A Watermarking Framework for Copyright protection of Digital images

G.Voyatzis and I.Pitas
Department of Informatics
University of Thessaloniki, Thessaloniki, 54006 GREECE
fax: +3031-996304, email: {voyatzis,pitas}@zeus.csd.auth.gr

1 Introduction

Security issues for digital data were intensively discussed in the scientific community in the past decade. The rapid evolution of digital networks, digital libraries and other World Wide Web services is obstructed by digital data piracy. The convenient exposition of digital products in the web pages can be easily followed by creating illegal identical copies or performing illegal retransmissions. The same happens with transmitted data through insecure channels. Nowadays, digital data security covers topics like access control, authenticity and copyright protection of still images, audio, video and, extensively, multimedia products [1]. The future networking environment requires tools that provide

- Secure and fast digital data encryption/decryption
- User capability to verify the originality of the received data.
- Robust and trustworthy marks for indicating copyright and legal ownership.

Private or public key cryptography has been widely used for data access control. Well-established algorithms (e.g. RSA and DES) can be used [2]. *Digital signatures* are also based on cryptographic algorithms and have been proposed for checking authenticity of digital messages [3]. The concept of *digital watermark* is a new topic [4]. It is associated with the technique of data hiding known as steganography [5]. Steganography or "covered writing" has a long history and includes various methods for secret communications. In contrary to cryptography, steganography does not arouse suspicion for an important message, possibly carried inside a harmless one. Watermarking hides a secret and personal message in order to protect the copyright property of a product or to demonstrate its data integrity (referred also as tamper proofing or content verification) [6]. An important difference between steganography and watermarking, is related to the attackers' goal. A pirate tries to reveal the information carried by a steganography message. In the watermarking cases, pirates either try to remove the watermark, in order to violate copyright, or to cast the same watermark, after data alterations, in order to create false authenticity proof. Watermark hiding is based on imperceptible alterations of digital data. Generally speaking, human perception tolerates much more modification on the audio or video data than on still images. Therefore, we have much more freedom for watermarking

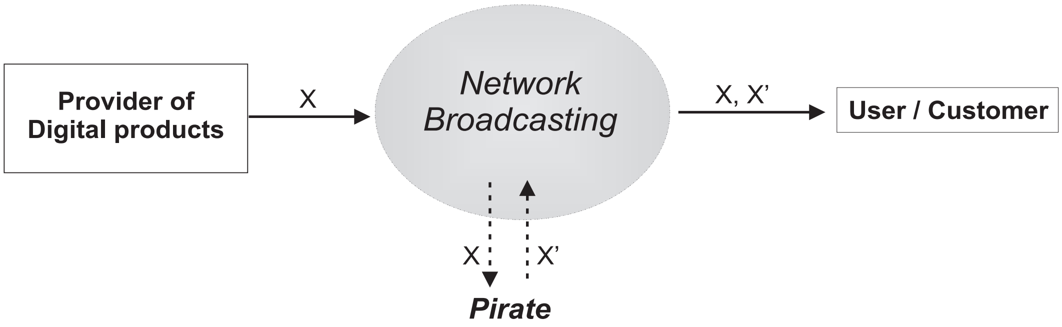

Figure 1: Elementary system for digital image distribution.

digital audio/video than still images. Without significant loss of generality, we refer to the watermarking of images having sufficient number of grayscale levels or colors (e.g. 8-bit grayscale or 24-bit color images) and we discuss watermark efficiency for copyright protection.

2 Digital image protection via watermarking

Digital data manipulation and delivery can be carried out through network services or broadcasting. Building a realistic framework and dealing with issues related to intellectual property rights, is a complicated problem. Watermarks can contribute significantly for drawing up a digital data protection system. We illustrate the role of the watermarks by considering the elementary digital media delivery system presented in Fig. 1. The user gets a digital product from a provider (copyright owner or authorized distributor). Access and transmission take place in a global network environment. Users do not violate the copyright property because they do not retransmit the products. Pirates may harm the copyright owner by reproducing and retransmitting digital products illegally. Thus, pirates can be considered as unauthorized providers. The provider demands a reliable scheme for browsing the network and searching efficiently for copies that originally belongs to him/her. Strong indications for asserting legal ownership should be also supplied by the protection scheme.

