DIGITAL IMAGE WATERMARKING BASED ON A RELATION BETWEEN SPATIAL AND FREQUENCY DOMAINS

Murat Furat[1] Mustafa Oral[2]
e-mail: mfurat@cu.edu.tr e-mail: moral@mku.edu.tr
[1]Cukurova University, Faculty of Engineering, Department of Electrical & Electronics Engineering, 01330, Yuregir, Adana, Turkey

[2]Mustafa Kemal University, Faculty of Engineering & Architecture, Department of Electrical & Electronics Engineering, 31040, Antakya, Hatay, Turkey

Key words: Digital image watermarking, copyright protection, discrete cosine transform (DCT)

ABSTRACT

This paper presents a digital watermarking algorithm used for the copyright protection of gray-level images. The proposed algorithm is a blind, invisible-robust watermarking scheme and uses both frequency and spatial domain components of an image. The algorithm is novel in the sense of both embedding and extracting algorithms rely on the information gathered from the both domains. The energy and the frequencies of each block are calculated using Discrete Cosine Transform (DCT). For each block, the selected frequency coefficients from middle-frequency band are modified by comparing the energy of the block with the sum of DC coefficient and selected AC frequency coefficient of the corresponding block. The watermark can be chosen as copyright information, owner information or a digital logo in the form of a bitmap image. The experiments showed that the watermark data embedded into digital image with the proposed algorithm was successfully recovered after various attacks; JPEG lossy compression, cropping and low pass filtering.

I. INTRODUCTION

The current information technology and Internet network all around the world provide fast communication in the recent years. Most of information is transferred into digital form to benefit the advantages of the emerging technologies. Digital media can be copied and distributed without any loss in fidelity, resulting with problems for the protection of intellectual rights of the works [1, 2, 3]. Especially in photograph industry, this is the problem that must be solved. One technical way to protect copyright of the works in digital form is to embed watermark by modifying the work. The watermark can be owner information, copyright data, digital label or a company logo which completely characterizes the owner of the work. Therefore, watermarking has become very active research area in literature.

This paper deals with image watermarking to solve the protection of copyright problem on the digital images. Digital image watermarking can be applied in either spatial domain or frequency domain or both of them. In spatial domain watermarking algorithms, the host image is directly manipulated pixel-wise to embed watermark data. The frequency domain methods, initially decompose the host image into frequencies, and then manipulate the properly selected frequencies. There is no reported work that constructs embedding and extracting algorithms around the parameters that are obtained from the both domains.

According to the human perception, the watermarking methods are divided into two parts: visible and invisible watermarking. In visible watermarking, the watermark can be directly seen on the host image. On the other hand, in invisible watermarking methods, the watermark is embedded in the host image imperceptibly [2, 3]. A dual watermarking technique that contains both visible and invisible watermarks is proposed in [4]. The invisible watermarks can be classified as robust and fragile. Robust watermarking algorithms are designed so that the watermark should be resistant to image processing operations. In contrast, the fragile watermarking algorithms do not provide resistant watermarks [5].

In terms of extraction method, watermarking algorithms can be separated into two types as follows:

- Non-blind watermarking
- Blind watermarking

In non-blind watermarking algorithms, the watermark is extracted using either the original host image or the embedded watermark. On the other hand, in blind watermarking algorithms, the watermark can be extracted using neither the original host image nor the embedded watermark. In this paper, a novel watermarking scheme

that is invisible-robust and blind watermarking technique is presented. The use of parameters obtained from both spatial and frequency domains in the embedding and extracting mechanisms, is proposed in this work.

The paper is organised as follows; the watermarking algorithm is explained in Section II in details. Section III illustrates the experimental results and Section IV briefly discusses the algorithm and the experimental results. In section V, we conclude this paper.

II. WATERMARKING ALGORITHM

In this work, we will propose a blind, invisible-robust watermarking technique for digital images. The watermark is selected as a digital image in bitmap format.

The distortion caused by watermarking on the host image is directly proportional to the amount of embedded watermark image. Instead of using a gray-level watermark, a black-white image is chosen. To decrease the distortion, the watermark is transformed into binary image. In addition, the distortion is proportional to the size of watermark. So, choice of the smallest watermark is appropriate to decrease the distortion on the host image.

