

Approaches on watermarking

Leonardo Carneiro Araujo

Abstract—A watermarking approach for copyright protection and content authentication based on wavelets decomposition is proposed here. The scheme proposed works for color images, since it relays on hiding the watermark in the chrominance channels in order to make it invisible. Experimental results show that the watermark could be invisible, still retrievable and resist to distortions such as noise, crops and shifts.

Index Terms—Authentication, copyright protection, image watermarking, wavelets, Fourier transform, robust watermarking.

I. INTRODUCTION

Watermarks are images of patterns usually applied to a piece of paper which shows more bright when seen through the transmitted light or darker when seen under reflected light. The watermarks were first created in 1281, Bologna (Italy). Watermarks are used as a way to authenticate and certifies the origin of documents or products. They are largely used in stamps, bills and other documents.

With the expansion of telecommunications, especially the Internet, bringing an abundance of multimedia content, rises the problem of ownership protection of digital information. Although a good progress has been made on the last couple years, many challenging problems still remains. The watermark should be invisible, so that it does not affect the quality of multimedia data, and it should be difficult for nonauthorized personnel to remove or counterfeit it. It should also be spread all through the multimedia content, so that every little piece is watermarked itself. Among the problems, an outstanding one is the resilience of watermarking to distortions, what could include noise and geometric attacks, such as: scaling, cropping, translation, rotation, shearing, bending, change of aspect ratio or a combination of those. Such attacks can destroy the synchronization in the watermarked bit stream, which is vital for most of the watermarking techniques [7]. Another factor that would aggravate the watermark retrieval process is the absence of the original image. It is desirable to create a watermark which retrieval process does not depend on the availability of the original image.

Several approaches have been proposed to overcome geometric attacks. Ruanaidh and Pun proposed in their article [9] a scheme based on the invariant properties of Fourier-Mellin transform (FMT) to deal with distortions caused by rotation, scaling and translation (RST). It was a good theoretical approach, but hard to implement. An alternative, proposed in [3] is a watermarking algorithm which is also robust to RST and is obtained from a transform that is quite similar to the Fourier-Mellin transform. The watermark is embedded into a one-dimensional (1-D) signal obtained by taking the Fourier transform of the image, re-sampling the Fourier magnitudes into log-polar coordinates, and then summing a function of those magnitudes along the log-radius axis.

A different approach was proposed in [2]. This one is adaptive to the image content. Salient features points are first extracted from the image, defining a number of triangular regions. A 1-bit watermark is then embedded inside each triangle using an adaptive spread spectrum scheme. For this approach to work it is necessary to have a good detection of those salient points in the image.

In [7] two approaches are proposed. The first one is a multibit public watermarking scheme based on image normalization, which main concern is to be robust to general affine geometric attacks. This multibit schema is based on direct-sequence code division multiple

access (DS-CDMA). The second approach was based on a watermark resynchronization scheme, aimed to be robust to random geometric distortions and to be used in the context of private watermarking, where the original image is known. This scheme uses a deformable mesh model to correct the distortion so that the resynchronization is achieved.

Maximum-likelihood (ML) detection schemes based on Bayes' detection theory have been considered for images watermarking in transform domain. In [1] a decoding algorithm is presented which is optimum for nonadditive watermarks embedded in the magnitude of a set of full-frame discrete Fourier transform (DFT) coefficients of the host image. By relying on statistical decision theory, the structure of the optimum decoder is derived according to the Neyman-Pearson criterion, thus permitting to minimize the missed detection probability subject to a given false detection rate. To achieve optimum behavior of the maximum-likelihood detector, a probability distribution function (PDF) that correctly models the distribution of the discrete Fourier transform are modeled using Weibull PDF.

A Mexican Hat wavelet is used as a feature extraction in [11]. The extracted features points can survive a variety of attacks and be used as reference points for both watermark embedding and detection. A normalized image is nearly invariant to rotations [10], making the detection task simpler. If the image normalization process is applied to the entire image, it would be sensitive to cropping and local region distortion. It was applied the normalization to nonoverlapped image disks separately. The disks are centered at the extracted features points. The scheme proposed is robust to survive low-quality JPEG compression, color reduction, sharpening, Gaussian filtering, median filtering, row or column removal, shearing, rotation, local warping, cropping and linear geometric transformations.

In the article presented in [4], it is emphasized that many of the existing watermarking schemes are "focused on the robust means to mark an image invisibly without really addressing the *ends* of invisible watermarking schemes." They've shown that many existent invisible watermarking schemes cannot resolve the ownership problem of any image watermarked with multiple ownership signatures (what will be further explained). The same authors show in [5] some scoops on some watermarking schemes that do not require original images for watermarking detection. They suggested a watermark which results from a one-way hash of the original image. As in [12], many watermarking scenarios are not fake proof. It was shown that "for a particular application of resolving rightful ownership using invisible watermarks, it might be crucial to require that the original image not be directly involved in the watermark detection process."

II. THE CLAIM OF OWNERSHIP

A generalized formulation of watermarking schemes consists in, given the original image I , and a generated signature S , the process of embedding S in I may consist of a simple addition, creating a watermarked image I' which is visually close to I . We have then $I' = I + S$.

