Copyright Protection of Digital Images by Means of Frequency Domain Watermarking

A. Piva[a], M. Barni[a] and F. Bartolini[a]

[a]Dipartimento di Ingegneria Elettronica, Università di Firenze
via di S. Marta, 3, 50139 Firenze, Italy

ABSTRACT

Notwithstanding the high availability of image contents, multimedia products propose very low quality pictures, primarily due to the fact that effective systems for the copyright protection of multimedia works are unavailable. A digital image can, in fact, be easily reproduced obtaining as many identical copies of it as we want, without any possibility to prevent it. To get around the problem, further than scrambling the data to be protected by means of cryptograpic techniques, a code carrying information about IPR (Intellectual Property Rights) could be invisibly embedded into them, in such a way to provide a mean to control their distribution. This is the aim of image watermarking techniques. In this paper general issues related to copyright protection of digital data as well as some items referring to the embedding of a watermark in the frequency domain, are discussed. Results are also presented showing the robustness of the proposed algorithms.

Keywords: Digital watermarking, Copyright protection, Security, Image authentication

1. INTRODUCTION

All around the world, a huge and rich pictorial patrimony is available, nevertheless multimedia products often supply very low quality pictures. The primary contributing factor to the limited development of the commerce of electronic images is the unavailability of effective means to protect the rights of the owners. Once a digital image has been sold, the purchaser can, in fact, reproduce as many identical copies as he wants. Encryption systems do not solve the problem of unauthorized copying, because, once encryption is removed from a document, there is no more control on document dissemination. To cope with this problem, further than encrypting the data to be transmitted, a code carrying information related to the IPR of the data, could be invisibly embedded into them, in such a way not to limit the number of copies allowed, but to provide a mean to control their distribution. This is the aim of image watermarking techniques. The embedded code should be easily and reliably identifiable, its insertion should not visibly deteriorate the image, and its identification should also be possible after the image has been processed. In this paper general issues related to copyright protection of digital data as well as some items referring to the embedding of a watermark in the frequency domain, are presented. The class of watermarking techniques described here embeds a sequence of M randomly generated real numbers $X = \{x_1, x_2, .., x_M\}$ (where each value x_i is a sample of a random sequence with normal distribution) in some coefficients of the image full-frame DFT. Results are also presented showing the robustness of the proposed class of algorithms against geometric attacks.

2. REQUIREMENTS FOR WATERMARKING SCHEMES

Though, the requirements watermarking techniques have to fulfill are application-dependent, some of them are common to most practical applications. In the sequel such general requirements will be listed and briefly discussed.

2.1. Security can not be based on algorithm ignorance

As for cryptography, it is well known that the effectiveness of an algorithm can not be based on the assumption that possible attackers do not know how the codemark has been embedded into the multimedia document.[1] Nevertheless, the robustness of virtually all the commercial products available on the market is based on such an assumption. Though some of them are claimed to be exceptionally resistant, by knowing how the watermark encoder and decoder work, it is usually very easy to make the watermark unreadable.[2] Furthermore, some of the most promising techniques use the original non-marked data in the decoding process, and, as it will be discussed below, very often the resort to the comparison between the marked and non marked documents is not allowed.

Other author information: (Send correspondence to A. Piva)
A. Piva: E-mail: piva@cosimo.die.unifi.it

2.2. Invisibility

Even if in some applications a visible watermark can be required, in the following we will only focus on invisible watermarking (the term invisible refers to image watermarking, in general the term imperceptible should be used). So far researchers have tried to hide the watermark in such a way that it is impossible to be noticed. However this requirement conflicts with other requirements such as tamper resistance and robustness, especially against lossy compression algorithms. Compression algorithms currently used still permit such a goal to be reachable, however, this may be no more possible in the future, thus to survive the next generation of compression algorithms, it will probably be necessary for a watermark to be noticeable to a trained observer which is asked to compare the original and the marked version of the document. Of course this may not be a problem in practical situations, where, for example, an user does not have the possibility of comparing the marked and non-marked versions of a work.

2.3. Number of bits which can be hidden

Depending on the application at hand, the watermarking algorithm should allow a predefined number of bits to be hidden. General rules do no exist here, however, in the image case, the possibility of embedding into the image at least 300-400 bits should be granted. In any case, system designers should keep well in mind that the number of bits which can be hidden into data is not unlimited, nay very often is fairly small.

2.4. Low error probability

Even in the absence of attacks or signal distortions, the probability of failing to detect the watermark (false-negative error probability) and of detecting a watermark when, in fact, one does not exist (false- positive error probability), must be very small. Usually, statistically-based algorithms have no problem in satisfying this requirement, however such an ability must be demonstrated if watermarking is to be legally credible.

2.5. Robustness

The use of music, images and video signals in digital form, commonly involves many types of distortions, such as lossy compression, or, in the image case, filtering, resizing, contrast enhancement, cropping, rotation and so on. For watermarking to be useful, the mark should be detectable even after such distortions occurred. It is a common opinion[3–5] that robustness against signal distortion is better achieved if the watermark is placed in perceptually significant parts of the signal. This depends on the behaviour of lossy compression algorithms, which operate by discarding perceptually insignificant data not to affect the quality of the compressed image, audio or video. Consequently, a watermark hidden among perceptually insignificant data is likely not to survive compression. In the image watermarking case, resistance to geometric manipulations, such as translation, resizing, rotation and cropping is still an open issue, yet such operations are very common and a solution needs to be found before watermarking is successfully applied to image copyright protection.[6] Some objective criteria to measure the robustness of image watermarking techniques will be discussed in the next section.