In order to survive the watermark from picture cropping, a pseudorandom permutation is applied to the binary watermark by using a seed number. The binary watermark can be permuted more than one. Assume that the binary watermark is W, the selected seed is K and the permutation number N. Then the resultant permuted binary watermark W_p can be found as

$$W_p = Permute(W,K,N) \tag{1}$$

In the literature, many watermarking techniques are based on either spatial domain or frequency domain using Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), DCT, etc [6]. Our watermarking technique is based on a relation established between spatial domain and frequency domain. First of all, the host image is divided into blocks of size 8×8 pixel. The energy of each block is calculated in spatial domain using Equation 2 and DCT (Equation 3) is used to decompose the frequency coefficients of the blocks.

$$E_b = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}[h_b(x,y)]^2 \tag{2}$$

where $h_b(x,y)$ is the pixel in the block ranging 0–255.

$$\tilde{H}_b(u,v) = \alpha(u)\,\alpha(v)\sum_{x=0}^{7}\sum_{y=0}^{7} h_b(x,y)\cos\left(\frac{(2x+1)u\pi}{2\times 8}\right)\cos\left(\frac{(2y+1)v\pi}{2\times 8}\right) \tag{3}$$

where

$$\alpha(i) = \begin{cases} \sqrt{\frac{1}{8}}, if & i = 0 \\ \sqrt{\frac{2}{8}}, if & i = 1,2,...7 \end{cases}$$

The first transform coefficient $H_b(0,0)$ is the average value of the sample sequence. In literature, this value is referred to as the DC coefficient. All other transform coefficients are called the AC coefficients [7]. Because of the reasons explained in [2, 3, 4, 5], block-based DCT is used in our watermarking algorithm by modifying the AC coefficients in the middle frequency band. Meanwhile, the watermark image is divided into same number of blocks with host image.

For a uniform-colour image, the DC coefficient of an image block is equal to the square root of the energy of the corresponding block. On the other hand, for real images, there is difference between the values. The difference is proportional to the high frequency coefficients' weight of the image blocks. Square root of energy is proposed to be the reference point and AC coefficients are modified by comparing the reference point with the sum of DC coefficient and the selected AC coefficients. This modification can be either additive or subtractive by the amount of embedding weight λ. In the following, R represents the reference point, DC and AC are the frequency coefficients in a block and f is the binary watermark data that is embedded into the corresponding AC coefficient. First of all, constant n is evaluated using Equation 4.

$$n = \begin{cases} R + \frac{4n-1}{2}\lambda < DC + AC \le R + \frac{4n+3}{2}\lambda, if & f = 1 \\ R + \frac{4n-3}{2}\lambda < DC + AC \le R + \frac{4n+1}{2}\lambda, if & f = 0 \end{cases} \tag{4}$$

By using evaluated n, the new AC coefficient AC' is calculated with Equation 5.

$$AC' = \begin{cases} R + \frac{4n-1}{2}\lambda - DC, if & f = 0 \\ R + \frac{4n+1}{2}\lambda - DC, if & f = 1 \end{cases} \tag{5}$$

After modifying each AC coefficient in the host image blocks, inverse DCT is applied to the block to get watermarked image (Equation 6).

$$h'_b(x,y) = \sum_{u=0}^{7}\sum_{v=0}^{7}\alpha(u)\,\alpha(v)\,\tilde{H}_b(u,v)\cos\left(\frac{(2x+1)u\pi}{2\times 8}\right)\cos\left(\frac{(2y+1)v\pi}{2\times 8}\right) \tag{6}$$

where

$$\alpha(i) = \begin{cases} \sqrt{\frac{1}{8}}, if & i = 0 \\ \sqrt{\frac{2}{8}}, if & i = 1, 2, ...7 \end{cases}$$

The proposed algorithm is a blind watermarking technique. Therefore, in the extraction algorithm, we do not need to use the original host image. During the extraction, embedding weight λ, selected AC frequencies, number of pseudorandom permutation and the seed number will be used.

The extraction algorithm begins with block-based DCT of the image in question using Equation 3. Meanwhile, the energy of each block is calculated (Equation 2). The extracted watermark data will be binary (0 or 1), from the equation below.

$$f = \begin{cases} 0, if & R + (2n-1)\lambda < DC + AC \le R + 2n\lambda \\ 1, if & R + 2n\lambda < DC + AC \le R + (2n+1)\lambda \end{cases} \quad (7)$$

where, n is an integer number and R is the reference point equal to the square root of energy of the corresponding block.

