Digital Image Watermarking: an Overview

N. Nikolaidis, I. Pitas
Artificial Intelligence and Information Analysis Laboratory
Department of Informatics, Aristotle University of Thessaloniki
email pitas@zeus.csd.auth.gr

Abstract

Usage of digital media has witnessed a tremendous growth during the last decades, as a result of their notable benefits in efficient storage, ease of manipulation and transmission. However these features make digital media vulnerable to copyright infringement, tampering and unauthorized distribution. In the last five years the protection of digital information has received significant attention within the digital media community, and a number of techniques that try to address the problem by hiding appropriate information (e.g. copyright or authentication data) within digital media have been proposed. In this paper we will review data hiding techniques for copyright protection of still images and describe some recent research results on this field.

1. Introduction

One of the biggest technological events of the last two decades was the invasion of digital media in an entire range of everyday life aspects. As digital audio/video/images and multimedia documents reach an ever expanding consumer base, their domination in entertainment, arts, education etc. is just a matter of time. Digital data can be stored efficiently and with a very high quality and manipulated easily using computers. Furthermore, digital data can be transmitted in a fast and inexpensive way through data communication networks.

The easy transmission and manipulation of digital data constitutes a real threat for information creators and distributors e.g. news agencies, museums, libraries, artists, scientists, authors of multimedia documents etc. Copyright owners want to be compensated every time their work is used. Furthermore, they want to be sure that their work is not used in an improper way (e.g. modified without their permission). However when it comes to digital data, copyright enforcement and content verification are very difficult tasks. One solution would be to restrict access to the data using some encryption technique. However encryption does not provide overall protection; once the encrypted data are decrypted, they can be freely distributed or manipulated.

During the last five years significant research efforts have been directed towards facing the challenges posed by digital technology. The solution seems to lie in a technique that dates back to ancient Egypt and Greece: data hiding or steganography. Steganography discusses methods of embedding data within a medium (host medium) in an imperceptible way. All forms of digital data (still images, audio, video, text documents, multimedia documents) can be used for information hiding. In the following we shall limit our discussion to still images which is the topic of this work. Data hiding techniques explore the so-called masking property of the Human Visual System (HVS) that refers to the decrease in the perceived intensity of a visual stimulus when this is superimposed over another stimulus.

A number of distinct application areas, each with different requirements and limitations, have been envisaged for data hiding:

- Copyright protection and fingerprinting. Embedded data can be used as a proof of digital media ownership in case of a copyright dispute or for tracing the image recipient that produced unauthorized copies. The most important requirement in both cases is that embedded data are robust to deliberate or unintentional attacks. Copyright protection data are expected to serve complementary to encryption and copy protection mechanisms.
- Authentication or tamper-proofing. This functionality is equivalent to data integrity verification. Classic data integrity checks, i.e., digital signatures that are based on hashing can be used for this purpose. However, such schemes are sensitive even to the slightest change of the digital medium, whereas it would be desirable that the method in use signals an authentication violation only when significant modifications of the visual content occur. Contrary to copyright protection applications, data inserted for authentication purposes should be fragile, i.e. they should be modified when the image is manipulated.
- Covert communications, i.e., exchange of messages secretly embedded within images. In this case, the

main requirement is that the hidden data do not raise any suspicion that a secret message is being communicated. An ability to secretly convey a fairly large amount of data is a basic requirement for such applications.

- Captioning, i.e., embedding of descriptive information within images for applications like labeling and annotation of medical data, video indexing etc. This is the application with the less stringent requirements, since in most cases no malicious attacks are expected for caption data. The amount of the embedded data in this case is moderately large.

It is obvious that there is no unique set of requirements that all data embedding techniques must satisfy. In this paper we will deal with data hiding for the purpose of copyright protection and will refer to the hidden data using the term watermark.

2. Copyright protection watermarking

In the last years, a plethora of watermarking techniques for copyright enforcement have been proposed in the signal processing literature. A recent review paper [1] lists almost one hundred papers describing watermarking techniques for multimedia data, mostly still images. In a watermarking scheme one can distinguish between three fundamental stages: watermark generation, embedding and detection. Watermark generation aims at producing the watermark pattern using an owner and/or image dependent key. Watermark embedding can be considered as a superposition of the watermark signal on the original image. Finally, watermark detection is usually performed using watermark correlators or hypothesis testing. For a more detailed discussion of the general watermarking framework the interested reader can consult [2, 3].

