Communications to SIMAI Congress,
ISSN 1827-9015, Vol. 1 (2006)

DOI: 10.1685/CSC06002

A wavelet-based watermarking for digital images of different size

Santa Agreste
Department of Information Science, University of Milan
Via Comelico, 39/41 - 20135 Milano
agreste@dsi.unimi.it

Guido Andaloro
Department of Mathematics, University of Messina
Salita Sperone, 31 - 98166 Messina
guandalo@dipmat.unime.it

Abstract

We describe a digital watermarking algorithm for color images protection and authenticity: robust, not-blind, wavelet-based. Our algorithm can process any image, in fact it includes resize techniques that adapt the size of original image for Wavelet transform. The watermark signal is calculated in correlation with the image features and statistic properties. In detection step we apply a re-synchronization between the original and watermarked image according to the Neyman-Pearson statistic criterion. Experimentation on a large set of different images has shown to be resistant against geometric, filtering, and StirMark attacks with a low rate of false alarm.

1. Introduction

The growth of the Internet has increased the phenomenon of the digital piracy, in multimedia objects, like software, image, video, audio and text. Protection of these assets is usually based upon the insertion of digital watermark. The watermarking software introduces, into the object being watermarked, small intensional errors, called *marks*, that must not have a significant effect on the usefulness of the data. This error can be visible or not visible, depending on the object under watermarking. The watermark must be *robust*, that is it should not be removable by unauthorized person and should be resistant against intentional and unintentional attacks. Thus, the watermark does not prevent copying, it deters illegal copying so as to provide a means for establishing the original ownership of a redistributed copy.

The watermarking algorithm is particularly useful to protect the digital images. In general, an algorithm of watermark is consisting of two steps: watermark embedding and watermark detection. According to embedding process, the watermarking techniques can be classified in two categories such as spatial domain methods and transform domain methods [4]. Spatial domain techniques are less complex but they are less robust to tampering and geometrical attacks than transform domain techniques which locate the watermark signal in the most perceptually significant components of a transform domain (Fourier, Wavelet, Cosine), [3], [7], [6]. Another classification of digital watermarking algorithm can be made according to the detection step in private (*not blind*) and public (*blind*), in fact the first requires the original image during this process.

The rest of the paper is organized as follows: in section 2 we describe in detail the proposed algorithm, in the section 3 we explain our strength points, in the section 4 we present some experimental results and in sections 5 we report the conclusive remarks.

2. Watermarking Algorithm

The realized algorithm is a watermarking not blind one, which embeds watermark signal into high-frequency sub-bands Discrete Wavelet Transform (DWT) coefficients, in according to the Human Visual System directives [5]. It makes a pre-processing of the image depicting it into component Value of color model HSV (Hue, Saturation, Value) and resizing the Value matrix according to the parameters and mathematical base conditions of DWT, that is we modify one, or more, block (called C) of the original plane matrix whose order is a power of 2. Wavelet function and DWT level decomposition are fixed respectively according to image features and image resize. In the embedding process, watermark signal and DWT coefficients to be modified are chosen depending on the statistic function values of the image. Both in embedding step and in detection step, original image I and watermarked image $\tilde{I}$ (in the latter phase) are computed the same steps from pre-processing to DWT decomposition.
This algorithm has been implemented in MatLab 6.x using the image processing, wavelet and statistic toolbox.

2.1 Watermark Embedding

Let C be the matrix associated to block to be watermarked. In the watermark embedding step DWT decomposition is applied to C, k-times, depending on C dimension, to obtain the 4 sub-matrices C_k^{LL}, C_k^{HL}, C_k^{LH}, C_k^{HH} of order $n_k = n/2^k$, that have, as elements, the DWT coefficients of the k-th decomposition level. Only the entries of high frequencies details matrices C_k^{θ}, where $\theta \in \{HL, LH, HH\}$ are modified by watermark. Watermark embedding is calculated with following formulas:

