Digital Watermarking Based on Image Centroid Resistant to Rotation and Scaling

J. Alberto Méndez-Polanco, A. Cristina Palacios García, Raúl Rodríguez-Colín, Claudia Feregrino-Uribe
National Institute for Astrophysics, Optics and Electronics
Luis Enrique Erro No. 1, Sta. Maria Tonantzintla, Puebla, Mexico C.P. 72840
{polanco, raulrc, cferegrino}@inaoep.mx

Abstract

In this paper an algorithm resistant to geometrical (rotation and scaling) distortions is presented in order to embed a watermark based on the centroid of a color image. Tests with different kinds of color images and different watermarks were made and the results are compared against other approach.

1. Introduction

Watermarking schemes are methods used to protect intellectual property in digital contents. These methods are based on the insertion of watermarks such as text or images which carries author information.

Usually, the watermarking schemes must satisfy some properties [1]:

- **Imperceptibility:** It refers to the fact that the embedded watermark is imperceptible if the degradation in the watermarked image is difficult to detect.

- **Capacity:** The amount of information that can be hidden without degrading the image quality. This amount depends on the application (copyright protection, fingerprint, medical safety, etc).

- **Robustness**: In analogy to cryptography, the robustness of watermark schemes is measured by their resistance to different types of attacks such as compression, filtering, geometrical attacks, etc.

One of the most important properties is the robustness; however, if the information to be hidden corresponds to digital images, there is a great variety of attacks that can be generated. It makes difficult to get similar robustness to the security that may be found in cryptographic systems. Many of the watermarking schemes fail when the image is geometrically distorted, i.e., if a rotation or scaling is applied to the image where the information was hidden, this information can be lost.

In general, a color image can provide more perceptual information, i.e., sufficient evidence, against any illegal copyright invasion. However, in the past few years, most researches focused on developing watermarking schemes for gray-level images. Only a comparatively small number of researches on color image watermarking can be found, whereas their application to color images is scarce and usually works on the luminous or individual color channel. Kutter et al. [6] proposed a color image watermarking scheme that embeds the watermark into the blue-channel of each pixel by modifying its pixel value. Alterations made in the blue channel are less sensitive to the human eyes.

Ke Ding once proposed a scheme [3] to protect copyright based on image centroid resistant to rotation and scaling for gray-level images. In this paper, we extend the original scheme for color images and make some modifications to further improve performance. The proposed scheme is robust against geometrical distortions caused by rotating or scaling the host color image. This paper is organized as follows: section 2 shows the most used methods to embed watermarks in digital images; section 3 studies the process of inserting or extracting the watermark based on the image centroid. Section 4 shows the test carried out for the scheme applied in different images and finally conclusions are drawn in section 5.

17th International Conference on Electronics, Communications and Computers (CONIELECOMP'07)
0-7695-2799-X/07 $20.00 © 2007 IEEE

2. Image Watermarking

The difficulty to hide the watermark in the image depends on the format used, i.e. JPEG, BMP, PNG, GIF, etc. The most appropriate ones are those without data compression due that the higher the redundancy the lower the effect caused by an alteration in the watermarked image. Furthermore, the use of 24 bit/pixel images is better than 8 bits/pixel images due to the higher capacity they have. There are several watermarking schemes [5] some of them are described next.

2.1. Modification of the Less-Significant-Bit (LSB)

Least significant bit (LSB) embedding is a common and simple approach to insert information in a host image. This kind of scheme is vulnerable to even a slight image manipulation. This technique involves replacing the ***n*** least significant bits of each pixel of a host image with the data of a message to hide.

2.2. Statistical Approximation

It deals with the modification of some statistics of the image to keep information. A simple example would be the increase and decrease of brightness of certain pixels of the image. The pixel selection is determined by a pseudorandom number generator. In this way, the statistic of the difference between two pixels from the image taken randomly is altered.

