A DUAL TECHNIQUE FOR WATERMARKING COLOR DIGITAL IMAGES

Monica RADULESCU[1], Felicia IONESCU[2]

Principalele cerințe impuse unui algoritm de watermarking viabil sunt: păstrarea calității imaginii gazdă și rezistența marcajului introdus la cât mai multe tipuri de atacuri. În această lucrare autorii propun o metodă dual care combină o tehnică spațială de marcare și o tehnică bazată pe o transformare în frecvență. Cele două metode au proprietăți complementare în ceea ce privește rezistența marcajului la atacuri ceea ce face ca metoda propusă să fie rezistentă la mai multe tipuri de atacuri. Pentru că cele două marcaje sunt introduse în coeficienți diferiți ai imaginii, acestea nu interferă păstrându-se calitatea imaginii. Pentru o imagine astfel marcată, rezultatele experimentale arată rezistență la atacuri geometrice și non-geometrice.

The main requirements of a viable watermarking algorithm are: maintaining the host image quality and achieving a very high robustness to any kind of attacks for the introduced markup. In this paper, the authors propose a dual watermarking method. It combines a spatial watermarking technique with a frequency based technique. The two used methods have complementary results for image resistance to attacks. Since both watermarks are embedded in a different portion of the image coefficients, they do not interfere and the image quality is preserved. The resulting double watermarked image is extremely robust with respect to a wide range of attacks, including geometrical and non-geometrical transformations.

Keywords: watermarking, frequency transformation, attacks, robust message hiding, adaptability

1. Introduction

During the last years, Internet has made the access of information possible from any computer and from any location. In these conditions, the transmitted information has to be protected from the unauthorized ones, without blocking the distribution to clients. The techniques of digital marking were developed for transparent protection of the most exposed information category: images.

In this paper, after studying the watermarking techniques evolution (by input image categories and influences from other research fields), the authors

[1] PhD Student, Faculty of Electronics, Communications and Informatics Technology, University POLITEHNICA of Bucharest, Romania
[2] Prof.dr.ing., Faculty of Electronics, Communications and Informatics Technology, University POLITEHNICA of Bucharest, Romania

propose a dual coding technique which improves mark resistance without affecting host image quality. Two different methods are chosen, applied to the same image and a lot of experimental results are evaluated (after PhotoShop transformations). We analyze the possibility of a mix between their advantages and the results confirm that. We obtain a simple and robust algorithm and high quality for marked image.

2. Watermarking techniques evolution to robustness

For an image, low frequency coefficients are correlated with its uniform regions, with its vital information, and high frequency coefficients are keeping edges, texture regions and details. By modifying the low frequency coefficient the image is strongly affected, distortions are important, so invisible watermarking techniques and other image processing techniques do not disturb this kind of components. For example, image processing methods, like compressions, filters, noise addition or removing use only medium or high frequency coefficients.

Low and high frequency coefficient are separated through frequency transformations like: Fourier [1], Cosines [2], wavelet [3], Hadamard or combinations of them [4]. Using frequency space in watermarking algorithms improves very much the robustness. The mark can be detected even after lossy compression, low pass filters, noise addition, color, contrast modifications, etc.

It's also important to have marked pixels all over the image. The experimental results show that a big mark is less resistant than a repeated small mark, especially to cropping. For improving the robustness, the mark is added in a random way, without cover the host image in any order, sometimes just in some pixels or pixels blocks randomly chosen (or chosen using a secret key [3]).

Robustness to geometrical attacks needs special care. Resynchronization between possible coded image and mark [5] is an expensive and complex process. Besides, most of the times, we need the original, unmarked image for finding the geometrical transformations to inverse. For these reasons, special watermarking techniques were developed for achieving robustness to geometrical attacks. In [6] the marked pixels correspond to feature points. The feature point's extraction operators are invariant to geometrical transformations, such as rotations, scaling and translations. Around these points we build circular areas where the mark in added in sectors to achieve robustness to rotations. In [7] the invariant coefficients are established using a Fourier-Mellin transformation and log-polar coordinates.

Because we have a big number of different attacks and only one marking method, usually the mark is not resistant to all o these. For this reason dual coding is used. Two different watermarking methods are used. The methods have to modify different types of coefficients so we can detect al least one mark. The two methods (example: one spatial and one using the frequency coefficients) do not

interfere. The only disadvantage is that two marking methods can affect to much the coded image quality. The quality is always maintained through a compromise between robustness and appearance.