$$\tilde{C}_k^{\theta}(i,j) = C_k^{\theta}(i,j) + \omega * \alpha(i,j) \qquad i,j = 1,2,...,n_k \tag{0.1}$$

where α is a weight matrix of order equal to the order of C_k^{θ} whose generic element $\alpha \in \{-1,0,1\}$ is chosen depending on the to an interval belonging of the corresponding DWT coefficient. The interval depends on false alarm probability P_f and from ω, that is equal to standard deviation (STD) of the DWT coefficients. To determine α we consider the variance σ^2:

$$\sigma^2 = \frac{1}{(3N)^2} \sum_{\theta} \left[\sum_{i=1}^{n_k} \sum_{j=1}^{n_k} \tilde{C}_k^{\theta}(i,j)^2 - C_k^{\theta}(i,j)^2 \right] \tag{0.2}$$

and the probability of false positive P_f:

$$T_{\rho} = erfc(2 * P_f * \sqrt{2\sigma^2}) \tag{0.3}$$

where *erfc* denote the error function. Thus the value of weight matrix element $\alpha(i,j)$ is:

$$\begin{cases} \alpha(i,j) = 0, & \text{if } -\omega < C_k^{\theta}(i,j) < \omega; \\ \alpha(i,j) = 1, & \text{if } C_k^{\theta}(i,j) > T_{\rho}; \\ \alpha(i,j) = -1, & \text{otherwise} \end{cases}$$

The Inverse Discrete Wavelet Transform (IDWT) is computed k-times on $\tilde{C}^{\theta}_{k}$, obtaining $\tilde{C}$, so we apply the inverse pre-processing scheme then we store in JPEG format to obtain the watermarked image.

2.2 Watermark Detection

Watermark is detected computing the correlation ρ between the watermarked coefficients and watermark signal, in comparison to the threshold T_ρ, where:

$$\rho = \frac{1}{3N} \sum_{\theta} \left[\sum_{i=1}^{n_k} \sum_{j=1}^{n_k} \tilde{C}^{\theta}_{k}(i,j) - C^{\theta}_{k}(i,j) \right] \tag{0.4}$$

To compute T_ρ we supposed that the probability of false positive detection P_f is fixed to 10^{-8} and we computed σ by (0.2).

$$P_f \leq \frac{1}{2} erfc(\frac{T_\rho}{\sqrt{2\sigma^2}}) \tag{0.5}$$

Then if $\rho > T_\rho$ watermark signal is detected, otherwise watermark signal does not detected.

3. Our Strength Points

A strength point of our algorithm is the mixed use of DWT e HSV color model. In fact Human Visual System considerations indicate that the eye is less sensitive to noise in those areas of the image where brightness is high or low. Moreover two fundamental considerations suggested us to apply the wavelet transform not on the whole Value matrix of the original image, but on its sub-matrices: the first reason is that, in this way, the watermark can well cover the whole image and the second reason is that the host images can have different dimensions when they belong to real multimedia galleries.

3.1 More Extension of the Watermark

After splitting the Value plane of the original image, to create the block C (or, similar, $\tilde{C}$ to watermarked image in the detection) we check the ratio between the row and column number (and viceversa). If it is bigger than 2 (as Figure 0.1), to support a good mark distribution, we divide ideally the plane by entire part of the ratio, so on each block we adapt the dimensions as described in next sub-sections.

3.2 Adaptive Dimension

To apply the wavelet transform, the matrix C must be square of order p power of 2. So we consider as order of matrix, the power of 2 that is nearest to the longest dimension of the original image. If the order of the matrix associated to the block is greater than the longest dimension of the original image, we insert crammed full information of image, as reply the pixel values of the first and last row, and of the first and last column (as the Value plane of image in Figure 0.2(b)).Otherwise we select the central part, power of 2, of the image, deleting the remaining part (as the Value plane of image in Figure 0.2(a)). It is also possible to have an hybrid of two previous case as the Value plane of image in Figure 0.2(c).