2.1. Taxonomy

Watermarking techniques can be categorized in a number of classes on the basis of their distinct features.

A number of watermarking techniques require that the original image is available during the detection phase. Such schemes are sometimes referred to as private schemes or image escrow schemes. Since the host image plays the role of noise for the detection phase, its availability greatly facilitates and robustifies detection. Furthermore, the original image can be used to register the watermarked image in order to compensate for geometric distortions such as cropping, scaling, rotation etc. Despite their obvious advantages, methods based on the original image do not fit well in certain applications e.g. automatic Internet search. Image watermarking methods that do not require the original image for watermark detection are called oblivious or blind methods and do not suffer from the above-mentioned disadvantages of private methods. However, their robustness to image modifications and attacks is limited in comparison to private methods.

Another classification scheme for watermarking techniques can be devised by taking into account the domain where the watermark signal is embedded. Certain methods do data embedding in the spatial domain by modulating the intensity of certain pixels, while other techniques modify the magnitude of coefficients in an appropriate transform domain i.e., the DCT, DFT or DWT domain. Watermark embedding on the DFT phase has been also proposed.

Watermarking techniques can be also classified on the basis of the watermark signal dependence on the image where it is hosted. Image dependence is necessary if image characteristics are to be exploited in order to obtain invisible watermarks using masking properties of HVS (see subsection 2.3). Furthermore, image dependent watermarks are inherently more robust to counterfeit attacks, e.g. the SWICO attack that will be presented in subsection 2.4.

Finally, one can distinguish between restricted and unrestricted key watermarks. Restricted key watermarks can be decoded only by individuals that have access to a secret key whereas unrestricted key watermarks can be read (decoded) by every image recipient, although only the image creator can embed or erase the watermark.

2.2. An overview of typical watermarking schemes

One of the most cited watermarking schemes that makes use of the original image at the detection phase is proposed in [4]. According to this scheme the watermark sequence x_i is placed on the n highest magnitude coefficients u_i of the DCT transformed image using the following formula:

$$u_i' = u_i + a u_i x_i \tag{1}$$

The watermark coefficients x_i are zero mean, unit variance normally distributed i.i.d samples. Watermark detection is done by correlating the watermark signal with an estimate of the embedded watermark that is derived by subtracting the original image from the watermarked one. The utilization of the original image by the detection scheme robustifies the proposed technique against a wide range of attacks.

The Fourier transform followed by the so-called Fourier-Mellin transform (FMT), i.e. the Fourier transform applied on a log-polar coordinate system, can be proven to be rotation, scale and translation invariant. In [5] the authors exploit this property in order to construct watermarks that are invariant to such signal manipulations. The watermark is a spread spectrum signal that is embedded in the transform domain. For watermark detection, the original image is subtracted from the watermarked image and the residual is transformed to the FT-FMT domain where correlation with the watermark signal takes place.

A multiresolution watermarking technique is proposed in [6]. The host image is decomposed into subbands using a two-step Discrete Wavelet Transform. The watermark sequence, which has the form of zero-mean unit variance Gaussian noise, is added to the largest coefficients that do not belong to the lowest resolution band. Decoding requires the original image and is done in a hierarchical way. The proposed subband decomposition technique can facilitate placement of the signal in a way that exploits HVS characteristics to obtain imperceptibility.

In [7] the authors embed a binary digit b_i by increasing ($b_i = 1$) or decreasing ($b_i = 0$) the blue channel value $B_{i,j}$ at a certain color image pixel. The magnitude of the modification is proportional to the pixel luminance. In order to recover the embedded bit, an estimate $\hat{B}_{i,j}$ of the pixel's value prior to the bit insertion is obtained by evaluating the mean value in a neighborhood around the current pixel. This estimate is subtracted from the value $B'_{i,j}$ of the pixel under investigation and the difference δ is compared against a threshold δ_T to decide whether a 0 or a 1 has been embedded. In order to achieve robustness the same bit can be embedded in a number of different, randomly selected pixels. An image-specific evaluation of the threshold δ_T is also proposed.

In [8] a method that embeds a binary watermark image in the spatial domain is proposed. A spatial transform that maps each pixel of the watermark image to a pixel of the host image is used. Chaotic spread of watermark image pixels in the host image is achieved by means of the so-called toral automorphisms. For watermark embedding, the intensity of the selected pixels is modified by an appropriate function that takes into account neighborhood information in order to achieve watermark robustness to modifications. For detection a suitable function is applied on each of the watermarked pixels to determine the binary digit (0 or 1) that has been embedded. The inverse spatial transform is then used to reconstruct the binary watermark image.