3. Watermarking techniques evolution to invisible mark

The main research direction for achieving image quality is establishing hiding possibilities by studying human visual system (HVS) properties. Because color space RGB is used for displaying images on monitors and the image format Bitmap was the most popular, first color watermarking schemes used these color components. The studies made on HVS showed that human eye is less sensitive to modification on blue component and watermarkers used this component especially.

RGB space has a strong correlation between its components, correlation that can make vulnerable the mark. Image processing algorithms, especially the segmentation ones, use a wide range of color spaces, which can be obtained through linear transformations from RGB [8]. Any transformation applied on host image must be perfect reversible, as we have to be able to reconstruct the initial image. For this reason, watermarking digital color images techniques use only linear color space transformations. From these transformations we frequently use: YIQ, YUV, $I_1I_2I_3$, XYZ, CO (Color Opponency), YCM.

For a certain image, using one color space or another can bring improvements. The studies made in this direction [9] and [4] showed that the used color space isn't a significant component of a watermarking algorithm. The big difference is between using RGB or one of the color spaces presented here. In this last case, the correlation function has better results.

There are two types of image quality measurements: pixel oriented measures and perceptual measures. Pixel oriented measures are an evaluation of differences between original image and coded one. Perceptual measures do not evaluate metric distance between pixel's values, but the impact of modifications on human visual system. They are influenced by contrast sensibility, masking phenomenon of HVS or other eye sensibility aspects. MPSNR (masked Peak Signal to Noise Ratio), wPSNR (Weighted PSNR) and Watson measure are some examples of perceptual measures. Watson [10] describes a perceptual model that estimates several differences between images called Just Noticeable Differences (JND). Watson model is much better than mean square error in estimating the visual effect of adding a mark to an image [11].

The gain factor is sometimes called mark's transparence. Watermarking natural images is depending on each pixel properties, by properties meaning color information and position. For protecting marked image quality, the most important step in watermarking evolution is developing adaptive methods. This

kind of methods is based on choosing a different gain factor for each pixel or pixel block. The methods of establish the gain factor are called masking methods. The starting point of these masking methods is HVS properties. They calculate the maximum gain factor for each pixel (pixel block) by evaluating the pixel position into a textured or uniform region of the image. The masking methods are diverse. In [12] a masking method based on JPEG quantization tables is proposed, in [13] stationary and non-stationary Gauss model based methods. In [2] the proposed masking method is JND and in [9] is described a masking method based on segmentation algorithm JSEG [14]. The impact of masking methods over the existing watermarking algorithms was important and they are now a base component of a watermarking system.

The goal of adaptive watermarking is to achieve maximum of performance with minimum of quality costs. Adaptability can be defined like a masking method or by any other way of adapting the method to image: choosing different mark for every image or choosing mark position relaying to host image.

4. Watermarking techniques evolution to dedicated algorithms and using other research areas

A two-dimensional digital image can be binary, gray-level or color. It can be a natural image or an abstract one; can be a scene with some object or a crowd photo. It is hard to define the character of an image and the class it belongs to. We also cannot exclude from coding any of these image categories. On the other side, a watermarking algorithm has some initial parameters, bounded to host image and its adaptability cannot exceed the coasts between a color image and a binary one for example. In these conditions, developing universal watermarking algorithms is a utopia.

The most exposed to attacks type of images is the color type. This is the frequent image type on Internet. Color image watermarking can use a gray-level watermarking method, adapted to color necessities. Changing the color space can be a method of adapting gray-level techniques. But a color image has more information that can be efficiently used into a watermarking technique. Color can be a major partner. In this research direction we found several methods [15].

The powerful development of watermarking algorithms from the last years includes watermarking schemes based on techniques developed for other research areas. The frequently imports are made from image processing area: segmentation algorithms, filtering, compression, color quantization, color spaces, frequency transformations, edge extractors, feature point's extractors, etc. There are also a lot of influences from statistics, cryptography, genetic algorithms and medicine. A new chapter in watermarking history is implementing them on cellular automata. CNN-UM (Cellular Neural Network – Universal Machine) offers fast possibilities

for implementing watermarking algorithms and can be use for video sequences coding in real time [16] [17].