2.3. Texture Block Coding

It consist on selecting and copying a portion of the image determined by texture (herbs, asphalt, etc) in other area of the image with similar characteristics. In this way two zones with identical textures can be obtained from the image. To detect these regions in a watermarked image it will suffice to calculate the image self-correlation to detect the position, and subtract the image itself but shifted to the position indicated by the self-correlation. After this process, zones where the difference is 0 can be appreciated. The geometrical form described by the profile of the copied zone may be the watermark (industry name, geometrical figure, etc). If the entire image suffers a uniform transformation, both regions will be affected in the same way and it will be possible to detect these two equal parts. However, this method requires a visual inspection to detect possible zones to copy, and the visual impact that the process produces.

2.4. Watermarking in Transform Domain

These schemes hide information in frequencies domain of the images, changing the value of the spectral coefficients. Most of these approaches are inspired in coding and compression methods (DCT, DFT and DWT).

3. Watermarking Scheme

In this section the proposed watermarking scheme based on the work of P. Bas et al. [2] and Ke DING et al. [3] is explained. This scheme is divided in three stages:

- Calculate the reference circle based on the centroid of the image.
- Transform the rectangular watermark in a circular watermark representation.
- Embed the circular watermark in the host image.

In the next sections, the method to obtain the circular reference is presented; after that, the embedding and the extracting process are explained.

3.1. Statistical Approximation

In order to increase the robustness of the watermark embedded in the host image against geometrical distortions, the watermark must be embedded in certain points of the image that are invariant to this kind of attacks.

To find these points the invariant features of the gravity center or centroid of an image are used. Let $f(i,j)\ \ 1 \le i \le N, 1 \le j \le N$ be a gray-scale level pixel of the host image. The gravity center of the host image is $M(m_x, m_y)$ is calculated using (1):

$$m_x = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} i \cdot f(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{N} f(i,j)} \qquad (1)$$

$$m_y = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} j \cdot f(i,j)}{\sum_{i=1}^{N}\sum_{j=!}^{N} f(i,j)}$$

In addition to the host image, we have to obtain a supplement image defined by:

$$\tilde{f}(i,j) = G_{level} - f(i,j) \qquad (2)$$

Where G_{level} is the maximum gray-scale level of the host image. Likewise as the host image, we obtain the gravity center of supplement image denoted by $M' = (m'_x, m'_y)$. The distance between M and M' is close, because the gravity center in the host image is near to the center of gravity of the supplement image. In order to be able to hide more information, the distance must be higher. To obtain a higher distance between the gravity centers, the equation (1) is modified to obtain a gravity center using a quantization parameter Δ as it can be seen in (3).

$$m'_x = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} i \cdot \left(f(i,j)/\Delta\right)}{\sum_{i=1}^{N}\sum_{j=1}^{N} \left(f(i,j)/\Delta\right)} \qquad (3)$$

$$m'_y = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} j \cdot \left(f(i,j)/\Delta\right)}{\sum_{i=1}^{N}\sum_{j=!}^{N} \left(f(i,j)/\Delta\right)}$$

Up to now, the watermark is not embedded in the host image and the parameter Δ is only used to calculate the gravity centers.

The next step consist on calculating the Euclidean distance between the obtained gravity centers; the Euclidean distance is called *reference distance* and can be denoted as L_{ref} and is obtained using (4).

$$L_{ref} = \sqrt{\left(m'_x - \tilde{m}'_x\right)^2 + \left(m'_y - \tilde{m}'_y\right)^2} \qquad (4)$$

The center of the reference circle that will be used to embed the watermark is:

$$O = \left(\frac{m'_x + \tilde{m}'_x}{2}, \frac{m'_y + \tilde{m}'_y}{2}\right)$$

3.2. Circular Watermark Generation

Once calculated the reference circle and reference distance L_{ref} the next step is to generate the circular watermark using a Cartesian mapping to polar mapping and vice versa.