A digital watermark (called also copyright label or invisible stamp) is associated with a unique private identification number (ID), which is called *watermark key* (K_{pr}). Each provider possesses a unique secret key K_{pr} (or a finite set of keys) and the watermarking based protection scheme consists of the following actions:

- The copyright owner alters the digital data of the original image I_0 and produces the watermarked one I_w by using the private key and a *public* or *private* algorithm $\hat{E}$:
$$I_w = \hat{E}(I_0, K_{pr}) \tag{1}$$
- The copyright owner can detect the watermark by using an algorithm $\hat{D}$:

$$\hat{D}(I, K) = \begin{cases} 1 & \text{if } I \sim I_w \text{ and } K = K_{pr} \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

The relation $A \sim B$ means perceptual similarity between the images A and B. We note that $I \sim I_w$, since watermarking should produce almost invisible alterations.

In order to complete the watermarking scheme, we include, additionally, the following optional actions that might be performed by the provider:

- The provider possesses a personal library $\mathcal{L}$ of his/her digital images and a "matching procedure" $\hat{m}$ such that:

$$\hat{m}(I, \mathcal{L}) = \begin{cases} 1 & \text{if } \tilde{I} \in \mathcal{L} \text{ and } \tilde{I} \sim I \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

- The provider registers his/her watermark key K_{pr} to an authority and ensures its uniqueness.

- The provider registers his/her images $I \in \mathcal{L}$ to an authority to ensure (time-stamp) his/her ownership on I.

The aim of the above copyright protection system is to give to the provider the facility to check possible violation of his/her copyright property by examining effectively as many as possible digital images exposed in the distribution network. A positive watermark detection ($\hat{D}(I, K_{pr}) = 1$) is an indication of ownership and can be used as substantiated evidence to demonstrate legal ownership in a court of law.

3 Elementary watermarking procedures

Various definitions for digital watermark can be met in literature. For digital images of size $N \times M$, it is convenient and quite general to consider two dimensional (2D) watermark signals that consist of binary or, more generally, ternary elements:

$$W = \{w(\mathbf{k}); \mid w(\mathbf{k}) \in \{-1, 0, 1\}\ ,\ \mathbf{k} \in \hat{W}\} \tag{4}$$

where $\hat{W}$ denotes a 2D grid of size $N \times M$. Vector $\mathbf{k}$ stands for pointing the grid positions (watermark pixels). We can distinguish three fundamental watermarking stages, namely, watermark generation, embedding and detection. A schematic presentation of the overall algorithm is shown in Figure (2).

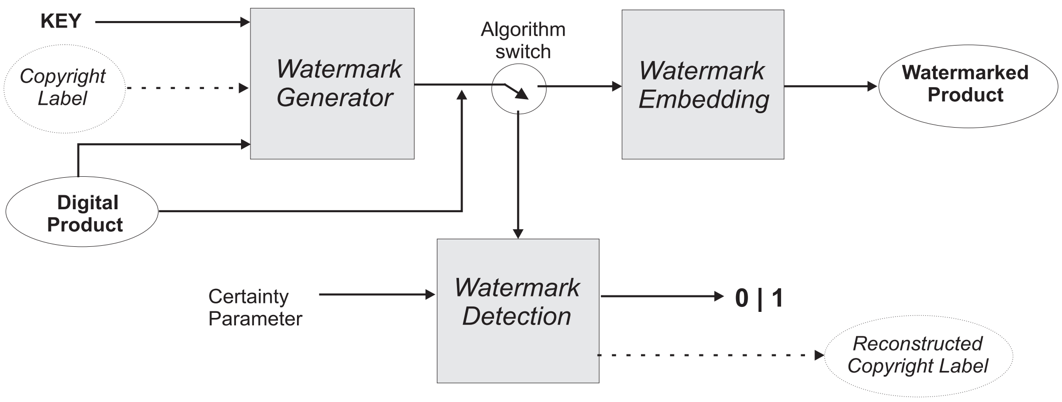

Figure 2: Overall watermarking algorithm including embedding and detection. Watermark generation take place for both procedures. The copyright label is a binary stream that carries public information about ownership.

