Combined Spatial and Frequency Domain Watermarking

David Asatryan
Institute For Informatics and Automation Problems of NAS Armenia
Yerevan, Armenia
e-mail: dasat@ipia.sci.am

Naira Asatryan
Russian-Armenian (Slavonic) University
Yerevan, Armenia
e-mail: Naira1973@yandex.ru

ABSTRACT
In this paper, we propose a novel watermarking algorithm, based on combining of spatial domain watermarking approach and an embedding procedure, which uses the DCT pattern instead of required original watermark. This method allows the usage of bigger watermark because of reducible sizes of its DCT pattern. The robustness of algorithm is investigated under JPEG attacks. An algorithm for malicious tamper detection is considered.

Keywords
Watermark, adaptive, spatial domain, transform domain, DCT, JPEG compression, robustness, tamper detection.

1. INTRODUCTION
Last two decades are characterized by rapid development of digital methods of protection of the multimedia information from the non-authorized access, use and change, and also wide application of these methods in the processes of storage, processing and transfer of information. At that most intensively are developed the protection methods, based on modern information technologies by application of mathematical methods of digital signal and image processing. One of the most effective means of protection of the multimedia information consists of embedding of invisible labels - digital watermarks in protected object.

In the scientific literature one can find huge amount of watermarking methods and algorithms. One of comprehensive reviews on this topic is done in [1-2]. The main attribute distinguishing these algorithms is approach used at the watermark embedding into a signal or an image in that way in order to protect the object with high robustness of results at the influence of various distorting factors and attacks. It is well known that these algorithms can be divided into two large groups of algorithms, based on embedding a watermark directly into the spatial or the frequency (transform) domain.

Spatial domain methods. These methods are based on direct modification of the values of the image pixels, so the watermark has to be imbedded in this way. Such methods are simple and computationally efficient, because they modify the color, luminance or brightness values of a digital image pixels, therefore their application is done very easily, and requires minimal computational power.

Frequency (transform) domain methods. These methods are based on the using of some invertible transformations like discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete wavelet transform (DWT) etc. to the host image. Embedding of a watermark is made by modifications of the transform coefficients, accordingly to the watermark or its spectrum. Finally, the inverse transform is applied to obtain the marked image. This approach distributes irregularly the watermark over the image pixels after the inverse transform, thus making detection or manipulation of the watermark more difficult. The watermark signal is usually applied to the middle frequencies of the image, keeping visually the most important parts of the image (low frequencies) and avoiding the parts (presented by high frequencies), which are easily destructible by compression or scaling operations. These methods are more complicated and require more computational power. The rest approaches are based on various modifications of both methods above, using useful details of them to increase the quality of whole watermarking process.

Each of considered methods has advantages and disadvantages [3], which can be arose depending on a solution of concrete problem of information protection. It is well known that there are three main mutually conflicting properties of information hiding schemes: *capacity, robustness and indefectibility* [4]. It can be expected that there is no a single watermarking method or algorithm with the best quality in the sense that three mentioned above properties have the maximum value at once. But at the same time it is obvious that one can reach quite acceptable quality by means of combining various watermarking algorithms and by means of manipulations in the best way operations both in the spatial and in the frequency domains of an image.

In paper [5] an approach to combining of DWT and DCT to improve the performance of the watermarking algorithms, which are based solely on the DWT, is proposed. Watermarking was done by embedding the watermark in the first and second level DWT sub-bands of the host image, followed by the application of DCT on the selected DWT sub-bands. The combination of these two transforms improved the watermarking performance considerably when compared to the DWT-only watermarking approach.

In paper [6], a hybrid watermarking method joining a robust and a fragile or semi-fragile watermark, and thus combining copyright protection and tamper proofing is proposed. As a result this approach is at the same time resistant against copy attack. In addition, the fragile information is inserted in a way which preserves robustness and reliability of the robust part. The superior performance of the proposed approach is demonstrated.

There are many other papers to show the effectiveness of combining of various watermarking algorithms.

The aim of this paper is to propose a simple watermarking algorithm, based on combining the adaptive spatial domain algorithm [7], when the embedding information is a

compressed DCT pattern of watermark required. An investigation is done in [7], which allows embedding a Gray Scale image into a Gray Scale image by splitting the last to blocks in proportion with the watermark and changing the pixels of each block in proportion with the watermark pixels. This algorithm is robust to random and JPEG attacks and has some other attractive properties. So it is reasonable to use this algorithm with a modification, which allows the embedding of DCT coefficients into blocks instead of original watermark.