2.6. Blind/non-blind, public/private watermarking

Particular attention must be paid to the mechanism used to recover the mark from the image. In some cases, in order to develop a very robust algorithm, the watermark is extracted by comparing the marked version of the document to the non-marked one. Examples of such an approach in the image case are given in,[4,7–11] where several methods are proposed which are resistant to a large variety of image processing techniques and possible attacks aiming at removing the watermark or making it unreadable. However, very often, in real-world scenarios the availability of the original image (audio file, video) can not be warranted, thus making the algorithms which need it to recover the mark unsuitable for many practical applications. Besides, this kind of algorithms can not be used to prove rightful ownership, unless additional requirements are satisfied such as the non-quasi-invertibility of the watermark, which is quite difficult to achieve and almost impossible to prove.[12–14] Techniques which recover the watermark without resorting to the comparison between the marked and non-marked signals are sometimes called oblivious or blind.[15] In other cases the term public watermarking is used as opposed to private watermarking.[3,13] Indeed, we prefer to use the term public/private watermarking to indicate a different concept: a technique is said to be private if only the document owner, or authorized personnel, can extract the watermark, either because he is the only one able of accessing the original image, or he is the only one knowing the correct key to extract if from the host data. In contrast, techniques that allow anyone to read the watermark are said public. It is widely believed that private mechanisms are likely to be significantly more robust than public ones, in that once the codemark has been read, it is much easier for an attacker to remove it or to make it unreadable, for example by inverting the encoding process or by encoding an inverse watermark (watermark reversibility). Generally speaking, it can be noticed that among image watermarking algorithms proposed so far, commercial products usually adopt public schemes, whereas research is more focused on the private approach.

Recently, several blind image watermarking algorithms have been proposed,[15–20,6,21,22] but none of them is able of surviving to all the most common image manipulations, thereof the need for further research in this field.

2.7. Readable vs. detectable watermarking

A watermark that can be detected only if its content is known in advance is referred to as a detectable watermark. Conversely, techniques which permit the watermark to be read even if its content is ignored, will be referred to as readable. In other words, according to the detectable approach, one can only decides whether a given mark is present in the data or not. On the contrary, it is not possible to analyse the multimedia document looking for a watermark, if one does not have any idea of what the watermark is. This is not the case with readable techniques, whose embedding and retrieval mechanisms are such that the watermark can be read by anyone. Of course the readable/detectable nature of the watermark heavily affects the way it can be used in practical applications. As an example, let us consider a situation in which one wants to know which is the owner of an image he found somewhere in Internet. Also, suppose that the owner identification code has been embedded in the image by means of a detectable watermarking scheme. There is no mean to read the code if some hypothesis about the possible owner can not be done, since due to the detectable nature of the watermark, it is only possible to verify if the image belongs to a particular author whose identification code is known.

2.8. Watermark invertibility and reversibility

Though robustness is commonly indicated as the major requirement to be satisfied, great attention should be given to watermark invertibility as well. In the literature the term *invertibility* has been used with different meanings, the most natural one defining a watermark to be invertible if authorized users can remove it from the document. In many applications, this kind of invertibility would be a desirable feature, since it would permit to change the status of a given document according to its history, without the need to hide too many bits of information inside it. A different meaning has been given to watermark invertibility by Craver et al..[12,13] In their interesting work the authors analyse the possibility of invalidating ownership claims supported by watermarking by reverse engineering the watermarking process. The conclusions arrived at by Craver et al.[12,13] are that for a watermarking scheme to be successfully used to demonstrate rights ownership, non-invertibility of the watermark has to be granted. Furthermore, this is only a necessary condition to be satisfied, since, more generally, non-quasi-invertibility is needed. Here the terms invertibility and quasi invertibility assume a different sense with respect to the natural meaning discussed above. Without going into much details, which is outside the scope of this brief work, we can say that a watermark is invertible if it is possible to generate a false watermark and a fake original document which is perceptually equal to the true one, such that by embedding the false watermark in it a document which is equal (invertibility) or perceptually equal (quasi invertibility) to the true marked one is obtained. In[12,13] it is demonstrated that invertible or quasi invertible watermarking schemes are likely to be of little use in many practical applications. The analysis by Craver et al. applies mainly to non-blind techniques, even if an example is given extending the discussion to the blind case. However, some doubts exist on whether non invertibility and non-quasi-invertibility are needed in the case of private-blind techniques.[14] In order to avoid the ambiguous use of the term invertibility, we propose to use the term *reversibility* to indicate that a watermark can be removed from the host image once its content is known. As to watermark invertibility the meaning suggested by Craver et al.[12,13] should be retained.