Let P and Q be the dimension of the rectangular watermark (fig. 1); the reference circle is divided in homocentric regions. In order to generate the circular watermark, the X and Y axis of the rectangular watermark are mapped to a radio and to the direction angle of the reference circle. The relation between rectangular and circular watermarks coordinates are:

$$x = \frac{r_i - r_0}{r_M - r_0} \cdot P; \quad y = \frac{\theta}{\Pi} \cdot Q \quad if\ 0 \le \theta \le \Pi$$

$$x = \frac{r_i - r_0}{r_M - r_0} \cdot P; \quad y = \frac{\theta - \Pi}{\Pi} \cdot N \quad if\ \Pi \le \theta \le 2\Pi$$

where x, y are the rectangular watermark coordinates, r_i and θ are the circular watermark coordinates, r_M is the radio of the reference circle, i.e. $L_{ref}/2$.

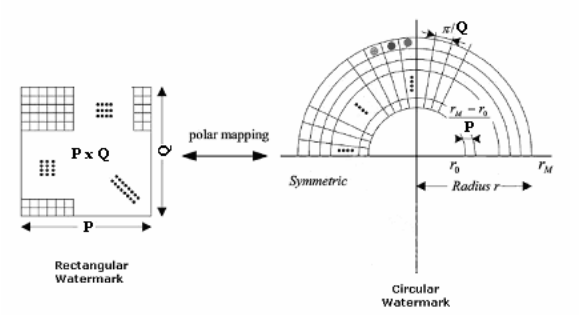


Figure 1 Rectangular watermark to circular watermark transformation [2].

3.3. Watermark Embedding

The steps to embed the circular watermark in the host image are:

- Decompose the host color image in its RGB components.
- For each color component image:
  - Calculate the reference circle based on the gravity center as shown in section 3.1.
  - Generate the circular watermark, section 3.2.

Map circular watermark to Cartesian coordinates and embed the data using a LSB method.
A diagram of watermarking scheme can be seen in figure 2.

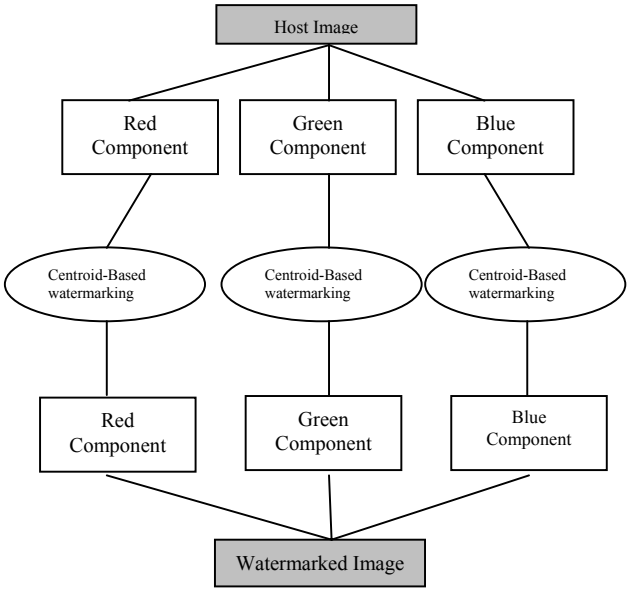


Figure 2 Diagram of the watermarking method.

3.4. Watermarking Extraction

The process to recover the watermark is:

- Decompose the watermarked image in its RGB components.
- For each color component image calculate the gravity centers, obtain the supplementary images and calculate the centers of gravity of the supplementary images.
- Based on the gravity centers, obtain the reference distance between each component of the watermarked image and its corresponding supplementary images, get the centers of the reference circles of each couple of images.

Using equation (5) obtain the polar coordinates in which the data was embedded with a LSB method.