2. DESCRIPTION OF METHOD

Let's consider at first the algorithm [7] of embedding a Gray Scale watermark image W of size $K \times L$ into a Gray Scale image I of size $M \times N$. Let K и L be, for simplicity, divisors of M and N correspondingly. We have to break the image I into KL blocks of size $(M/K) \times (N/L)$ and establish one-to-one correspondence between pixels of W and blocks of image I (using some pseudorandom or secret key). Let a pixel b of the watermark W have to be embedded into a block $A_0 = \{a_{ij}\}$, $i = 0,1,..., M/K - 1;$ $j = 0,1,..., N/L - 1$ with pixels a_{ij}. Then we use the embedding procedure proposed in [7], based on the formula as follows

$$a_{ij}^W = (1-\alpha)a_{ij} + \alpha b, \qquad (1)$$

where a_{ij}^W denotes the corresponding pixel of watermarked image with a gain $\alpha > 0$, fixed for whole image. Thus, all pixels of block A_0 are modified by using the same pixel b of the watermark W. Denote by I_W the image I watermarked by watermark W.

The extracting procedure is based on using the least-squares method (LSM) for estimating the unknown parameter b (i.e. a pixel of watermark) by pixels $a_{ij}^{W,X}$ of current block of possibly attacked watermarked image $I_{W,X}$, where X denotes an attack. So we can obtain an LSM-estimate as follows

$$\hat{b} = \frac{\mu^{W,X} - (1-\alpha)\mu}{\alpha}, \qquad (2)$$

where

$$\mu^{W,X} = \frac{KL}{MN} \sum_{i=0}^{M/K-1} \sum_{j=0}^{N?L-1} a_{ij}^{W,X}, \mu = \frac{KL}{MN} \sum_{i=0}^{M/K-1} \sum_{j=0}^{N/L-1} a_{ij}.$$

When attack absents, we have $\hat{b} = b$.

In this paper, we propose to use its pattern W_{DCT} instead of the origin watermark W, calculated by DCT and then compressed by choosing reduced enough number of DCT coefficients. We call this algorithm *combined watermarking algorithm*.

The block-scheme of combined algorithm is depicted in Figure 1. The protected image is split up to blocks, to be superposed with the watermark pattern. Then the DCT coefficients of watermark image are calculated. Compression in the frequency domain is made by nulling of non-significant coefficients of the spectrum, and performing the inverse DCT to compare with the original watermark. If the quality of compressed watermark image is acceptable, the modulus of chosen DCT coefficients are considered as a watermark pattern W_{DCT} and superposed with blocks of the host image. It is necessary, of course, to map preliminarily the values of DCT coefficients to the interval [0,255] by fixed linear transform.

The watermark extracting process is made for each block as it is described above. The resulting array of numbers consists of all extracted pixels and presents only the transformed DCT coefficients. To get the extracted watermark we must recover the DCT coefficients, and calculate the inverse DCT of this array, then we can see or compare obtained image with the origin watermark.

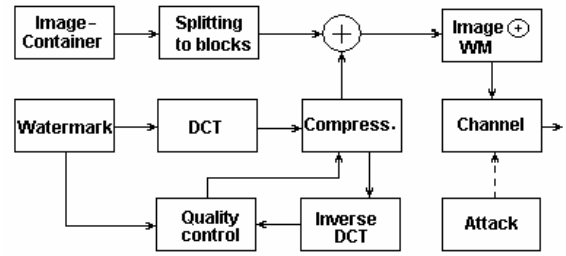


Figure 1. Block-scheme of combined watermarking algorithm.

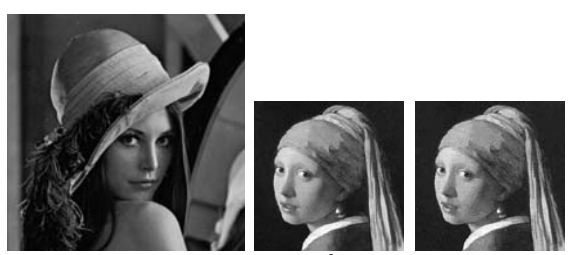
We shall note that the elements of watermark pattern W_{DCT} must be performed to the interval of pixel intensities [0,255] multiplying them by an appropriate coefficient.