3. ROBUSTNESS CRITERIA

Watermarking tools must grant that the embedded information is not removed neither by accidental image modifications nor by collusion and forgery attacks. Many tools are widely available for processing digital images, aimed at enhancing or at modifying them. The available processing techniques can be distinguished in two classes: signal processing modifications and geometric transformations. Among signal processing modifications the most common are:

brightness and contrast enhancement : usually do not prevent watermark detection, on the contrary, they are often applied before detection is performed to obtain better results[4];

sharpening, blurring, linear and non linear filtering : if heavily applied, these operations can deteriorate the watermark but, in this case, they also severely degrade the image; one of the most powerful filters available is the so called despeckle filter, it processes the image in an adaptive way, reducing random fluctuations and preserving details, usually, it does not deteriorate perceptively the image but highly reduces the readability of the watermark;

lossy JPEG compression : it can be considered the most common signal processing operation performed on images: JPEG is accurately tuned to eliminate the perceptively irrelevant part of the images, and thus is a good test for assessing watermark robustness; furthermore JPEG is the most used compression algorithm for archiving images, thus it is compulsory that a watermarking algorithm is resistant against it.

Geometric manipulations aim at changing the aspect of the image, without loosing quality, they are:

resizing : image dimensions are changed with respect to the original, it causes the algorithms that embed the watermark at fixed locations in the image to fail;

cropping : a sub-part of the image is cut, it causes the algorithms that do not spread or replicate the watermark all over the image to fail;

translation : it is meaningful if considered with cropping, in fact, if a sub-image is extracted from the original, it can not be known (if the original is unknown) at which location cropping has occurred, thus the sub-image may appear as being translated. Translation causes the algorithms that embed the watermark at fixed locations in the image to fail;

rotation : the most important cases to be considered are 90 and 180 degrees rotations: similar problems as for resizing occur;

Resistance to geometric manipulations is very important because they usually do not degrade the quality of the image severely. Furthermore they can be applied just for the purpose of making the watermark unreadable: if an image is cropped by 1 column or 1 row, or rotated 0.5 degrees, or scaled to 101%, the difference to the original is irrelevant, but the watermark detector/reader may be no longer able to detect/read it. Furthermore, robustness against geometric manipulations is very important while the capability to detect the watermark in printed images is required: it is in fact unlikely, if the original is unknown, that the scanned copy results perfectly aligned to the original image.

It is widely agreed that watermarking algorithms should allow for multiple codes to be embedded at different time instants,[3] previous watermarks should not be deteriorated by successive ones. This last characteristic is strictly related to robustness to forgery attacks. In particular an algorithm must be robust against tampering (i.e. try to change the watermark) and collusion attacks (i.e. many persons join their efforts in destroying the watermark). Tampering may be aimed either at erasing the watermark (by performing signal processing or geometric manipulations) or at modifying it to the attackers advantage, it is more easily accomplished if the embedded code is publicly readable. Collusion attacks are mainly aimed at erasing the watermark and can be performed very easily, for example, by averaging multiple differently watermarked copies of the same image. No solution appears to be feasible for this last attack: the watermark can, in fact, be considered as something that is added to the image, i.e. a noise signal, by averaging multiple images affected by different watermarking signals, the energy of each watermark is reduced, while the image is almost unchanged. In general, it seems that it would be better to discourage the diffusion of images not having a clearly detectable/readable watermark, thus it is important that the purchaser be allowed to detect/read the watermark. As a consequence, it should also be granted to the purchaser that he can not accidentally remove the watermark by processing in some way the image.

In general, robustness of a watermarking technique should be granted until image visual quality is severely deteriorated. It is, thus, important that the watermark be embedded in perceptively important regions of the image, in such a way that such regions should be highly deteriorated by any attempt to erase the watermark.[4] Watermark robustness can be evaluated based on its ability to resist to the most important modifications; in particular JPEG compression, despeckle and median filtering, geometric manipulations. Most important, the algorithm should resist also to concurrent modifications, e.g. JPEG, printing, scanning, filtering.

4. INVISIBILITY

As mentioned before, it has been demonstrated in[3,4] that robustness against signal distortion is enhanced if the watermark is placed in perceptually significant parts of the signal. However, this constraint contrasts with the requirement that the embedded watermark should be invisible, i.e., unperceivable to the Human Visual System (HVS); thus, watermarking techniques have to be developed taking into account the masking properties of the HVS. In particular, three characteristics of the Human Visual System can be exploited: frequency sensitivity, that is the different sensitivity of the human eye to sine wave gratings at different frequencies; luminance sensitivity, that is the different sensitivity of the eye to a noise signal on a constant background, depending on the average value of the background luminance and on the level of the noise luminance; and contrast masking, which refers to the perception of a signal in presence of a masking stimulus, and which depends on the relative spatial frequency, location, and orientation. These phenomena have been deeply studied in the field of source coding and compression, and appear to be easily applied to watermark hiding also.

5. CLASSIFICATION OF IMAGE WATERMARKING ALGORITHMS

Though image watermarking is a recent field of research, many techniques have already been proposed both by academic as well as by commercial institutions. In this section, we try to offer some criteria to classify the various techniques proposed so far. In particular, given that image watermarking is the process of modifying image data in order to insert a code carrying a given amount of information bits, a possibility for classifying watermarking techniques relyes of the type of image features that are modified. In particular, two main classes of methods can be identified according to the way the code is embedded into the image: the image data can be directly modified (spatial domain techniques), or they can be transformed into another domain, modified, and then backward transformed to obtain the marked image (transformed domain techniques). A third class can also be defined, including techniques exhibiting a hybrid behaviour. The main characteristics of the algorithms adopting these approaches will be now presented.