Given a test image X , assumed to have been watermarked, to determine its ownership, we extract the original image I from the test image X to obtain the signature S' , which is compared to the original signature S . A similarity measure is made of S' against S to determine if X is indeed a similarity version of I . However, this



Fig. 1. Binary watermark.

approach is not always safe, since it may allow multiple claims of ownerships. The pixel-wise subtraction of X and I is considered as a potential watermark inserted. If there is more than one person claiming to be the owner of the image, they may claim to have the original image simply creating a counterfeit original image X' which should be visually close to I . This image X' is created by a simple subtraction of X and the claimer signature S_X , $X' = X - S_X$. The image X and I are statistically equivalent, and the possessor of X may claim to have the original image X' , and both I and X to be watermarked versions of X' . In this scenario, there is no way to identify the true owner of the image.

A simpler scenario consists in the situation in which the possessor of X may claim to be the owner without even generating a third image X' . He may simply argue that X is indeed the original image and somehow the possessor of I took X and subtracted his signature, creating the image he claims to be the original I . In this case, the owner of I knows the relationship between X and I whereas the possessor of X does not. Since there is no way to verify which one is the original image, there is no way to decide who is the real owner.

Since the problem in watermarking process presented above are due to the invertible nature of the watermark (additive, in the case exemplified) encoding process, it was suggested in [4] the non-invertibility of the watermarking process, in order to establish rightful ownership. It is very hard, if not impossible, to design a noninvertible encoding process that results in watermarks that can be later extracted. It seems the main problem lays on the detection process, not in the watermark encoding process itself. A way to avoid those problems seems to be to detect the watermark without using a second image, which authenticity is also questionable.

III. APPROACHES

It is presented here some approaches and considerations devised by the author on the process of embedding an invisible watermark on images. Only the process of embedding a binary image watermark was considered here. In all examples, the watermark used is illustrated in figure 1.

As we intend to create a invisible watermark it would be appropriate not to add the watermark directly on the image domain, instead we have tested two approaches which consist on adding the watermark in the transform domain. We have used the Fourier transform and wavelet transform in order to do so. After carrying the original signal to the transform domain, we add the watermark to it and then we transform back to the signal domain. There might be many ways for adding the watermark to the signal, but only some of them are presented here. In either approach, wavelet's or Fourier's, we have

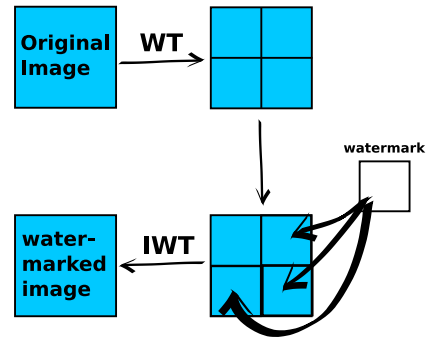


Fig. 2. Watermark wavelet embedding process.

at first tested to embed the watermark in a grayscale version of the image. In this approach we have realized that the watermark doesn't get invisible as desired and, for this reason, it would not attend the desired specification to watermark grayscale images. We know from [8] that the human visual perception is more accurate for luminance component than to the chrominance one. So we have chosen to hide the watermark only inside the chrominance channels. We performed the conversion from RGB to $YCbCr$ space, then we applied the transforms to Cb and Cr components and finally we embedded the watermark inside them. When we transform back again to the spatial domain we will have a better result than achieved when dealing with grayscale images.

The first approach proposed consists in taking the wavelet transform of the image and applying the watermark to its wavelets coefficients, but not to its scale coefficients, i.e. we add the watermark to the detail information provided by the wavelet transform (high frequency coefficients), but not to the coarse version (low resolution, low frequency coefficients). After doing this, we do the inverse wavelet transform to obtain the watermarked image. This process is shown in figure 2. As we might see on the results, the watermark seems invisible when its weight is low (see figure 5). The process of adding the watermark to the transformed image consists simply on adding a weighted matrix to the matrix of coefficients. The greater the weight the easier it will be to retrieve the watermark, but the greater will be its interference on the image. When we increase its weight the watermark doesn't become visible resembling the way the watermark looks like, but it resembles a noise, like a grid added to the image. As we add the watermark to the high frequency component of the image, inevitably it will not be resistant to low pass filtering, but it is resistant to shifting, noise (to a certain degree), cropping and a combination of them. We've also tested rotation but unfortunately, it was resistant only to rotations that are multiple of $\pi/2$. An example of a retrieved watermark after noise corruption is presented in figure 6. The signal to noise ratio in this example was $23dB$.

Another two approaches were tested by the author, but neither of them produced good results, so they are not reproduced here. One of them consists on simply adding the watermark to the chrominance channels. There is no way to retrieve the watermark, unless making it visible. The other approach consisted on performing the Fourier transform on the image and then apply the watermark to the phase of its chrominance channels, in order to make it invisible. Unfortunately, this approach also didn't show a good result.