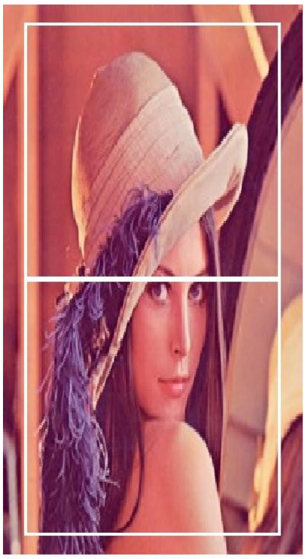
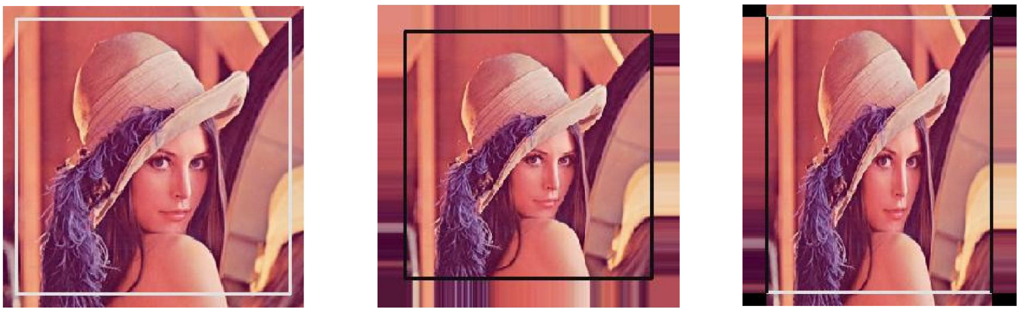


Figure 0.1: Example of more blocks for better extension of the watermark



(a) From original image (280x280x3) to resized (cutted) image (256x256x3)

(b) From original image (210x210x3) to resized (extended) image (256x256x3)

(c) Hybrid of cases shown in figure 0.2(a) and 0.2(b)

Figure 0.2: Example of adaptive dimension

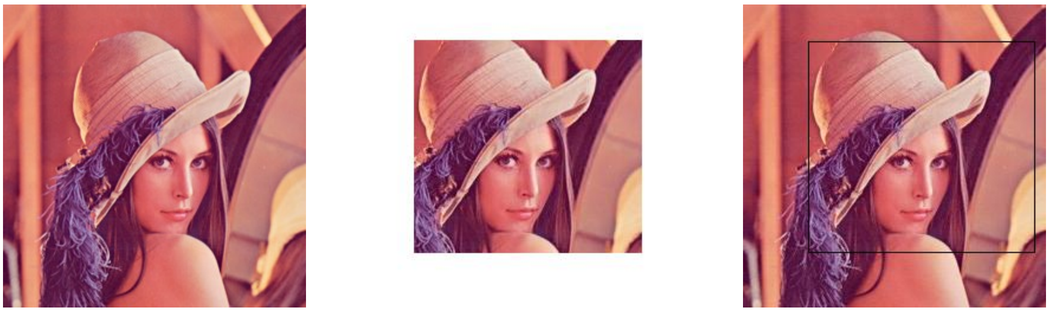
3.3 Synchronization between original and watermarked image

In detection step, we apply a check procedure to the size of original and watermarked image that might have been modified intentionally. If they are different a synchronization process (Figure 0.3) considers a central block of the original image to be used a comparison some blocks of the watermarked image by means the Mean Square Error (MSE) function, so as to resize the original image in order to make congruent both of them.

4. Attacks and experimental results

The experimentation consisted in testing the algorithm with regard to false alarm and attack resistance. To thus purpose 1000 images with different size have been used in low and high resolution, to build up a real and commercial database. Experimentation results have shown that our algorithm is robust against attacks of geometric operation, filters, and Stirmark [8], with ratio more than 88%. It has a low probability of false positive alarm. In particular, Figure 0.4 shows the values of ρ and T_ρ for different choice of P_f

from 10^{-15} to 10^{-5}.