5.1. Spatial Domain Techniques

For this class of techniques, the values of the image pixels are directly modified based on the code that has to be embedded. Usually, modification consists in adding a modulated signal to the image brightness or to one of the colour bands or to a combination of them. One way to modify pixels values is to add them small pseudo random numbers, sampled from 1D[9] or 2D[11] random sequences. It has also been proposed[17] to use the pseudo-random numbers to scale pixels values. The pseudo random sequences depend on a generating key, which has to be known for detecting the watermark (private watermarking): this key ensures that only authorised persons can detect the watermark. Techniques originally developed for spread-spectrum communications, have also been employed.[21] Usually, watermark detection is performed through a correlation operation. Another approach is to modify the values of randomly selected pixels. For example, the image can be randomly partitioned into two complementary randomly generated sets, then different values are added to each set. Watermark detection is accomplished by estimating the difference between the mean values computed over pixels of each set.[19,20] The watermarking signal is the configuration chosen for the partition sets. Bits of information can be inserted by summing or subtracting a given value to randomly chosen locations in the image: to grant robustness, the same bit is inserted many times (repetition code).[23] Modifications can also be performed on a block by block basis. A given number of blocks, usually square shaped, can be selected based on a pseudo-random rule, a fixed value is then added or subtracted to some of the pixels in the block, in order to carry a bit of information.[18] Classification of each block (hard contrast, progressive contrast and noise contrast) can also be performed, in such a way to adapt the rule for embedding the bit to the local properties of the image.[23] In general, spatial domain techniques are more effective in exploiting the characteristics of the Human Visual System; in fact, they can easily adapt the embedding rule to the local image content. To be resistant to cropping, spatial domain techniques have to recursively embed the same information in different regions of the image. Furthermore, such techniques are intrinsically sensitive to image translation: a technique for synchronising the embedded code has, thus, to be provided. Spatial domain techniques also appear to be quite weak against image resizing.

5.2. Transformed Domain Techniques

Techniques belonging to this class apply some mathematical transform to the image before embedding the watermark. Image data are represented in a domain which is different from the image space, almost always the frequency domain. Such representation is obtained without loss of information (invertible transforms are used). The transformed domain coefficients are, then, modified by the watermark. The inverse transform is finally applied to produce the watermarked image. The two most commonly used transforms are the Discrete Fourier Transform (DFT) and the Discrete Cosine Transform (DCT). By transformed domain techniques we mean only those watermarking algorithms performing a full-frame transform of the image; techniques transforming the image on a block by block basis are considered to belong to the hybrid category. Only a few techniques can be considered to belong to this category. Usually a spread spectrum signal is added to a subset of the DCT[15,4,21] or DFT[6] transformed data. An advantage of using full-frame transforms is that the watermark is spread over the whole image, thus, these techniques are intrinsically more robust to cropping. Furthermore, by embedding the watermark in the magnitude of the DFT, these techniques also result to be resistant to translation. In[6] a particular procedure for mapping the DFT domain is presented, which adds immunity to rotation and scaling. The main drawbacks of frequency domain techniques are their computational cost, and the difficulty they present in adapting the watermarked signal to the local image content, thus making the exploitation of the characteristic of the Human Visual System more difficult.

5.3. Hybrid Techniques

By hybrid techniques methods that, though using a mathematical transformation before embedding the watermark, do not lack spatial adaptivity are meant. Two approaches can be distinguished, those based on JPEG-like block-DCT and those based on wavelets. Given that JPEG is the most common method to compress and archive images, watermarking techniques must be robust against it. Many watermarking tools are, thus, tailored to ensure such characteristic. The image is usually partitioned into blocks (often of the same dimension of JPEG blocks), that are, then, DCT transformed. Some of the DCT coefficients in the block are modified to carry the watermark.[16,22] Results of previous research on perceptual efficient JPEG coding can also be exploited to reduce watermark visibility and enhance robustness.[10,24] In[8] it is proposed to embed the watermark in the phase of the DFT coefficients of the blocks. Another transform that is commonly used for compression purposes is the wavelet transform, since wavelets are very suitable to model perception of the Human Visual System.[25]

Hybrid techniques are very efficient in adapting the watermark embedding level to the local image content, on the other side, due to this characteristic, they are rather sensitive to image translation (some mechanism should be provided to recover synchronisation) and scaling.

6. A CLASS OF FREQUENCY DOMAIN WATERMARKING ALGORITHMS

A technique which does not resort to the comparison between the marked and non-marked images and operating in the transformed domain is here briefly described. The mark consists of a set $X = \{x_1, x_2, \ldots, x_n\}$ of n normally distributed samples which are used to modify the magnitude of a selected set $V = \{v_1, v_2, \ldots, v_n\}$ of full-frame DFT coefficients. The mark is always inserted in the same set of coefficients: in particular, to respect the symmetry of the DFT spectrum, the coefficients of the four quadrants are reordered according to a zig-zag scan as shown in Figure 1. For each reordering, the coefficients from the $(k+1)$-th to the $(k+n)$-th are taken; the samples of the watermark from x_1 through $x_{n/2}$ are used to modify simultaneously the magnitude of the coefficients belonging to the I and III quadrant, whereas the samples from $x_{n/2+1}$ through x_n are used to modify the magnitude of the coefficients in the II and IV quadrant.