In the method proposed in [9] the image I is split into two random subsets A, B and the intensity of pixels in A is increased by a constant embedding factor k. Watermark detection is performed by evaluating the difference of the mean values of the pixels in sets A, B. This difference is expected to be equal to k for a watermarked image and equal to zero for an image that is not watermarked. Hypothesis testing can be used to decide for the existence of the watermark. The above algorithm is vulnerable to lowpass operations. Extensions to this algorithm are proposed in [10]. According to this paper, the robustness of the method can be increased by grouping pixels so as to form blocks of certain dimensions e.g. 2×2, a fact that enhances the lowpass characteristics of the watermark signal. Alternatively, one can take advantage of the fact that different embedding factors k_{ij} can be used for each pixel, to shape appropriately the watermark signal. An optimization procedure that calculates the appropriate embedding value for each pixel so that the energy of the watermark signal is concentrated at low frequencies is proposed. Constraints that ensure that the watermark signal is invisible can be incorporated in the optimization procedure.

In [12] the authors derive analytical expressions for the probabilities P_-, P_+ of false negative and false positive watermark detection. Their model assumes an additive watermark and a correlator-based detection stage. Both white watermarks and watermarks having lowpass characteristics are considered. The host image is treated as noise, assuming a first order separable autocorrelation function. The probabilities P_-, P_+ are expressed in terms of the watermark to image power ratio. The authors conclude that detection error rates are higher for watermarks with lowpass characteristics.

Correlation detectors are optimal only if the channel noise, i.e. the host image, can be modeled as additive white Gaussian noise. In [11] it is proven that detector reliability can be improved by prefiltering the host image and the watermark with a whitening filter.

In [13], the authors study the performance of a 2-D multipulse amplitude modulation watermarking scheme. According to this scheme, the information-carrying signal is expressed as a linear combination of a set of L orthogonal functions $p_i[m,n]$:

$$w[m,n] = \sum_{i=0}^{L-1} b_i p_i[m,n] \tag{2}$$

The authors derive analytic expressions for the correlation coefficients $r_i = < y, p_i >$ where y is the watermarked image and $< \cdot >$ denotes inner product. Both uncorrupted images and images that have undergone linear filtering are considered. Using the derived expressions, the maximum likelihood detector structure and the corresponding decision regions are inferred and the probability of bit error is calculated. The detector structure in cases where the exact location of the watermark pulses is unknown due to attacks like cropping and affine transformations, is also derived.

Spatial patterns that can be embedded in a watermark image in order to facilitate registration for translation or cropping compensation are presented in [14].

2.3. Perceptual masking and image watermarking

During the last decades significant research efforts within the context of vision science have been directed towards understanding and modeling the operation of the human visual system (HVS). Obviously, results obtained through this research are directly applicable to image processing, since the final judge for the output of an image processing system is the human observer. Understanding properties of HVS is of paramount importance for many areas including image coding, image quality assessment, filtering etc [15]. A fundamental property of the HVS that is usually incorporated in such techniques is *noise masking* or *distortion masking* which refers to the decrease in the perceived intensity of a visual stimulus when this is superimposed over another stimulus. The noise masking properties can be used for the evaluation of the *Just Noticeable Distortion* (JND) and the *Minimally Noticeable Distortion* (MND). JND refers to the biggest possible invisible image distortion, whereas MND refers to a distortion which is less visible than any other distortion of the same power. The evaluation of JND for a certain image is equivalent to the evaluation of a distortion map $jnd(m, n)$, called JND profile. Each element of the JND profile gives the absolute value of the biggest invisible distortion that we can cause in the corresponding image pixel. Noise masking properties have been studied not only for the intensity domain but also in other image representation domains, e.g., in the DCT domain. HVS understanding is also crucial for the development of image quality metrics that mirror viewer's assessment of picture quality. It is obvious that results obtained for perceptual masking in the area of image compression are directly applicable in image watermarking. Spatial domain JND and MND profiles can be readily incorporated in the design of invisible watermarks by providing an upper limit for the intensity alterations caused by watermark embedding. Frequency domain watermarking techniques can make use of the DCT / DFT coefficient visibility thresholds and perceptual weighting factors in order to provide imperceptible watermarks. Finally, perception-based image quality metrics can be used for assessing the invisibility of a certain watermarking scheme or be incorporated in the watermark design procedure as an optimization criterion.

