On the Image Watermarking Techniques Applications, Properties and fields

Mohamed-Salim Bouhlel (1) , Hanène Trichili (1) , Nabil Derbel (2) and Lotfi Kamoun (1)
(1) Electronic and Information Technology Laboratory (LETI) (2)
Research Unit: Intelligent Control, design & Optimisation of complex Systems (ICOS)
National Engineering School of Sfax
P.B W, 3038 Sfax, Tunisia
E-mail:*medsalim.bouhlel@enis.rnu.tn hanene.tn@voila.fr nabil.derbel@ieee.org lotfi.kamoun@enis.rnu.tn*

Introduction

The growth of networked multimedia systems has magnified the need for image copyright protection. One approach used to address this problem is to add an invisible structure to an image that can be used to seal or mark it [1]. These structures are known as digital watermarks. In fact, as the increasing of the electronic publishing, the data distribution is becoming faster, and require less attempt to be copied. One of the major challenges is that of discouraging illegal copying. In order to trace the illicit copies, it has been suggested to mark the image with a signature or copyright message. Such message must be secretly embedded and the difference between the coded image and the original one could be indistinguishable.

Besides, a robust signature coding approach should survive several possible attacks [2-4], such as image processing, lossy image compression... In this paper, we present an overview about image watermarking in terms of applications, and properties. We will try, after that, to present the most used watermarking insertion domain and to evaluate them. This study will concern spatial, frequency and wavelet domain.

1. Watermarking Applications

Watermarking applications are numerous. We can mention for this the copyright protection, the fingerprinting, the copy limitation, and others... In this section we propose to present these applications in order to more clarify the importance of such field in our environment.

The main reason where image watermarking is very useful is the intellectual property protection. Since, Copyright protection was the first application of watermarking methods and is still the most popular. This fact is common to major copyright and author's right laws. There is national and international legislation aiming at protecting intellectual property, the US Copyright Act, the Bern Convention, the WIPO treaties, etc.

Nevertheless, additional means are needed in order to facilitate the application of these laws, such as technical protection tools.The owner can embed a digital mark in order to save his innovation in any academic, brain, or artistic field. This operation is needed nowadays after the great exploration of Internet and the easy information access. An other application of image watermarking is the Fingerprinting.Technically fingerprinting techniques are very similar to private watermarking but they differ in an application and a security level. Fingerprints are embedded for each image delivery or trading. They can be associated with a peer to peer contract, in this case they can be situated at the server side. The server knows the identity of the customer and embeds it in the image before delivery. In image watermarking, this application is useful to draw the resource of unlawful copies. Since, the owner can embed different watermarks in the copies of the data supplied to different customers. This technique can be compared to embedding a serial number related to the customer's identity in the protected data. It enables the intellectual property owner to identify customers who have broken their license agreement by supplying the data to third parties. In commercial advertisements, we need watermarking when we need to embed marks in an automated monitoring system. It's the Broadcast Monitoring. By this, one can check all broadcast channels and charge the TV stations according to their findings. Fragile watermarks can also be useful to check the image

authenticity. It's known as the Image Authentication [6]. This application help to indicates whether the protected image has been altered. An other field, that can be mentioned in this mean, is the image indexing. In fact, even if watermarking techniques try to embed digital signatures, we can use the same procedure to insert in the image informations relevant to its contain. Also, we can't forget the medical field as an elemental field when we find watermarking. Since, we use the same method to embed the patient's informations in medical images as a safety technique that promote telediagnosis.