With regard to watermark embedding, the following, very simple, rule is used:

$$v_i' = v_i + \alpha v_i x_i \tag{1}$$

where v_i' is the magnitude of the modified DFT coefficient, and α is the watermark energy. After watermark embedding, the modified magnitudes of DCT coefficients are reinserted in their position, and an inverse DFT is applied, obtaining a temporary watermarked image. To enhance watermark robustness, without compromising its invisibility, the characteristics of the Human Visual System are exploited by mixing the original image and the temporary watermarked one based on a spatial masking image.[26] In watermark detection, the correlation between the marked and possibly corrupted DFT coefficients and the mark itself is taken as a measure of the presence of a

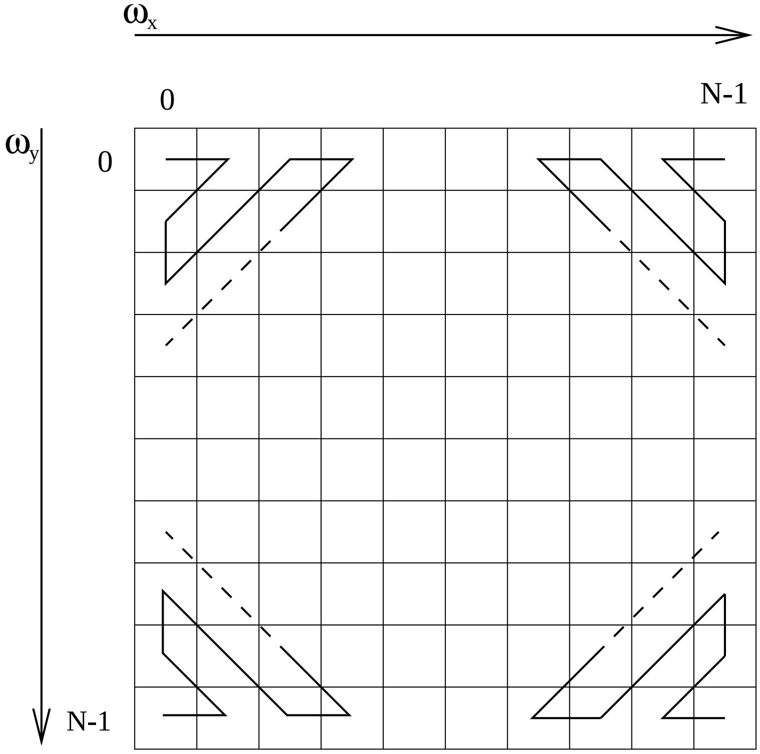

Figure 1. Selection of the DFT coefficients where the watermark is embedded in.

given mark. According to the application at hand, the correlation can be used to determine whether a given mark is present or not (detectable watermark), or to distinguish between a set of known marks (readable watermark). In the first case the correlation is simply compared to a predefined threshold, whereas in the second case the mark with the largest correlation from the set of known watermarks is assumed to be the one really present in the image.

In the following, some results are presented to demonstrate the robustness and the invisibility of the watermark. On the left of Figure 2 a grey level image representing a particular of the worldwide known painting 'La Nascita di Venere' ('The birth of Venus') by Botticelli, conserved at the Uffizi Gallery in Florence, is depicted. On the right side of the Figure the same image, after watermarking, is shown. As it can be seen, the two images are not distinguishable, thus proving that the requirement of watermark invisibility is satisfied. The watermarked image was then attacked in many ways to test the algorithm robustness. Here only results concerning robustness against geometric distorsions are considered, the interested reader may refer to the work by Barni et al.[15] for a more detailed analysis of the robustness of frequency-domain watermarking to other kinds of attacks.

6.1. Robustness to Translation

The choice to embed the watermark in the magnitude of the DFT coefficients is strictly dependent on the well-known property of the Discrete Fourier Transform: given the 2D discrete function $f(n,m)$, where $0 \le n \le N-1$, $0 \le m \le M-1$, its DFT is defined as:

$$F(k,l) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} f(m,n) e^{-\frac{j2\pi km}{M}} e^{-\frac{j2\pi ln}{N}} \qquad 0 \le k \le M-1, 0 \le l \le N-1 \ . \tag{2}$$

If a translation (n_0, m_0) is performed, then the DFT of $f(n-n_0, m-m_0)$ is:

$$F(k,l) e^{-\frac{j2\pi km_0}{M}} e^{-\frac{j2\pi ln_0}{N}} = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} f(m-m_0, n-n_0) e^{-\frac{j2\pi km}{M}} e^{-\frac{j2\pi ln}{N}} \qquad 0 \le k \le M-1, 0 \le l \le N-1, \tag{3}$$