A number of attempts to incorporate perceptual masking in watermarking techniques have been reported in the literature. In [16] a combination of frequency domain and spatial domain perceptual masking is proposed. The image is split into 8×8 blocks and their DCT is evaluated. Then a frequency mask that predicts the contrast threshold for each coefficient is computed for each block. This perceptual mask is used to scale the DCT transform of a pseudo-noise watermark sequence. After using the inverse DCT the authors use a spatial masking model similar to the one used in [17] to verify that the watermark is invisible.

In [18] the authors embed a watermark signal in the DCT domain by modifying a number of predefined DCT coefficients. Then they use a weighting factor β_{ij} to weight the watermark signal in the spatial domain according to the HVS characteristics. The following relation is used:

$$y''_{ij} = y_{ij}(1 - \beta_{ij}) + \beta_{ij} y'_{ij} \tag{3}$$

where y_{ij} is the original image, y'_{ij} is the initial watermarked image and y''_{ij} is the watermarked image after the perceptual weighting operation. β_{ij} is chosen so that in low noise sensitivity regions $\beta_{ij} \approx 1$ and thus $y''_{ij} = y'_{ij}$, whereas in image regions that are sensitive to noise $\beta_{ij} \approx 0$ and $y''_{ij} = y_{ij}$. β_{ij} was chosen to be the normalized sample variance within a 9×9 block around the current pixel.

In [19] the following scheme is used to embed the watermark in the DCT domain in a perceptually meaningful way:

$$X^*_{uv} = \begin{cases} X_{uv} + J_{uv} w_{uv} & if \;\; X_{uv} > J_{uv} \\ X_{uv} & otherwise \end{cases} \tag{4}$$

where X_{uv}, X^*_{uv} are the DCT coefficients of the original and the watermarked image respectively, w_{uv} is the watermarking sequence and J_{uv} is the just noticeable difference value for uv coefficient, as predicted by the models reported in either [21] or [20].

2.4. Attacks

A number of specially engineered attacks that remove or render unusable certain types of watermarks have been reported in the literature. An extensive list of attacks and the related counter measures can be found in [3]. In [22] the authors present simple and almost invisible image distortions (deletion of a small number of image columns or combination of minor geometric distortions followed by blurring) that render watermarks produced by several methods undetectable. In [23] the authors propose an attack for the so-called unrestricted key watermarks assuming that the pirate has access to a watermark detector. The method uses a trial and error procedure to estimate a combination of pixel values that has the largest influence on the detector for the least disturbance of the image, and then uses this estimate in order to eliminate the watermark.

Another class of attacks utilize counterfeit watermarking schemes to raise multiple claims of copyright ownership. Such an attack, named Single Watermarked Image Counterfeit Original (SWICO) is introduced in [24]. Suppose that individual A has watermarked an image I by adding a watermark signal W to obtain $\hat{I}$. An attacker constructs a fake original image $\hat{I}'$ by subtracting another watermark W' from $\hat{I}$. She can then claim that her fake original $\hat{I}'$ is the true original and that $\hat{I}$ is her watermarked image. Furthermore, W' can be detected on I. Watermark schemes that are vulnerable to this type of attacks are called invertible. Non-invertible schemes can be devised e.g. by using watermarks that depend on both the host image and the image owner. Another attack called Twin Watermarked Image Counterfeit Original (TWICO) that involves two watermarked versions of the same image is described in the same paper.

3. Current Research Topics

In this section two new watermarking schemes will be presented. The main advantage of the first method is its robustness against geometric distortions. The second scheme uses a chaotic watermark with lowpass characteristics.

3.1. Ring-shaped watermarks

Let I be a grayscale $N \times N$ image and $W(k_1, k_2)$ a watermark signal in the DFT domain. Watermark embedding is performed in the magnitude of the DFT image coefficients :

$$M^{'}(k_1, k_2) = M(k_1, k_2) + aW(k_1, k_2) \qquad (5)$$

where $M(k_1, k_2) = |I(k_1, k_2)|$ is the magnitude of the original image DFT coefficients. The watermark consists of a 2-D zero-mean random bi-valued sequence. The frequency region in which the watermark is embedded is a ring covering the middle frequencies. The ring is separated in S sectors and in homocentric circles of radius $r \in [R_1, R_2]$. Each circular sector is assigned the same value 1 or -1. Watermark detection does not involve the original image and is carried out using a correlator detector.