5. A dual watermarking method for coding color images

In this chapter a new watermarking method for digital color images is proposed. This dual technique applies two different marks successive, using two different watermarking techniques. First one is a spatial method, color image dedicated, and second one is a frequency based gray-level image watermarking algorithm, adaptive and based on wavelet coefficients. It is interesting that the two methods do not interfere. Each one results are preserved. In the same time, by a proper chose of those two methods we build a very efficient watermarking algorithm, with robustness to much more kinds of attacks than each one separately.

The first proposed method organizes image color information by color components: R, G and B or by transformed color space components CO (Color Opponency) into a vector. Through this specific organize the mark isn't geometrically synchronized with the host image anymore and it achieves robustness to this kind of attacks. The proposed algorithm uses a pseudo-random generated mark, which is introduced additively.

CO color space is obtained from RGB by linear transform:

$$\begin{aligned} A &= R + G + B \\ BY &= 2B - R - G \\ RG &= R - 2G + B \end{aligned} \tag{1}$$

The perceptual studies revealed that CO color space is very good for hiding small color perturbations because it is very similar with the chromatic channels of human visual system. CO color space is used in color or texture recognizing algorithms (for example in human skin recognizing algorithms). It's been noticed also that modification made in BY (blue-yellow) direction are less perceptible to HVS than other directions [15]. For this reason, the proposed algorithm adds the mark in RG (red-green) and in BY direction; in the last case the gain factor is three times bigger than for RG direction.

The experimental results obtained for image from Fig. 1a) express the values of correlation function from equation (2), for both color directions RG and BY.

In Table 1 we note the correlation function values, for original and coded image and also after applying different attacks. The threshold that separates a marked image from an unmarked one is experimental chosen. For our results we choose a threshold equal to 2. This is the first disadvantage of detection based watermarking methods.

From the experimental results we notice that the mark isn't resistant to contrast, luminance or color modifications. We have to say that we used PhotoShop 7.0 for these attacks and the modifications made are visible.

The correlation coefficient is computed using this equation:

$$(i,j) = m,m \in M,image \cdot pixels \quad k = BY(i,j)$$

$$\rho = \frac{\sum_{m=0}^{M} k*W(k)}{N} \tag{2}$$

where N is the number of different values for A component, which means 255*3, BY are the marked coefficients and W is the mark sequence.

Table 1

Correlation function values, obtained after decoding the image from Fig. 1a) and the original one

The kind of attack	The values of the correlation function for marked image		The values of the correlation function for original (un-marked) image	
	BY	RG	BY	RG
No attacks	22	7	- 6	-2
4º rotation	18	6	- 6	-2
0.5 scaling	15	4	- 6	-3
59º rotation	18	6	-6	-2
Gauss blur	11	3	-6	-3
Gauss noise addition 5%	16	6	-3	-1
Uniform noise addition 15%	11	4	-1	0
Sharpening	22	8	-6	-2
JPEG Q =40%	10	2	-6	-3
. gif 32 colors	10	2	-5	-3
Brightness and contrast modifications	7	0	0	-2
Color modifications	10	3	-11	-3

For other kind of attacks we obtained very good results. The greatest advantage of our proposed method is its robustness to geometric attacks, because this kind of robustness it is very hard to obtain without important distortions or complex algorithms.

In [13] an adaptive, wavelet based watermarking algorithm is presented. The algorithm uses first level of discrete wavelet transform and adds the mark into all four sub-bands coefficients. It uses masking methods, based on Gauss stationary and non-stationary models. One masking method is spatial and the other one is based on wavelet coefficients, but both of them are using only the luminance component.

The coding method is given in relation (3), where W is the mark; S_0 and S_1 are maximum allowed distortions for a texture zone pixel and for a uniform zone pixel. They usually are around 5 to 15 for S_0 and 3 for S_1 for most of real world and computer generated images [18]. NVF (Noise Visibility Function) is the gain factor adaptive value calculated with one masking method [18].

$$I_W = I + (1 - NVF) * W * S_0 + NVF * W * S_1 \quad (3)$$

In the decoding step, we build a vector from wavelet coefficients of the possible marked image and compute the normalized correlation coefficient between information vector and mark. The expression of normalized correlation coefficient is in (4).

$$C = \frac{1}{N} \frac{\sum_{i=0}^{N-1} \left(I_{W,i} - \mu_{I_w}\right) \cdot \left(W_i - \mu_W\right)}{\sigma_{I_w} \sigma_W} \quad (4)$$

where N is the mark length, I is image vector, W is the mark, μ_I and μ_W are corresponding means and σ_I and σ_W are corresponding standard deviations.