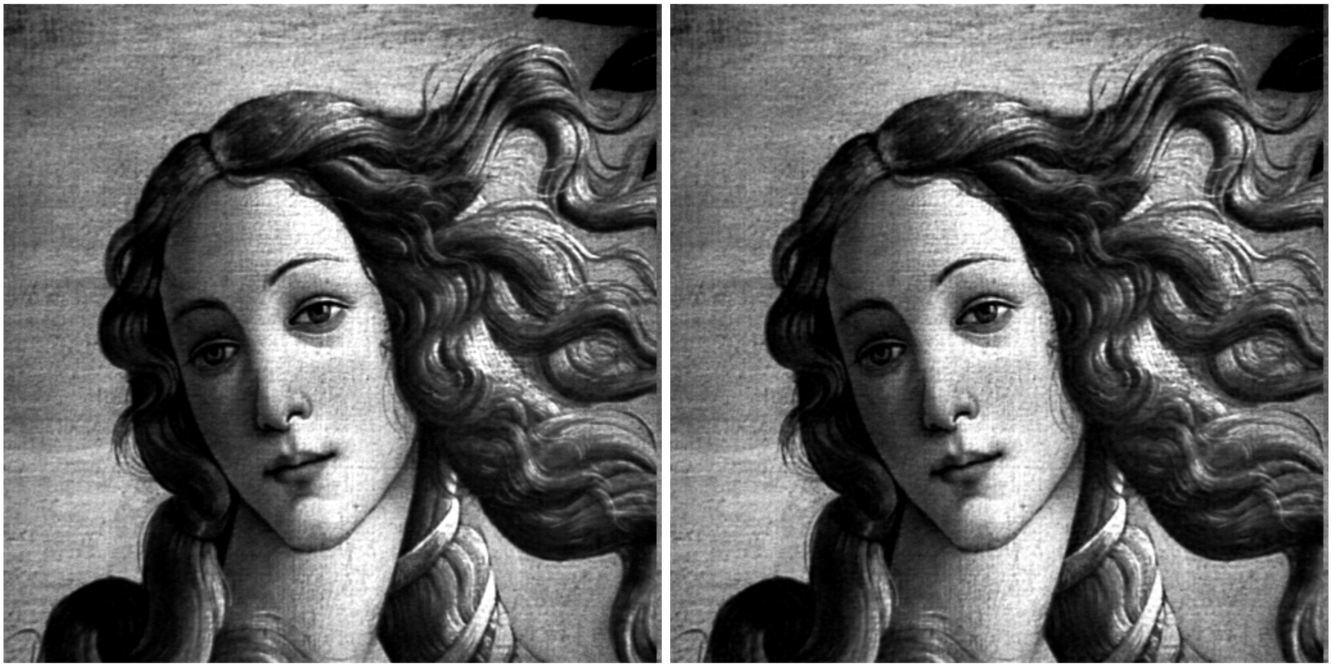

Figure 2. The original, non-marked, image "Venus" (left), and the the corresponding marked image (right)

that is to say, a spatial translation corresponds to a shift of the phase of the DFT, whereas the magnitude is unaltered. In other words, by marking the DFT magnitude spectrum of the image, robustness against image translations is automatically achieved.

6.2. Robustness to Cropping

Let us demonstrate the effects of cropping on a 1D signal.

If cropping is performed on the 1D signal, its temporal duration is reduced from N to M samples, where $M < N$, so that in the frequency domain the sampling step changs from $\Delta f = \frac{1}{N}$ to $\Delta f' = \frac{1}{M} > \Delta f$ (normalized frequency are considered). In such a case, in detection it is not possible to recover the modified DFT coefficients, since, because of the lack of the original image, we do not know the original sampling step. To cope with this problem, in watermark embedding and detection, the image is extended always to the same size of 1024 × 1024 by means of zero padding (see Figure 3); in this way, the sampling step in the DFT domain has always the same value $\Delta = \frac{1}{1024T_C}$, and the resampling effect is avoided (see Figure 4).

6.3. Robustness to Resizing

The algorithm described above turns out to be intrinsically robust against resizing. As a matter of fact, the response of the detector does not depend, or depends only slightly on the image size. The effect in the transformed domain of image resizing is exemplified in Figure 5, where for sake of clarity the case of a 1-dimensional signal is considered. In Figure 5 (a), the spectrum of the marked image is sketched with the marked coefficients highlighted. When the signal is magnified by means of an ideal interpolation process, the spectrum reported in Figure 5 (b) is obtained. As it can be seen the repetition period of spectrum replicas is enlarged, but, since the number of samples is increased by the same factor, the marked coefficients do not change. Conversely, when the signal is shrunk, replicas get closer thus causing some aliasing to occur. However, once again, if the shrinking factor is not too large, the portion of the spectrum the watermark is embedded in, does not change. Analogous considerations apply to the 2D case, even when a different scaling factor is applied in the horizontal and vertical directions, thus ensuring watermark robustness against both isotropic and anisotropic resizing.

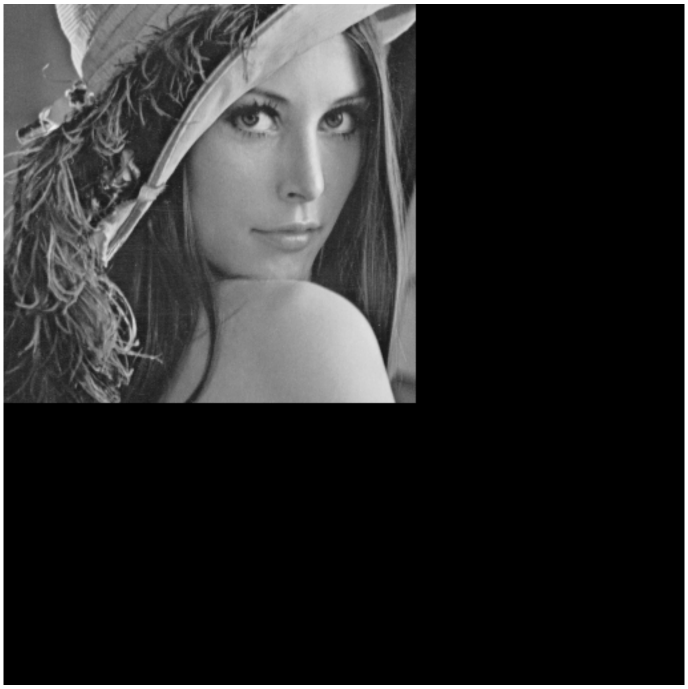

Figure 3. The image "Lenna" extended by means of zero padding to a fixed size of 1024 × 1024.