2. Watermarking Properties

The watermarking properties are the parameters allowing to identify the signature characteristics. The first property is the perceptual transparency. In fact, the embedded signature mustn't affect the image quality. As this, the watermark can be perceptually imperceptible. On the other way, users of watermarked image usually don't have access to the unmarked one they cannot perform the difference. On the other hand, the quantity of information stored in a given signature depends on the watermark application. So that, we must dose this quantity relatively to the data type and to the given request. An other property is the watermark robustness. This characteristic is the most important one and many research has been done in this field. In fact, the robustness of the watermark is strongly depending on the objective of the operation itself. In the case of the authenticity, a fragile watermark has to prove that the host image has been modified and is no longer authentic. However, for copy protection applications the watermark must be very robust and be able to withstand different types of alterations such as lossy compression techniques, filtering, , Digital to Analogic and/or Analogic to Digital conversions, and so on. Obviously, the security is furthermore a main property of a thrive watermarking. A watermarking technique is truly secure if knowing the exact algorithm for embedding and extracting the watermark does not help the unauthorized party to detect the presence of the watermark or remove it. In some applications, like copyright protection the

watermark extraction algorithm can use the original unwatermarked image to find the mark (usually called *nonoblivious* watermarking). Nevertheless, in most other applications such as copy protection the watermarking extraction algorithms have not access to the unwatermarked data. This makes the watermark extraction more difficult (this kind are called *oblivious*, *public* or *blind* watermarking techniques).

An other property of a good watermarking technique is called the reliability of the watermark. Since, in the watermarking detection process, the watermark detector can detect the existence of a false watermark or reject the existence of the watermark.

3. Watermarking Domain

In digital watermarking a host signal is transformed to a watermark domain in which modifications are imposed on the domain coefficients to embed the watermark. The modified coefficients are then inverse transformed to produce the marked signal. These domains are that needed to embed the signature. We discern the spatial domain, the frequency domain and the multiresolution one.

3.1 Spatial Domain

One of the earliest techniques for steganographically embedding data in digital images, the spatial method involves using the two-dimensional array of pixels in the container image to hold hidden data. The most common implementation is known as the least-significant bit (LSB) method. Taking benefit of the human visual system (HVS) approach to perceive images, this technique involves replacing the N least-significant bits of each pixel of a container image with the data of a hidden one. Since we are not very attuned to small variations in color, so image processing adjusting the small differences between adjacent pixels will leave a virtually unnoticeable result. As the least-significant bits of an 8-bit grayscale image encode the most minor variations in pixel color, they can be replaced with informational bits without altering the image in a perceptible way (provided that the number of bits

replaced at each pixel is kept reasonably low). . The pixels for grayscale images are encoded with 8 bits. Image imbedding involves replacing the lower N bits of the container image with the upper N bits of the hidden image. Thus, we swap the higher-resolution bits of the container image for the lower-resolution bits of the hidden image. If all goes well, in the end we will be able to extract a reduced-resolution, but still recognizable, version of the hidden image from the composite image. The LSB technique proves to be a rather well-rounded method and lends itself to a variety of information-hiding applications. Its principle advantage is the information quantity we can embed in the image. Since each pixel serves as a data carrier, a large quantity of imbedded information can be included. This method is also an excellent technique for embedding any type of hidden data such as image, audio, or text messages. Hence, the main advantage of the spatial domain techniques of data embedding stay the relatively low calculation complexity when compared to any technique requiring domain transforms. It should also be noted that the data capacity of the spatial techniques is
quite significant. Spatial methods, however, falter from most types of image attacks. Thus, the robustness of the spatial techniques limits the overall effectiveness.

3.2 Frequency Domain

The frequency domain representation of an image serves as a stronger channel for transmitting information covertly while minimizing distortion of the container image. Spatial techniques localize the data in an image through bit manipulation. Frequency methods encode the mark across the global frequencies of the image. This enables frequency methods to achieve a better robustness towards attack. The most known techniques in this field are those using the DCT transform (Cox) and Fourier-Mellin insertion (Ruanaidh).
The use of the frequency domain as a steganographic channel proves very useful. Although the process is more computationally complex, it is considerably more robust than the spatial domain techniques developed earlier. Whereas, this domain present some drawbacks. Indeed, while the DCT

transform provide a good robustness towards JPEG compression, it has the weakness of robustness toward geometric transformations.