3. EXPERIMENTS

To check effectiveness of proposed algorithm there were made a few experiments with Gray Scale images and watermarks.

3.1. Experiment 1

At first, let's show the result, when the watermark is directly embedded into a host image by algorithm [7] without any additional transformations. Let W_{extr} and $W_{X,extr}$ be the extracted watermark at attack absence and presence correspondingly.



a b c

Figure 2. Host image (a), original watermark (b), extracted watermark (c).

In Figure 2 the host image Lenna of size 512x512 and a watermark image Girl («Girl with a Pearl Earring», [8]) of size 128x128 are given. Let be $\alpha = 0.07$, then PSNR= 33.1 dB between the host and watermarked images. This value is quite acceptable from the point of view of watermark imperceptibility requirement. In Figure 2c the extracted watermark is shown (PSNR=43.2 dB relatively to the original).

Robustness of this procedure can be shown by compression of watermarked image using JPEG standard at quality parameter

q. In Figure 3 the extracted watermarks at various quality of compressed image are shown.

a b c

Figure 3. Watermarks extracted from the compressed watermarked image; a) $q = 80\%$, b) $q = 70\%$, c) $q = 30\%$.

We see that the extracted watermarks are quite recognizable even at a high rate of compression.

3.2. Experiment 2

Let's consider now the case of usage of the watermark DCT pattern instead of the original one. Compressing process of a watermark image can be performed in such manner that the number of chosen DCT coefficients was significantly smaller than the number of pixels of the original watermark. Thus the reliability of extracted information becomes respectively larger. The compression procedure implies the nulling of certain percent of DCT coefficients of highest order. Let γ be the percent of remained coefficients. Values of γ must be found by comparing the origin and recovered watermarks to save the recognizability of hiding information after its extracting from attacked image.

In Figure 4 the watermarks compressed by described manner are shown at various values of γ. The sizes of used DCT matrix are given in the third row. The values of PSNR between the compressed watermarks and the origin one are given as well. We can see that the recognizability of compressed watermark is still acceptable while the sizes of corresponding matrixes are significantly lower.

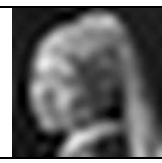
γ : 25%	6%	2%
		
DCT: 64 x 64	32 x 32	16 x 16
PSNR: 30 dB	24 dB	20 dB

Figure 4. Compressed watermarks at various γ, corresponding sizes of watermark and PSNR.

a b

Figure 5. Watermarked image with watermark pattern (a) and extracted watermark (b).

Following experiment we draw with the watermark at $\gamma = 6\%$ (see Figure 4) and the host image Lenna of sizes 512 x 512 shown in Figure 2. Let $\alpha = 0.07$. In Figure 5a the watermarked image is shown. Analyzing visually the images of Figure 2 and Figure 5a we can note that there are no significant differences between them ($PSNR \approx 36$ dB). The extracted watermark in this case is shown in Figure 5b.

Then the robustness examination of the proposed procedure is required. First of all, the robustness to JPEG attacks must be examined, because the preliminary DCT compression of watermark is performed. So it is interesting to examine the affect the watermark "double compression" to the robustness relatively to the "usual" watermarking procedure [7].

Let's examine the robustness of described watermarking procedure by JPEG-compressing the watermarked image above at the same compression rate of 70%, which was used in Experiment 1. The comparative results are collected in Table1.

PSNR, dB	Algorithm [7]	Proposed Algorithm
I, I_W	33.1	36.3
I, $I_{W,X}$	31.8	34.1
W, W_{extr}	43.2	22.0
W, $W_{X,extr}$	28.6	16.0

Table 1. Comparative results obtained in Experiment 1.

As seen from data presented in Table 1, the proposed algorithm leads nearly to the same watermark invisibility, even at considered JPEG attack. But extracted watermark has significantly lower quality, which can be putted down to specified "double compression" procedure, though the extracted watermark is quite recognizable.