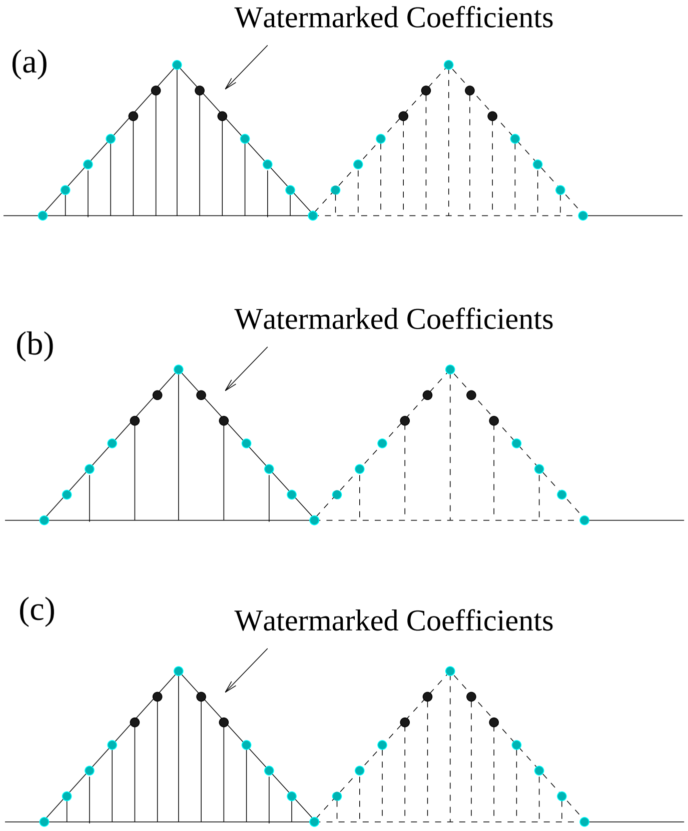

Figure 4. Example of the effects of cropping on DFT coefficients. In (a) the DFT magnitude spectrum of the unattacked watermarked signal is shown; in (b) the spectrum of the signal after cropping, and in (c) the spectrum of the signal after zero padding.

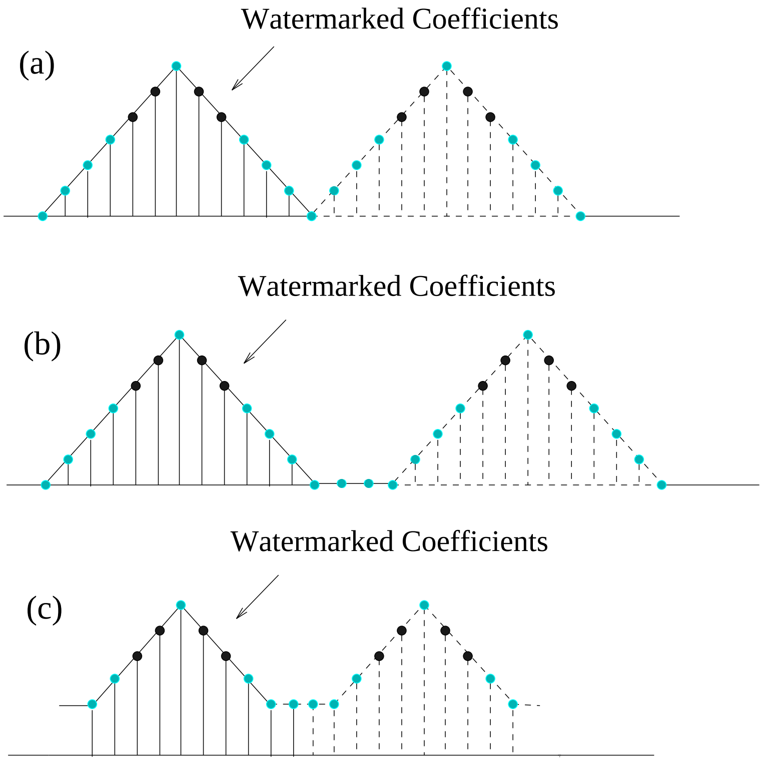

Figure 5. Example of the effects of resizing on DFT coefficients. The DFT spectrum of the unattacked watermarked signal (a) is shown, as well as that of a magnified (b) and a shrunk (b) copies.

ACKNOWLEDGMENTS

The present work was developed with support of "Progetto Finalizzato Beni Culturali - C.N.R." (Italian Finalized Project on Cultural Heritage - National Research Council).