Now, we have permuted watermark data. To recover the original watermark, we should perform same number of inverse-pseudorandom permutation with the same seed number used in embedding algorithm.

III. EXPERIMENTS

Experiments are performed on gray-level images of size 512×512 pixels and the black-white watermark of size 128×128 pixels. The well-known images Lena, baboon and peppers are selected to test our technique (Figure 1).

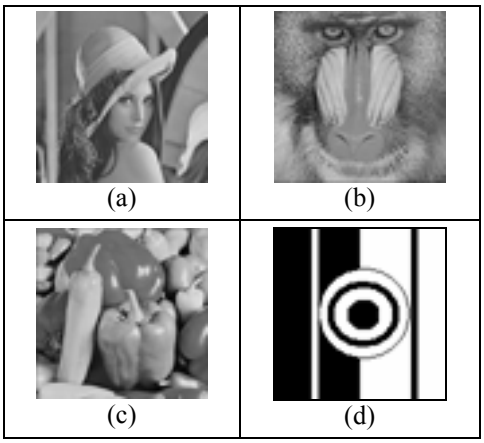


Figure 1. Test images, a) Lena, b) baboon, c) peppers, d) watermark

Watermarking of digital images by any method causes a distortion on the host image. Mean Squared Error (MSE) can be used to measure the difference between the original image and the watermarked image. MSE is defined by the equation in the following. Small MSE in magnitude means small amount of distortion.

$$MSE = \frac{1}{N_1 \times N_2} \sum_{i}^{N_1-1} \sum_{j}^{N_2-1} \left[X(i,j) - X_w(i,j) \right]^2 \quad (8)$$

where, N_1 and N_2 are the size of images, X is the original image and X_w is the watermarked image.

The test images are watermarked with different weights. It is observed that, the distortion on the host image is proportional to the embedding weight (Figure 2).

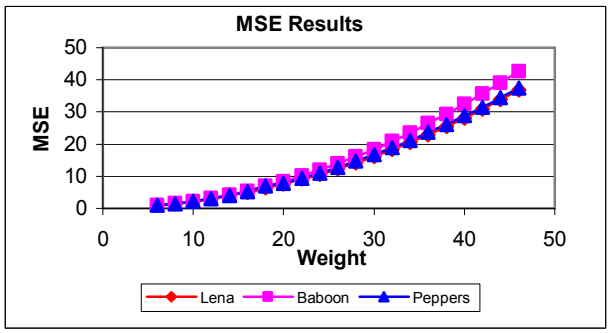


Figure 2. Distortion measurement of test images, MSE versus embedding weight.

Peak-to-Signal Noise Ratio (PSNR) is another criteria to measure the quality of watermarked images and is defined as

$$PSNR_{XX'} = 10 \log\left(\frac{255^2}{MSE_{XX'}}\right) \text{ (in dB)} \quad (9)$$

The result of quality measurements of watermarked images with different embedding weights is given in Figure 3.

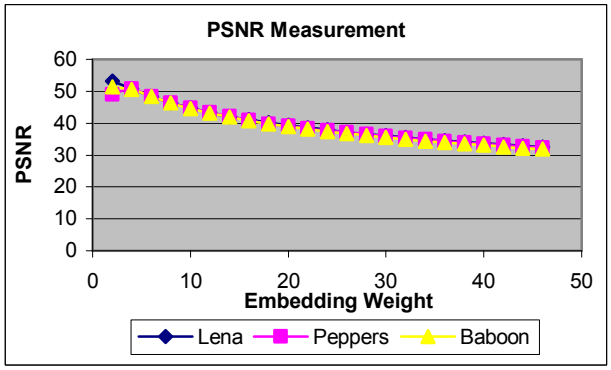


Figure 3. PSNR measurement of test images, PSNR versus embedding weight

It is obvious that, higher embedding weight decreases the quality of watermarked images. The acceptable PSNR for watermarked images is between 30 dB and 40 dB [5]. Higher PSNR values mean that the watermarked image is too similar to the original one.