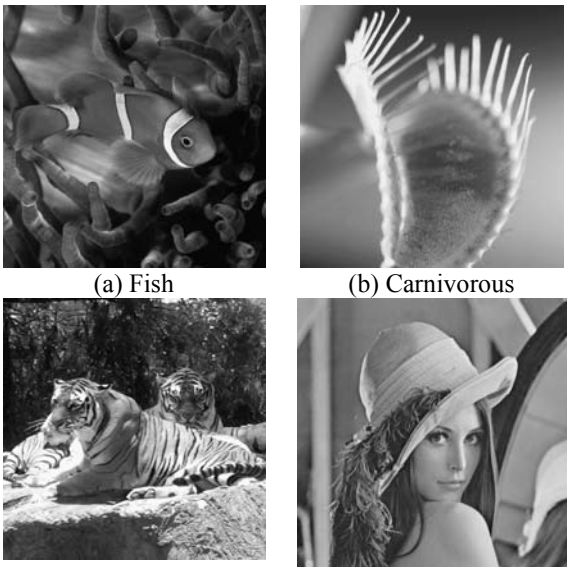
4. Experimental Results

The proposed embedding and extraction process was implemented in MatLab. Figure 3 shows the interface of the application. It shows the image to hide the information, the points selected to hide the information and the watermarked image. It allows also selecting the watermark to hide and the results.

Figure 3 Graphic interface implemented in MatLab.

The tests carried out in different kinds of images and several geometrical attacks. The images used in the experiments are 512x512 color images with 8 bits for each channel pixel. Figure 4 shows some host images used in the simulations. For each host image, a corresponding palette was generated by ACDSee version 5.0.1 with optimal palette selection. Each palette consisted of 256 colors and was indexed from 0

to 255. Each color in the palette contained RGB channels.



(a) Fish (b) Carnivorous

(c) Tiger (d) Lena

Figure 4 Four color host images of 512 *x* 512 pixels.

Likewise were used several watermarks of size 32x32 pixels, i.e. a 1024 bits. The quantization parameter (3) used in the tests was Δ=16. This value was obtained according to some experimental results reported in [3].

To evaluate the similarity between the original watermark and the recovery watermark after a geometrical distortion, we use the normalized cross-correlation (*NCC*).

$$NCC = \frac{\sum_{i=1}^{P}\sum_{j=1}^{Q} W(i,j)W'(i,j)}{\sum_{i=1}^{P}\sum_{j=1}^{Q} |W(i,j)|^2} \qquad \textbf{(6)}$$

Where *W* is the original watermark image, *W'* is the recovered watermark and the watermark size is *P* x *Q*.

To evaluate the degradation between the original image and the watermarked image, we use the peak signal-to-noise ratio (PSNR).

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE}$$

where **(7)**

$$MSE = \frac{1}{N \times N} \sum_{i=1}^{N}\sum_{j=1}^{N} (c_{i,j} - c'_{i,j})^2$$

$c_{i,j}$ denotes a pixel color of the original host image and $c'_{i,j}$ denotes a pixel color of the watermarked image, finally $N \times N$ is the image size.

When a geometrical transformation (rotation and scaling) is applied, the image requires interpolation that can be *nearest*, *bilinear* or *bicubic* [4]. In the experiments carried out the nearest interpolation was used.

Figure 5 shows the different watermarks used in the experiments.

(a) 32 x 32 binary image

(b) 32 x 32 binary image

(c) 32 x 32 binary image

(d) 64 x 64 binary image

Figure 5 Watermark used in the experiments.

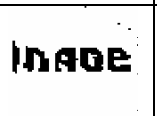
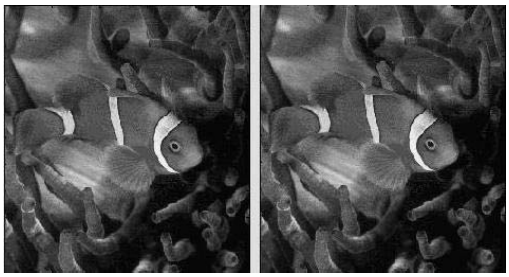
	The proposed scheme		
Scaling	2 times	3 times	4 times
Correlation	0.99726	0.99726	0.99726
PSNR	79.6444	79.6444	79.6444
			
Rotation	33 degrees	45 degrees	70 degrees
Correlation	0.99725	0.99505	0.99643
PSNR	32.1837	31.7598	33.1427
			
Rotation and Scaling	33 degrees and 2 times	33 degrees and 4 times	45 degrees and 2 times
Correlation	0.99613	0.99613	0.99505
PSNR	31.9531	31.9531	31.7598
			
	Sal y pimienta		
Correlation	0.99725		
PSNR	41.6553		
			

Table 1. Experimental results of the proposed scheme.



a) Original b) Watermarked

Figure 6 Example of original image and watermarked image.