We use a correlation test to establish if the image was marked or not. Test value (5) has a Student repartition law with N-2 freedom degrees. For a very high N – usually bigger than 35 – we can consider that Student law is very similar with the standard Gauss law.

$$t = \sqrt{N-2} \cdot \frac{C}{\sqrt{1-C^2}} \quad (5)$$

where t is the value test of a correlation test

Following the correlation test, we compare the test value, t, with $\alpha/2$ fractal of normal standard law - $z_{\alpha/2}$ -, where α is the significance level we choose. If t exceeds $z_{\alpha/2}$ there is a dependency between the input vectors of the normalized correlation coefficient and the test image is considered marked. If t is smaller than $z_{\alpha/2}$ the two input vectors are independent and the test image isn't marked. In these conditions, first type error is α - the probability to say that a test image isn't marked when it actually is marked, $P(|t| < z_{\alpha/2})$

Let's say that normalized correlation coefficient value is 0.01. For N = 65536 and after relation (5), t is 2.559. We compare this value with a chosen threshold $z_{\alpha/2}$ and decide if the image is marked or not. $z_{\alpha/2}$ is chosen for an accepted type I error. So, for type I error equal with α=0.05 we have $z_{\alpha/2}$ = 1.96 and a normalized correlation coefficient greater than 0.01 means a marked image. In Table 2, we consider the image marked if the correlation coefficient exceeds 0.03. The experimental results from Table 2 are obtained for coded image from Fig. 2. We used the same kinds of attacks and with the same intensities as we used in evaluating results for the first algorithm. From these results we notice than the algorithm is fragile to geometric attacks. The reason for this is the disturbing of

synchronization between mark and image introduced by a geometrical modification. This is why the algorithms robust to geometric attack are a different category of watermarking algorithms. This method is robust to all non-geometric attacks, even to strong color, contrast or luminance modifications.

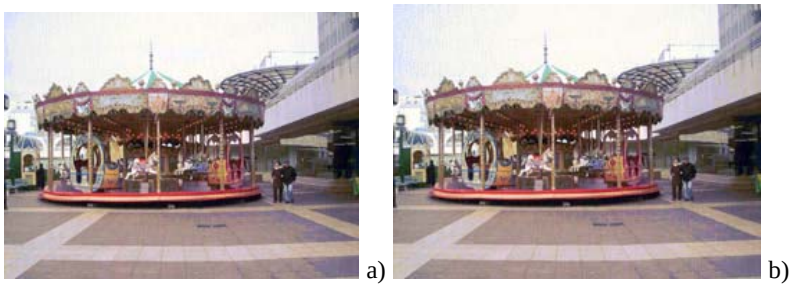
This section presented two different watermarking methods for digital color images. The experimental results of these two methods are complementary: the spatial algorithm, dedicated to color pictures, is robust to geometric attacks and to non-geometric attacks that doesn't significant affects colors; the wavelet based algorithm is robust to all kinds of non-geometric attacks, but the mark cannot be detected if the synchronization between image and mark was affected.

Applying both methods to the same image, we obtain the image from Fig. 2. From Fig. 2, a) and b) we notice that the order of methods isn't relevant; image quality is very good in both cases.

Fig. 1: a) marked image using a spatial algorithm, based on CO color space b) image marked using a frequency based watermarking algorithm

In Table 3 we have the experimental results for image from Fig. 2a) and for original one, after applying both decoding methods. The attacks and their intensities are the same from the previous evaluations (Table 1 and 2) and we also preserve the threshold: 2 for the first method and 0.01 for the second one.

