of validity of PSNR in image/video quality assessment," *Electronics Letters*, vol. 44, no. 13, pp. 800-801, 2008.

[11] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600-612, 2004.

[12] K. A. Navas, M. Sasikumar, and S. Sreevidya, "A benchmark for medical image watermarking," in Proceedings of *14th International Workshop on Systems, Signals and Image Processing*, Maribor, Slovenia, 2007, pp. 237-240.

[13] M. Kutter and F. A. Petitcolas, "A fair benchmark for image watermarking systems," in *Proceedings of SPIE 3657: Security and Watermarking of Multimedia Contents*. Bellingham, WA: International Society for Optical Engineering, 1999, pp. 226-239.

[14] "MATRAB function reference: imwrite v7.6.0.324," MathWorks Inc., Natick, MA, 2008.

[15] J. Mei, S. Li, and X. Tan, "A digital watermarking algorithm based on DCT and DWT," in *Proceedings of International Symposium on Web Information Systems and Application*, Nanchang, China, 2009, pp. 104-107.

Suhad A. ali

She is working as Assistant Professor in Computer Science Department, Science Collage for Women, University of Babylon, Iraq. She received M.S. and Ph.D. degrees from department of Computer Science, Babylon University in 2002 and 2014, respectively. Her areas of interest are digital image processing, pattern recognition and information hiding.

Majid Jabbar Jawad

He was born in Hilla, Babylon City, Iraq, on January 1, 1967. He received the B.Sc. degree in computer science on 1989 from the University of Technology-Computer Science Dept., Iraq. He received the M.Sc. degree in Steganography on 2003 from the same university. He received the Ph.D. degree in Digital Watermarking and GIS on 2013 from the University of Babylon, Iraq. Currently, he is Assistant Professor in the University of Babylon. His research interests include steganography, digital watermarking, processing of raster and vector image and applying the information hiding techniques in GIS (Geographical Information System).

Mohammed Abdullah Naser

He was born in Hilla, Babylon City, Iraq, on February 1, 1976. He received the B.Sc. degree in computer science on 1998 from the University of Technology, Iraq. He received the M.Sc. degree in Computer Security on 2001 from the same university. He received the Ph.D. degree in Computer Security and Data mining on 2006 from the Iraqi Commission for Computers and Informatics, Iraq. Currently, he is associated Professor in the University of Babylon. His research interests include computer and data security, Data mining applying the data mining techniques in security fields and applications.