In the invisible watermarking algorithms performed in frequency domain, the choice of frequencies is very important. The human eye is sensitive to changes in lower frequency coefficients. On the other hand, high frequency coefficients might be discarded after quantization operation of lossy compressions [2]. In [5], because of these reasons, the AC coefficients to be modified were selected with genetic algorithm. The best result after 200 iteration gives 34.79 dB PSNR value using embedding weight λ=10. This computation takes 2 minutes per iteration. In our watermarking algorithm, using same AC coefficients with same embedding weight, we get 44.725 dB, which means very high quality image. The comparison of our results with the results in [5] is in the following.

	Selected AC frequencies	PSNR λ=10	PSNR λ=30
Results in [5].	6, 9, 11, 12	34.790	34.090
Our results	6, 9, 11, 12	44.725	36.002
Our results	16, 19, 24, 25	44.794	36.033

Table 1. The comparison of our PSNR results with the results in [5].

In [3], a block-based DCT watermarking algorithm was proposed. The maximum quality (PSNR) of watermarking image was measured 39.6044 dB for the Lena image using the proposed algorithm. On the other hand, our embedding algorithm provides the qualities 44.794 dB with λ=10 and 51.340 dB with λ=2 for Lena image.

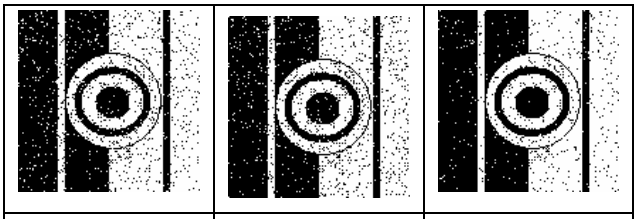
In our watermarking algorithm the watermark is selected to be a visually recognizable black-white digital image. To compare the similarity between original watermark and extracted one, a quantitative measurement is required. Therefore, we used Normalized Correlation (NC) defined in Equation 10 to measure similarities between the watermarks.

$$NC = \frac{\sum_{i=0}^{M_1-1}\sum_{j=0}^{M_2-1} W(i,j)\tilde{W}(i,j)}{\sum_{i=0}^{M_1-1}\sum_{j=0}^{M_2-1}\left[W(i,j)\right]^2} \qquad (10)$$

where, M_1 and M_2 are the size of watermark, W is original watermark and $\tilde{W}$ is the extracted watermark.

Our watermarking algorithm, the resistance of watermark was tested for JPEG lossy compression, picture cropping and LPF attacks.

JPEG lossy compression applies block-based DCT to the image and then discards high frequency coefficients with quantization by an amount of compression ratio. In order to obtain robust watermark against JPEG attack, we embedded the watermark using DCT. To survive the watermark from quantization operation of JPEG, the middle frequency coefficients are selected to modify. In the experiments, we applied JPEG lossy compression with different ratios. It is observed that the embedding weight increases the resistance of watermark against JPEG attack (Figure 4).

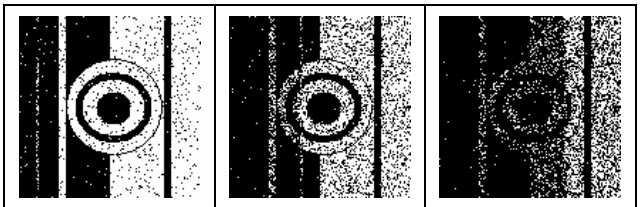


(a) λ=18, % 40 compressed	(b) λ=26, % 60 compressed	(c) λ=38, % 80 compressed

Figure 4. Extracted watermarks embedded with different weights from baboon image after JPEG attack.

In [2], Lena image is compressed with a ratio of 10.74 and the extracted watermark's similarity was measured as 0.413. On the other hand, in our algorithm, watermarked (λ=14) Lena image is compressed with a ratio of 10 and then extracted watermark similarity is measured as 0.999. Therefore, the watermark embedded with our algorithm is more resistant to JPEG lossy compression attack.

Picture cropping is another common attack on watermarked images. To test the proposed algorithm, watermarked images is cropped with different ratios and fill with uniform white colour. Since uniform white colour does not carry any information of watermark, extracted data from this part will be nothing. In the following pictures, extracted watermark from the watermarked Lena cropped from left side with different ratios.



(a)	(b)	(c)

Figure 5. Extracted watermarks from Lena image watermarked with λ=26 and cropped with ratios a) 10%, b) 40%, c) 70%.