The proposed method is robust to compression as well as translation, rotation, cropping and scaling. Robustness to translation stems from the fact that the DFT magnitude is translation invariant. Rotation in the spatial domain causes rotation of the Fourier domain by the same angle. Since the watermark consists of S sectors having identical values, its detection is possible even after a small rotation. It can be proven that the size of the watermark on the Fourier transformed scaled image remains unaltered. Therefore correlation-based detection can be easily performed. Cropping attacks change the frequency-sampling step. If the size of the initial image is known then, prior to correlation, the frequency sampling step of the watermark should be made equal to the frequency-sampling step of the cropped image. If the size of the initial image is unknown, the correlation should be repeated for different frequency sampling steps. A detailed description of the method along with experimental results can be found in [25]

3.2. Chaotic spatial domain watermarks

Bi-valued digital signals generated by properly tuned chaotic dynamical systems posses certain properties (complexity, controlled lowpass characteristics) that make them suitable for watermarking applications. A 1-D chaotic watermark signal can be produced using a one-dimensional discrete map $\mathbf{F} : U \to U,\ U \subset \mathbb{R}$:

$$z(n+1) \ = \ \mathbf{F}(z(n), \lambda) \ \ , \ \ z(n) \in U, \ \lambda \in \mathbb{R} \qquad (6)$$

where $n = 0, 1, 2, ...$ denotes map iterations. The mapping is chosen so that strongly chaotic signals are produced, a fact that is necessary to obtain watermarks with the desired characteristics. A bi-valued sequence $s(n) \in \{-1, 1\}$ is obtained by “thresholding” $z(n)$. Parameter λ controls the frequency of trajectory oscillations, and subsequently, the frequency characteristics of $s(n)$. A 2-D watermark W, of size $N \times M$, is then formed by applying Peano scan on a sequence $s(n)$ of size NM. A function $\mathcal{F}$ that modifies the original watermark signal W_0 according to the host image is used to produce image-dependent watermarks. Watermarks generated by this procedure can be embedded using general superposition and multiplication operators ($\oplus, \otimes$):

$$x_w(i,j) \ = \ x_o(i,j) \ \oplus h_{ij} \otimes w_{ij} \qquad (7)$$

where $X_o = \{x_o(i,j)\}$ is the original image, $X_w = \{x_w(i,j)\}$ is the watermarked one and $H = \{h_{ij} \in \mathbb{R}\}$ is an *embedding mask*. The detection module does not require the original image and implies a suitable test statistic similar to the one used in [26]. Further details of this method can be found in [27].

4. Conclusions

Image watermarking is a new challenging field that involves principles and techniques from a range of diverse disciplines like communications, signal processing, encryption and steganography. Despite the efforts spent during the last years towards devising an efficient watermarking scheme, none of the techniques proposed so far seems to be robust to all possible attacks and image processing operations. Furthermore, even if a watermark endures all present attacks, no one can be sure that new ingenious attacks will not be devised in the future. However, considering the enormous financial implications of copyright protection and the continuous increase of efforts spend by renowned research institutes around the globe, one can expect that sooner or later the field of watermarking will be able to provide efficient solutions to the problem of intellectual property rights protection. Of course, in order to establish confidence for the evolving technique among potential users, a few actions need to be taken. Such actions include establishing a globally accepted watermarking protocol and devising watermark performance benchmarks. In terms of the non-technical aspects (which, in this case are of equal importance) the legal status of watermarking should be investigated and clarified and a trusted central authority (similar to the Copyright Clearance Center) should be established and charged with the regulation and operation of the watermarking framework.

References

[1] M. Swanson, M. Kobayashi, A. Tewfik, “Multimedia Data-Embedding and Watermarking Technologies”, Proceedings of the IEEE, vol 86, no 6, June 1998.

[2] G. Voyatzis, N. Nikolaidis and I. Pitas, "Digital Watermarking: An Overview", IX European Signal Processing Conference (EUSIPCO'98), vol. I, pp. 9-12, September 1998

[3] G. Voyatzis, I. Pitas, "Protecting Digital-Image Copyrights: A Framework", IEEE Computer Graphics & Applications, vol. 19, no. 1, January/February 1999.

[4] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Processing, vol. 6, no. 12, pp 1673-1687, 1997.

[5] J. O Ruanaidh, T. Pun, "Rotation scale and translation invariant spread spectrum digital image watermarking", Signal Processing, special issue on Copyright Protection and Access control, vol 66, no 3, pp 303-318, May 1998.