Figure 6 shows the original image and watermarked image (watermark from figure 3a). It can be seen that there is no significant degradation for the human vision.

In figure 7 we present the recovered watermarks after applying several attacks on the watermarked image.

a) b) c) d)

Figure 7 Recovered watermarks after several attacks.

Image	Attack	NCC
Fig. 7 a)	Scaling 2 times	1
Fig. 7 b)	Rotating 33 degrees	0.98083
Fig. 7 c)	Rotating 45 degrees	0.98309
Fig. 7 d)	Rotating 33 degrees and scaling 2 times	0.98985

Table 2. Results obtained after the watermark extraction process.

Figure 8 shows the results comparing the percentage of recovered watermarks using the RGB components against the use of the gray-scale component to embed the watermark.

Table 1 lists the experimental results. The experiments show that the recovered watermarks can all be easily recognized after the attacks. It also shows that the proposed scheme outperforms the previous one for each attack. The accuracy rates are all higher than 99%. Table 1 also shows the *PSNR*. We use the *PSNR* as a measurement to express how severe the host image is attacked. The smaller the PSNR is, the more dissimilar the attacked image is. Usually, '36' is a tolerable bottom line. Observing Table 1 and Table 2, we can see that the host image comes under severe attacks.

0-7695-2799-X/07 $20.00 © 2007 IEEE

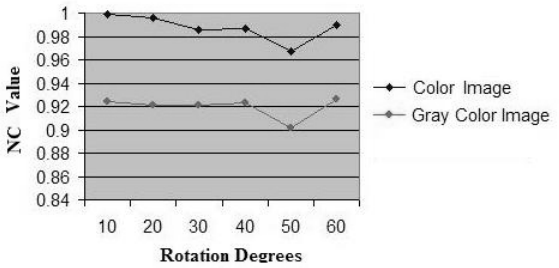


Figure 8 RGB components vs. gray-scale component.

Note that better results are obtained with scaling attacks (Table 1). From figure 8 it can be seen that as the rotation degrees increase, there is a slight difference of the NCC value.

5. Conclusions and future work

In this paper a watermarking method robust to geometrical (Rotation and scaling) was presented. Several watermarks and images in gray-scale and color were used obtaining good results. Further improvements may be done in the recovering watermarking process, due to the way the information that is inserted in the image depends mainly on calculated gravity centers. A wrongly calculated gravity center, even by a difference of a pixel, may cause a totally incorrect recovering of the watermark. As future work we will extend this algorithm in order to have a more robust watermarking scheme and enhance the security to avoid watermark detection.

6. References

1] Puech W., Rodrigues J.J.: A new crypto-watermarking method for medical images safe transfer. *In Proceedings of the 12th European Signal Processing Conference*, Vienna Austria (2004) 1481-1484.

[2] P. Bas, J.M. Chassery, and B. Macq. "Geometrically invariant watermarking use feature points", *IEEE Tans. Image Process.*,vol. 11, no. 9, pp 1014-1028, 2002.

[3] Ke Ding, Chen He, Ling-ge Jiang, Hong-xia, Wang, Geometrically Invariant Watermarking Based on Gravity Center, *IEICE Trans Fundamentals*, vol. E87-A, No. 2, pp 513-515, February 2004.

[4] Gonzalez, RC, Woods, RE, Digital Image Processing, Reading, MA: Addison-Wesley, 1992.

[5] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography." *IEEE Journal of Selected Areas in Communications*, vol. 16, no. 4, pp. 474-481, May 1998.

[6] M. Kutter, F. Jordan, F. Bossen, Digital signature of color image using amplitude modulation, in: I.K. Sethi, R. Jain (Eds.), *Storage and Retrieval for Image and Video Databases* V, Vol. 3022, SPIE, San Jose, CA, February 1997, pp. 518–526.