The experimental results for both methods show that a dual coding gathers all the advantages of the component methods, without disturbing image quality. Using two simple watermarking techniques we obtain a fast, very efficient and very robust method.



a) b)

Fig. 2: a) image marked using the spatial algorithm first and frequency based watermarking algorithm second; b) image marked using the frequency based watermarking algorithm first and the spatial algorithm second

Table 2

Correlation function values, obtained after decoding the image from Fig. 1b) and the original one

The kind of attack	The values of the correlation function for marked image	The values of the correlation function for original (un-marked) image
No attacks	0.021	0.387
4º rotation	0.0099	*0.0096*
0.5 scaling	0.014	*0.014*
59º rotation	0.0046	*0.0038*
Gauss blur	0.023	0.122
Gauss noise addition 5%	0.019	0.272
Uniform noise addition 15%	0.016	0.258
Sharpening	0.019	0.576
JPEG Q =40%	0.024	0.039
. gif 32 colors	0.019	0.073
Brightness and contrast modifications	0.017	0.315
Color modifications	0.025	0.226

Table 3

Correlation function values, obtained after decoding the image from Fig. 2a) using both decoding methods

The kind of attack	The values of the correlation function for marked image decoded using the spatial method (BY/RG)	The values of the correlation function for marked image decoded using the method based on wavelet transformation
No attacks	18/6	0.34
4º rotation	15/5	*0.013*
0.5 scaling	13/4	*0.0064*
59º rotation	15/5	*0.021*
Gauss blur	10/3	0.104
Gauss noise addition 5%	14/5	0.364
Uniform noise addition 15%	12/4	0.239
Sharpening	16/5	0.476
JPEG Q =40%	9/2	0.03
. gif 32 colors	21/7	0.0694
Brightness and contrast modifications	*8/0*	0.255
Color modifications	*8/3*	0.227

6. Conclusions

In this paper a dual watermarking technique is presented. The method is based on two different and complementary techniques, a spatial, color-based method and an adaptive wavelet based one. Watermarking techniques evolution and their multiple utilizations in so many different areas impose fast and efficient solutions. For achieving a qualitative marked image and a robust mark we prefer a combination of simple watermarking methods, instead of a complex algorithm. The results are very good and cover a great area of attacks, both geometrical and non-geometrical.

R E F E R E N C E S

[1] *Emir Ganic, Scott D. Dester, Ahmet M Eskicioglu,* Embedding Multiple Watermarks in the DFT Domain using Low and High Frecquency Bands, 2004
[2] *Mauro Barni, Franco Bartolini, Vito Cappellini, Alessandro Piva*, A DCT-Domain system for robust image watermarking, 1997
[3] *Zhao Dawei, Chen Guarong, liu Wenbo,* A chaos-based robust wavelet domain watermarking algorithm, 2004
[4] *SAM Gilani, I Kostopoulos, AM Skodras,* Color image-adaptive watermarking, 2003
[5] *Selena Kay, Ebroul Izquierdo,* Robust content-based image watermarking, 1999
[6] *Jin D Seo, Chang Yov*, Localized Image Watermarking Based on Feature Points of Scale Space Representation, 2003
[7] *BS Kim, JG Choi, CH Park, JU Won, DM Kwak*, Robust digital image watermarking method against geometrical attacks, 2003
[8] *HD Cheng, XH Jiang, Y Sun, Jinghi Wang*, Color Image Segmentation: advances and prospects, 2000
[9] *M Radulescu, F Ionescu, C Stoica, V Stoica*, Adaptive watermarking – two ways to define it 2005
[10] *M Kutter, FAP Petitcolas*, A fair benchmark for image watermarking schemes
[11] *A B Watson*, Visual optimization of DCT Quantization Matrices for individual Images, 1993
[12] *S Suthaharan, SW Kim, HK Lee, S Sathananthan*, Perceptually Tuned Robust Watermarking Scheme for Digital Images, 1998
[13] *Hyun-Chun Kim, Ki-Ryong Kwon, Jong-Jin Kim,* Adaptive Image Watermarking Using a Stochastic Multiresolution Modeling, 2002
[14] *Y Deng, BS Manjunath, H Shin*, Color Image Segmentation
[15] *S Battiano, D Catalano, G Gallo, R Gemaro*, Robust Watermarking for Images based on Color Manipulation, 1999
[16] *Mustak E Yalcin, Yoos Vandewall*, Fragile watermarking and Unkeyed Hash Function Implementation for Image Authentification on CNN-UM, 2002
[17] *Kaznya Tsuruta, Yoshifumi Nishio*, Reversible Watermarking Techniques using Small-World Cellular Neural Network, 2005
[18] *Sviatoslav Voloshynovskiyyz, Alexander Herrigely, Nazanin Baumgaertnery, Thierry Punz*, A Stochastic Approach to Content Adaptive Digital Image Watermarking,1999