3.3. Experiment 3

The previous experiment shows that it is possible to embed into a host image the watermarks, which have less sizes of DCT pattern with respect to a host image, but have the sizes of origin watermark perhaps larger, that the host image. In this experiment we examine this situation by an example. In Figure 6 a part of the host image Lenna of sizes 64 x 64 (a) and the original watermark image of sizes 128 x 128 (b) are shown. Watermark embedding for reduced DCT matrix of sizes 16x16 is performed. In Figure 6c the extracted and recovered watermark image is shown. We see that the extracted watermark visually is quite recognizable ($PSNR \approx 20$ dB relatively to the original watermark) in spite of the reducing of embedded information 64 times! This example shows the effectiveness of the proposed approach for various applications.

a b c

Figure 6. Host image (a), original watermark (b), extracted watermark (c).

3.4. Experiment 4

This experiment is oriented to apply the proposed watermarking procedure to a problem of image malicious tamper detection. For this purpose we put on image Lenna of

Figure 2a the text “05.12.09”. Then obtained image was watermarked at $\alpha = 0.07$ by watermark DCT-pattern at $\gamma = 6\%$ (as it is described in section 3.3). The watermarked image is shown in Figure 7a. Then the date printed to image was maliciously changed to “05.12.09”. This tampered image is shown in Figure 7b. In Figure 8 the watermark extracted by proposed algorithm from the tampered image is shown. We see that the watermark is highly damaged thereby detecting the fact of tamper.

Figure 7. Image Lenna with printed date 05.12.09 (a) and the same image with the changed date 05.02.09.

One can note that the observed distortions of the extracted watermark spread over the whole image in contrast to results obtained by usual methods used for tamper detection. This result is an effect of DCT procedure using for watermark pattern preparation. To determine the location of distortion the extracted DCT pattern of watermark can be analyzed.

Figure 8. Extracted watermark from tampered image.

4. CONCLUSIONS

In this paper, we propose a novel approach to a robust watermarking problem in the spatial domain. It is well known that one forced to embed watermark pixel into a block of pixels of a host image to increase the robustness of spatial domain watermarking algorithm. However, the capacity of embedding information will inevitably decrease, if it is necessary to keep the appropriate undetectability of the watermark. Therefore there arose an idea to embed the DCT-pattern of watermark of reduced size instead of the original one. This operation increases significantly the capacity of embedding information, while the recognizability of the watermark remains still on high enough level. In the paper, some experiments are performed to show the advantages of this approach. Particularly, we show that it is possible to embed a larger watermark image into a smaller one without essential losses of recognizability. These experiments show how to reach a compromise between the quality of a DCT-compressed watermark of smaller size and the quality of extracted watermark, while the robustness of procedure is fixed. The proposed algorithm is also useful for image tamper detection. Distortions of the extracted watermark detect the fact of tampering, while distortions in the DCT-pattern of a watermark indicate the location of distortions.

REFERENCES

[1] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn. “Information Hiding - A Survey”, *Proceedings of the IEEE, special issue on protection of multimedia content*, 87(7): pp. 1062-1078, July 1999.

[2] Frank Hartung, and Martin Kutter, Multimedia Watermarking Techniques. Proceedings of the IEEE, vol. 87, No. 7, July 1999.

[3] S. Voloshynovskiy et al., Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks, IEEE Communications Magazine, vol. 39(8), pp. 118–126, Aug. 2001.

[4] Jana Dittmann, David Meg´ıas, Andreas Lang, Jordi Herrera-Joancomart´ı, Theoretical framework for a practical evaluation and comparison of audio watermarking schemes in the triangle of robustness, transparency and capacity, accepted Journal in Springer LNCS Transactions on Data Hiding and Multimedia Security, 2006.

[5] Ali Al-Haj. “Combined DWT-DCT Digital Image Watermarking”, Journal of Computer Science 3 (9): pp. 740-746, 2007.

[6] F. Deguillaume, S. Voloshynovskiy, T. Pun. “Secure hybrid robust watermarking resistant against tampering and copy attack”. Signal Processing 83, pp. 2133 – 2170, 2003.

[7] Д.Г. Асатрян, Г.С. Шахвердян, Н.С. Асатрян. Устойчивый цифровой алгоритм защиты изображения. Известия НАН РА и ГИУА. Серия ТН, т. 62, N 1, сс. 69-75, 2009.

[8] http://www.sai.msu.su/wm/paint/auth/vermeer/earring.jpg.