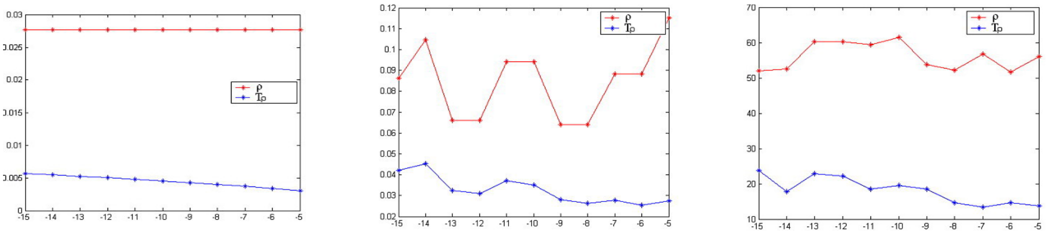


(a) Original Image of Lena

(b) Watermarked Attacked Image

(c) Synchronization process

Figure 0.3: Example of synchronization process



(a) Watermarked Image without attacks, plot of ρ and T_ρ

(b) Watermarked Image with Stirmark attack, plot of ρ and T_ρ

(c) Watermarked Image with geometric attack (cut-ut), plot of ρ and T_ρ

Figure 0.4: Plot of the values of ρ and T_ρ for different choice of P_f

5. Conclusion

In this paper, we have shown the features on an efficient wavelet-based watermarking algorithm for digital images. The watermark embedded has a high level of robustness against geometric and image processing attacks and a low rate of false alarm. Using DWT on HSV color model, image statistic features and image pre-processing step with blocks subdivision of the image, are key very efficient factors for the robustness, invisibility and a well signal watermark distribution over image.

References:

1. Agreste S., Castorina N., Giovinazzo S., Prestipino D., Puccio L.. *Tutela del diritto di proprieta'delle immagini digitali: Implementazione di un algoritmo di Watermark mediante funzioni Wavelet*, Atti della Accademia Peloritana dei Peric., Classe di Scienze Fis., Mat. e Nat. (on line). vol. LXXXI-LXXXII, 2005, pp. 1-15, ISSN: 1825-1242. Identification Number: C1A0401009 ID Code: 261.

2. M. Barni, F. Bartolini, A. Piva. Improved wavelet-based watermarking through pixel wisemasking. *Image Processing, IEEE Transactions* Volume 10, Issue 5, May 2001 pp.783 - 791.

3. F. M. Boland, J. J. K. Ruanaidh, W. J. Dowling. Watermarking digital images for copyright protection . *In IEEE Proceedings on Vision, Signal and Image Processing*, v. 143, n. 4, 1996, pp. 250-256.

4. I.Cox, ML. Miliier. A review of watermarking and the importance of perceptual modeling. *Proc of SPIE 1997*;3016:929.

5. Z. Dawei, C. Guanrong, L.Wenbo. A chaos-based robust wavelet domain watermarking algorithm. *ELSEVIER, Chaos, Solitons and Fractals* 22, 2004, pp. 47-54.

6. E. Koch, J. Zhao. Towards robust and hidden image copyright labaleing. *In Proc. of IEEE Workshop of Nonlinear Signal and Image Processing, Halkidiki, Greece, 1995.*

7. I. Pitas. A method for signature casting on digital images. *In Proc. of the International Conference on Image Processing*, v. 3, 1996, pp. 215-218.

8. Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn. Attacks on copyright marking systems,*in David Aucsmith (Ed), Information Hiding, Second International Workshop, IH98, Portland, Oregon, U.S.A., April 15-17, 1998, Proceedings, LNCS 1525, Springer-Verlag*, ISBN 3-540-65386-4, pp. 219-239.

9. A. H. Tewfik, M. Swanson. Data hiding for multimedia personalization, interaction, and protection. *IEEE Signal Processing Mag., vol. 14, pp. 4144, July 1997.*