3.3 The Wavelet Transform Domain

Wavelets are one of the newest topics in the image processing field. Because of its good temporal and frequency localization, the information hiding techniques used in the frequency domain were translated to the wavelet one. The first step is to convert an image to that domain. The Haar wavelet basis are the most chosen due to its simplicity [7]. The basic process involves a lowpass filter (h[n]) and a highpass filter (g[n]). The image is processed in 4 ways (producing 4 separate images as output). Its rows are convolved with h or g, as are its columns. The 4 image outputs have h rows and h columns, g rows and h columns, h rows and g columns, and g rows and g columns. These images are then downsampled by 2, meaning that every other row and every other column is eliminated. Lastly, the 4 images are combined into one having the same dimensions as the original source image, with hrowhcol in the upper left, growhcol in the lower left, hrowgcol in the upper right, and growgcol in the lower right. The inverse wavelet transform must break down the four-part image and upsample by 2, inserting a row of zeros after every row and a column of zeros after every column. Next, the 4 images have their rows and columns convolved with the same filters (h or g) as before. And lastly, the 4 component images are summed to regain the original image. The watermarking in wavelet domain is as follow: Given its fitness to model the HVS behavior, the DWT has gained interest among watermarking researchers, as it is witnessed by the number of algorithms following this approach that have been proposed over the last few years. In this section some of these algorithms are briefly reviewed, by particularly highlighting the approaches they embraced for considering HVS factors. In some methods [7,8], the most significant DWT coefficients are selected and modified to carry the atermark. In this case, the modified coefficients location is required to recover the watermark. To take into account visual effects, very large coefficients are left unchanged [7], or the watermarking signal is weighted according to a band-

dependent value[8]. Other algorithms hide into images binary logos which are also hierarchically decomposed. Kundur et al.[9], for example, first decompose a binary logo through DWT, then repeatedly add it to the subbands of the DWT decomposition of the host image; before being added, the watermark is scaled by a salience factor, computed on a block by block basis, related to the local image noise sensibility: visual masking is thus exploited up to a block resolution.

Conclusion

Watermarking is an enabling technology for securely hiding information in images. When associated with other technologies, it reveals very helpful to copyright protection and management. An overview of emerging protection tools and systems is done in this work. Besides copyright protection, watermarking can serve to other applications. A survey of them and their respective requirements is also done. We describe a number of image watermarking applications and scan the common properties of this field. We observe that these properties vary greatly depending on the application. Consequently, we conclude that evaluation of a watermarking algorithm is difficult without first indicating the context in which it is to be applied. Finally, a peer evaluation of different embedding domains is also presented.

Bibiographie

[1] J.Brassil and L.O'Gorman "Watermarking Document Images with Bounding Box Expansion", Information Hiding 1st International Workshop, June 1996.

[2] Y.Liu, Jonathon, E.Wong, S.Low., "Marking and Detection of Text Documents Using Transform-domain Techniques", Security and watermarking of Multimedia Contents, january 1999

[3] L. Sang-Kwang and Y.Sung., "Digital Audio Watermarking in the Cepstrum Domain", IEEE Transactions on Consumer Electronics, Vol. 46, No. 3, August 2000.

[4] Fabien A.P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn., "Attacks on Copyright Marking Systems", Information Hiding 2 nd International Workshop, April 1998.

[5] S.Sowers and A.Youssef., 'Testing Digital Watermark Resistance to Destruction", Information Hiding 2nd International Workshop, April 1998.

[6] M. G. Linnartz and M. van Dijk., "Analysis of the sensitivity Attack against Electronic Watermarks in Images", Information Hiding 2 nd International Workshop, April 1998.

[7] H. Inoue, A. Miyazaki, A. Yamamoto, and T. Katsura, "A digital watermark based on the wavelet transform and its robustness on image comression and transformation," IEICE Trans. Fund. Electron., Commun., Comput. Sci., vol. E82-A, pp. 2–10, Jan. 1999.

[8] H.J. M.Wang, P.-C. Su, and C.-C. J. Kuo., "Wavelet-based digital image watermarking," Opt. Express, vol. 3, no. 12, pp. 491–496, Dec. 7, 1998.

[9] D. Kundur and D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion," in Proc. 4th IEEE Int. Conf. Image Processing '97, Santa Barbara, CA, Oct. 26–29, 1997, pp. 544–547.