IV. CONCLUSIONS

A watermarking scheme which can be applied to achieve both authentication and protection of image and video data has been presented in this paper. Once a watermark is embedded in the hiding process, it can be blindly extracted for different applications in

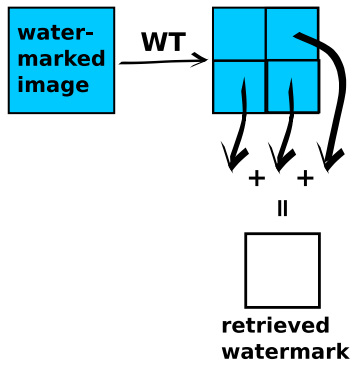


Fig. 3. Watermark wavelet retrieving process.



Fig. 4. Lenna (original image).

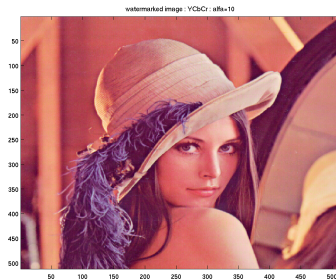


Fig. 5. Watermarked image.

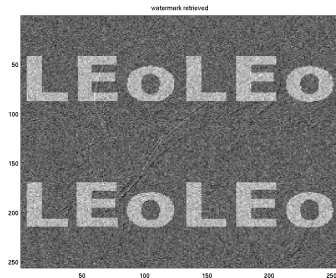


Fig. 6. Retrieved watermark.

the detection process. The wavelet based approach was successful in achieving an invisible watermark which is noise resistant to a certain degree. It showed not to be resistant to some distortions such as rotation and emboss, but was resistant to noise, reflection, $\pi/2$ multiple rotations, crops, shifts and combination of these. The proposed scheme works fine in color images, since it relays on hiding the watermark in the chrominance channels in order to make it invisible. Unfortunately, it doesn't solve completely the problem of ownership as described in the first section of this article.

There are still some issues that deserve further exploration. In the proposed approach, the watermark was embedded in the region which corresponds to the higher octave of the signal, what is a wide region. Maybe we could try to hide the watermark in a narrower region, in a way that we could make it stronger but still invisible. We could also try to wide the watermark in different subbands with different strengths, splitting the information and keeping it still invisible. In order to do so we have got to use a multiple filter bank wavelet decomposition as proposed in [6]. We would have more flexibility to design the wavelet filters, but it is still an open problem. We should also try to devise a general mechanism which can resist a greater variety of attacks. A wavelet transform variant could be used to make the watermarking resistant to rotation as well following the ideas on [3]. There are many possible schemes for embedding a watermark and only a very few were presented here. The key points still remains on how to make the watermark invisible but still retrievable after severe corruption process and how to make the watermarking process rightful to resolve authoring and authentication issues.

REFERENCES

- [1] Mauro Barni, Franco Bartolini, Alessia De Rosa, and Alessandro Piva. A new decoder for the optimum recovery of nonadditive watermarks. *IEEE Transactions on Image Processing*, 2001.
- [2] P. Bas, J.-M. Chassery, and B. Macq. Geometrical invariant watermarking using feature points. *IEEE Transactions on Image Processing*, 2002.
- [3] Jeffrey A. Bloom Ingemar J. Cox Matt L. Miller Ching-Yung Lin, Min Wu and Yui Man Lui. Rotation, scale, and translation resilient watermarking for images. *IEEE Transactions on Image Processing*, 2001.
- [4] S. Craver, N. Memon, B. Yeo, and M. Yeung. Can invisible watermarks resolve rightful ownerships? In *Proc. IS&T/SPIE Electronic Imaging: Storage and Retrieval of Image and Video Databases*.
- [5] S. Craver, N. Memon, B. Yeo, and M. Yeung. On the invertibility of invisible watermarking techniques. In *Proc. Int. Conf. Image Processing*.
- [6] Leonardo Carneio de Araujo. Wavelets with scaling factor greater than two. Master's thesis, Federal University of Minas Gerais, 2007.
- [7] Ping Dong, Jovan G. Brankov, Nikolas P. Galatsanos, Yongyi Yang, and Franck Davoine. Digital watermarking robust to geometric distortions. *IEEE Transactions on Image Processing*, 2005.
- [8] C. Fernandez-Maloigne, M.-C. Larabi, B. Bringier, and N. Richard. Spatio temporal characteristics of the human color perception for digital quality assessment. In *ISSCS 2005*. International Symposium on Signals, Circuits and Systems, 2005.
- [9] J. O'Ruanaidh and T. Pun. Rotation, scale and translation invariant spread spectrum digital image watermarking. *Signal Processing*, 1998.
- [10] Soo-Chang Pei and Chao-Nan Lin. Image normalization for pattern recognition. *Image Vision Computing*, 1995.
- [11] Chih-Wei Tang and Hsueh-Ming Hang. A feature-based robust digital image watermarking scheme. *IEEE Transactions on Signal Processing*, 2003.
- [12] Wenjun Zeng and Bede Liu. A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images. *IEEE Transactions on Image Processing*, 1999.