In Figure 5, it is seen that, the lost data is distributed on the watermark. This is the result of pseudorandom permutation performed before embedding.

In [3], the proposed algorithm was tested for cropping attack. The missing portions of the watermarked image were replaced with the portions of the original host image. The comparison of our cropping test results with the results in [3] for Lena image follows. The higher similarity of our extracted watermark is the result of pseudorandom permutation. The pseudorandom permutation applied to the watermark before embedding increases the watermark similarity against crop attack.

Cropping Ratio (%)	Our extracted watermark similarity (NC)	The extracted watermark similarity in [3] (NC)
10	0.935	0.88657
50	0.600	0.52558
90	0.137	0.11139

Table 2. The comparison of our NC results with the results in [3] for the selected ratios of cropping attack.

Low pass filter test is applied to the watermarked images. LPF is useful in noise smoothing. After LPF attack, it is seen that, the embedding weight is not so affected on the resistance of the watermark. In Figure 6, the watermark in Lena and peppers images are affected approximately same ratios while the watermark in baboon image is nearly not affected. The difference of these images is the amount of smooth surfaces.

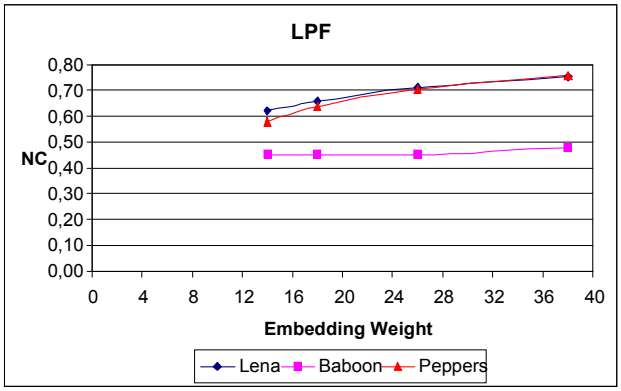


Figure 6. The similarity results of watermarks extracted after LPF attack.

IV. RESULTS AND DISCUSSION

In this paper, we proposed an algorithm that enables a blind, invisible-robust watermarking for digital images. With our algorithm, we can obtain quality watermarked images even if we used high embedding weights. In addition, after the common attacks against watermarked images, the extracted watermark is very similar to the original.

The embedding weighting factor generally increases the resistance of the watermark against the attacks. In contrast, high embedding weights decrease the watermarked image's quality. Choosing small embedding weighting factors results in fragile watermarks with high quality watermarked images. On the other hand, choosing higher embedding weighting factors results in robust watermarks with lower quality watermarked images. An optimum weight can be selected depending on the aim of the watermarking.

V. CONCLUSION

A blind, invisible-robust watermarking is one of the technical solutions to copyright protection of digital images. The experimental results show that the proposed algorithm embeds the watermark imperceptibly and it is resistant to common picture attacks. In comparison with the previous works, better watermarked image quality is measured and the extracted watermarks from attacked images have higher NC values.

REFERENCES

1. J. Zhao, E. Koch, Embedding Robust Labels into Images for Copyright Protection. Proceeding of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, 1-10, August 1995, Vienna.
2. C.T. Hsu, J.L. Wu, Hidden Digital Watermarks in Images, IEEE Transaction on Image Processing, 8(1):58-68, 1999.
3. Y.T Pai, S.J. Ruan, Low Power Block-Based Watermarking Algorithm, IEICE Trans. Inf. & Syst. Vol.E89-D, No.4, April 2006.
4. S. P. Mohanty, K. R. Ramakrishnan, M. Kankanhalli, A Dual Watermarking Technique for Images, Proceedings of 7th ACM International Multimedia Conference, ACMM-MM'99, 49-51, 1999, Orlando, USA.
5. C. S. Shieh, H. C. Huang, F. H. Wang, J. S. Pan, 2004. Genetic Watermarking Based on Transform Domain Techniques, The Journal of the Pattern Recognition, 37, 555–565, 2004.
6. F. Hartung, M. Kutter, Multimedia Watermarking Techniques. Proceedings of IEEE, 1079-1107, 1999.
7. K. Sayood, J. C. Borkenhagen, Use of Residual Redundancy in the Design of Jointsource/Channel Coders, IEEE Transactions on Communications, 39(6):838–846, June 1991.