REFERENCES

1. A. Kerkhoffs, "La cryptographie militaire," *Journal des Sciences Militaires* **9th series**, 1883.
2. F. Petitcolas, R. Anderson, and M. Kuhn, "Attacks on copyright marking systems," in *II Int. Workshop on Information Hiding*, (Portland Oregon, USA), April 14-17 1998.
3. I. J. Cox and M. L. Miller, "A review of watermarking and the importance of perceptual modeling," in *Proc. SPIE Conf. on Human Vision and Electronic Imaging II*, vol. 3016, pp. 92–99, February 1997.
4. I. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing* **6**, pp. 1673–1687, December 1997.
5. J. J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland, "Watermarking digital images for copyright protection," *IEE Proceedings Vission, Image and Signal Processing* **143**, pp. 250–256, August 1996.
6. J. O. Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking," in *Proc. IEEE Internat. Conf. Image Processing '97*, vol. 1, pp. 536–539, (Santa Barbara, CA), October 26-29 1997.
7. C. Hsu and J. Wu, "Hidden signatures in images," in *Proc. IEEE Internat. Conf. Image Processing '96*, pp. 223–226, (Lausanne, Switzerland), September 16-19 1996.
8. J. O. Ruanaidh, F. Boland, and W. Dowling, "Phase watermarking of digital images," in *Proc. IEEE Internat. Conf. Image Processing '96*, pp. 239–242, (Lausanne, Switzerland), September 16-19 1996.
9. R. V. Schyndel, A. Tirkel, and C. Osborne, "A digital watermark," in *Proc. IEEE Internat. Conf. Image Processing '94*, pp. 86–90, (Austin, Texas), November 13-16 1994.
10. M. Swanson, B. Zhu, and A. Tewfik, "Transparent robust image watermarking," in *Proc. IEEE Internat. Conf. Image Processing '96*, pp. 211–214, (Lausanne, Switzerland), September 16-19 1996.

11. P. Wolfgang and E. Delp, “A watermark for digital images,” in *Proc. IEEE Internat. Conf. Image Processing ’96*, pp. 219–222, (Lausanne, Switzerland), September 16-19 1996.

12. S. Craver, N. Memon, B. Yeo, and M. Yeung, “On the invertibility of invisible watermarking techniques,” in *Proc. IEEE Internat. Conf. Image Processing ’97*, pp. 540–543, (Santa Barbara, CA), October 26-29 1997.

13. S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, “Resolving rightful ownership with invisible watermarking techniques: limitations, attacks and implications,” *IEEE Journal on Selected Areas in Communications* , 1998. To appear.

14. W. Zeng and B. Liu, “On resolving rightful ownerships of digital images by invisible watermarks,” in *Proc. IEEE Internat. Conf. Image Processing ’97*, vol. I, pp. 552–555, (Santa Barbara, CA), October 26-29 1997.

15. M. Barni, F. Bartolini, V. Cappellini, and A. Piva, “A DCT-domain system for robust image watermarking,” *Signal Processing* **66**, May 1998.

16. A. Bors and I. Pitas, “Image watermarking using DCT domain constraints,” in *Proc. IEEE Internat. Conf. Image Processing ’96*, pp. 231–234, (Lausanne, Switzerland), September 16-19 1996.

17. G. Braudaway, “Protecting publicly-available images with an invisible image watermark,” in *Proc. IEEE Internat. Conf. Image Processing ’97*, vol. 1, pp. 524–527, (Santa Barbara, CA), October 26-29 1997.

18. G. C. Langelaar, J. C. A. Van der Lubbe, and J. Biemond, “Copyright protection for multimedia data based on labeling techniques,” in *17th Symp. Information Theory in the Benelux*, (Enschede, The Netherlands), May 1996.

19. N. Nikolaidis and I. Pitas, “Copyright protection of images using robust digital signatures,” in *Proc. IEEE Internat. Conf. Acoustics, Speech & Signal Processings ’96*, pp. 2168–2171, (Atlanta, GA), May 7-10 1996.

20. I. Pitas, “A method for signature casting on digital images,” in *Proc. IEEE Internat. Conf. Image Processing ’96*, pp. 215–218, (Lausanne, Switzerland), September 16-19 1996.

21. J. Smith and B. Comiskey, “Modulation and information hiding in images,” in *Proc. First Int. Workshop on Information Hiding R. Anderson ed., Lecture Notes in Computer Science, Springer-Verlag ????*, pp. 207–226, 1996.

22. J. Zhao and E. Koch, “Embedding robust labels into images for copyright protection,” in *Proc. Internat. Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies*, pp. 242–251, (Vienna, Austria), August 21-25 1995.

23. A. Control and C. P. for Images (ACCOPI), “Workpackage 8: Watermarking,” tech. rep., RACE Project M 1005, June 1995.

24. C. Podilchuk and W. Zeng, “Perceptual watermarking of still images,” in *Proc. The First IEEE Signal Processing Society Workshop on Multimedia Signal Processing*, (Princeton, New Jersey), June 1997.

25. D. Kundur and D. Hatzinakos, “A robust digital image watermarking method using wavelet-based fusion,” in *Proc. IEEE Internat. Conf. Image Processing ’97*, vol. 1, pp. 544–547, (Santa Barbara, CA), October 26-29 1997.

26. A. Piva, M. Barni, F. Bartolini, and V. Cappellini, “Dct-based watermark recovering without resorting to the uncorrupted original image,” in *Proc. IEEE Internat. Conf. Image Processing ’97*, pp. 520–523, (Santa Barbara, CA), October 26-29 1997.