[6] X. G. Xia, C. G. Boncelet, and G. R. Arce. A multiresolution watermark for digital images. In *Proceedings of ICIP'97*, volume I, pages 548–551, Atlanta, USA, October 1997.

[7] M. Kutter, F. Jordan, F. Bossen, "Digital Watermarking of Color Images Using Amplitude Modulation", Journal of Electronic Imaging, vol 7, no 2, pp 326-332, April 1998.

[8] G. Voyatzis and I. Pitas, "Digital Image Watermarking using Mixing Systems", Computer & Graphics, Elsevier, vol. 22, no. 4,pp. 405-416, 1998

[9] I. Pitas, "A Method for Watermark Casting in Digital Images", IEEE Trans. on Circuits and Systems on Video Technology, vol. 8, no.6, pp 775-780, October 1998

[10] N. Nikolaidis, I. Pitas, 'Robust image watermarking in the spatial domain' Signal Processing v 66 no 3 (May 98), pp 385-403

[11] G. Depovere, T. Kalker, J.P. Linnartz "Improved Watermark Detection Reliability Using Filtering Before Correlation" Proceedings ICIP98, vol I, pp 430-434.

[12] T. Kalker, J-P. Linnartz, and G. Depovere. "On the reliability of detecting electronic watermarks in digital images", in Proc. of EUSIPCO'98, vol I, pp 13-16,

[13] J. Hernandez, F. Perez-Gonzalez, J. Rodriguez, G. Nieto, "Performance Analysis of a 2-D-Multipulse Amplitude Modulation Scheme for Data Hiding and Watermarking of Still Images", IEEE Journal on Selected Areas in Communications, vol 16, no 4, pp 510-524, May 1998.

[14] A. Z. Tirkel, C. F. Osborne, and T. E. Hall. Image and watermark registration. *Signal Processing, sp. issue on Copyright Protection and Access control*, vol 66, no 3, pp 373-384, May 1998.

[15] N. Jayant, J. Johnston and R. Safranek, "Signal Compression Based on Models of Human Perception", Proceedings of the IEEE, vol. 81, no 10, pp 1385-1422, October 1993.

[16] M. Swanson, B. Zhu, A. Tewfik, " Transparent robust image watermarking", *Proc. 1996 IEEE Int. Conference on Image Processing* , vol III, pp 211-214.

[17] B. Zhu, A. Tewfik, O. Gerek, "Low Bitrate Near-Transparent Image Coding", 1995 SPIE Conf. on Wavelet Applications II, vol 2491, pp 173-184.

[18] M. Barni, F. Bartolini, V. Cappellini, A. Piva, " A DCT-domain system for robust image watermarking, Signal Processing v 66 no 3 (May 98), pp 357-372.

[19] C. Podilchuk, W. Zeng, "Image-Adaptive Watermarking Using Visual Models", IEEE Journal on Selected Areas in Communications, vol 16, no 4, pp 525-539, May 1998.

[20] R. Safranek, "Perceptually based prequantization for image compression", in Proc SPIE Conf Human Vision, Visual Processing and Digital Display V, 1994.

[21] A. B. Watson "DCT Quantization Matrices Visually Optimized for Individual Images" Proceedings, Human Vision, Visual Processing, and Digital Display IV, Bellingham, WA, SPIE, pp. 202-216.

[22] F. Petitcolas, R. Anderson and M. Kuhn. "Attacks on copyright marking systems" In David Aucsmith, Ed., Second Workshop on Information Hiding, in vol. 1525 of Lecture Notes in Computer Science , pp. 218–238, April 1998.

[23] I. Cox, J. Linnartz, "Some General Methods for Tampering with Watermarks". IEEE Journal of Selected Areas in Communications, vol 16 no 4, pp 587-593, May 1998.

[24] S. Craver, N. Memon. B. Yeo, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications", IEEE Journal on Selected Areas in Communications, vol 16, no 4 , pp 573-586, May 1988.

[25] V. Solachidis, I. Pitas, "The use of circular symmetric watermarks in the 2-D DFT domain", Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing, (ICASSP'99), accepted for publication.

[26] N. Nikolaidis and I. Pitas, Copyright protection of images using robust digital signatures, IEEE International Conference on Acoustics, Speech and Signal Processing, vol. 4, pp. 2168-2171, May 1996.

[27] G. Voyatzis and I. Pitas, "Chaotic Watermarks for Embedding in the Spatial Digital Image Domain", IEEE Int. Conference on Image Processing (ICIP'98), vol II, pp 432-436, October 1998