3.1 Watermark generation

Let $\mathbf{W}$ be the set of possible watermark signals, i.e., all the signals having elements in $\{-1, 0, 1\}$. We consider the finite and countable space $\mathbf{K}$ of keys. If $\mathbf{I}$ denotes the set of digital images, a watermark generation procedure should be defined by the following function :

$$\mathcal{G} \ : \ \mathbf{I} \times \mathbf{K} \to \mathbf{W} \ \ , \ \ W \ = \ \mathcal{G}(I, K) \tag{5}$$

where $K \in \mathbf{K}$ is the watermark key and $I \in \mathbf{I}$ is the image where the watermark will be embedded. Without loss of generality, we decompose $\mathcal{G}$ as it follows:

$$\mathcal{G} \ = \mathcal{T} \circ \mathcal{R} \ \ , \ \ \mathcal{R} : \mathbf{K} \to \mathbf{W} \ , \ \mathcal{T} : \mathbf{W} \times \mathbf{X} \to \mathbf{W} \tag{6}$$

$\mathcal{R}$ may be based on a pseudo-random number generator or, generally, on chaotic systems. When a key K is inserted in $\mathcal{R}$, a fixed watermark $W_0 = \mathcal{R}(K)$ is created. $\mathcal{T}$ modifies W_0 to obtain the final watermark W that depends on the particular image. The watermark modification function $\mathcal{T}$ should take into account only robust characteristics of the perceived image data. Both the original image I_0, the watermarked one I_w and a modified copy of I_w (denoted as I'_w) must result adequately in the same watermark when perceptual similarity is satisfied:

$$W = \ \mathcal{T}(W_0, I_0) \ \simeq \ \mathcal{T}(W_0, I_w) \ \simeq \ \mathcal{T}(W_0, I'_w) \ \text{ for any } \ I_0 \sim I_w \sim I'_w \tag{7}$$

3.2 Watermark embedding

The embedding procedure is defined as a superposition of the digital watermark signal $W = \{w(\mathbf{k})\}$ onto the original image $I_0 = \{x_0(\mathbf{k})\}$ of the same dimension. We denote the embedding procedure by $\mathcal{E}$ and we define it as:

$$\mathcal{E} : \mathbf{X} \times \mathbf{W} \times I\!R^2 \to \mathbf{X} \ \ , \ \ x_w(\mathbf{k}) \ = \ x_0(\mathbf{k}) \ \oplus H(\mathbf{k}) \otimes w(\mathbf{k}) \tag{8}$$

$H(\mathbf{k})$ is a 2D *watermark embedding mask* that controls watermark visibility and robustness. $\oplus$ is a superposition operator including appropriate truncations and quantisation and $\otimes$ is a generalized multiplication operator. The watermarked image is denoted by $I_w = \{x_w(\mathbf{k})\}$. The invertibility of $\mathcal{E}$ is desirable but not necessary, since the copyright owner can store the original securely. Instead of applying (8) directly on the intensity or luminance domain, DCT domain [7, 8] or the wavelet domain [9] can be used.

3.3 Watermark detection

Watermark detection is the most crucial part in a watermarking framework. By adopting an hypothesis testing framework [10], we obtain, in practice, detection errors from relation (2). Such errors are classified in two categories :

Type I error: Watermark is detected although it does not exist in the data. Such false positives contribute to the probability of false alarm (P_{fa}).

Type II error : Watermark is not detected in the data although it exists. Thus, we get false negatives that contribute to the probability of false rejection (P_{rej}).

By taken into account the above error probabilities, we define a detection procedure as follows :

$$\mathcal{D} \ : \ \mathbf{I} \times \mathbf{K} \to \ (0, 1) \subset I\!R \tag{9}$$

$$\mathcal{D}(I, W) = \mathcal{D}(I, \mathcal{G}(I, K_{pr})) \; = \; c \tag{10}$$

The output c denotes the *certainty* of a positive detection and a final decision is taken as follows:

$$c \; \geq \; c_{thres} \quad \Longrightarrow \quad \text{watermark exists} \tag{11}$$

The parameter c_{thres} is the *certainty level* for detection and is chosen by the image provider who applies detection. Generally, is $c = f(t)$, where t is a test statistic. The chosen certainty level c_{thres} is associated with a test value t^* that controls (balances) the two types of error. Figure 3 illustrates this situation. When c is close to unit, false negatives become insignificant ($P_{fa} \rightarrow 0$). However, at the same time, $P_{rej} \rightarrow 1$ and, subsequently, the performance of the detector is reduced. $\mathcal{D}$ approximates the ideal detector $\hat{D}$ of Eq. (2)when both P_{fa} and P_{rej} take values close to zero.

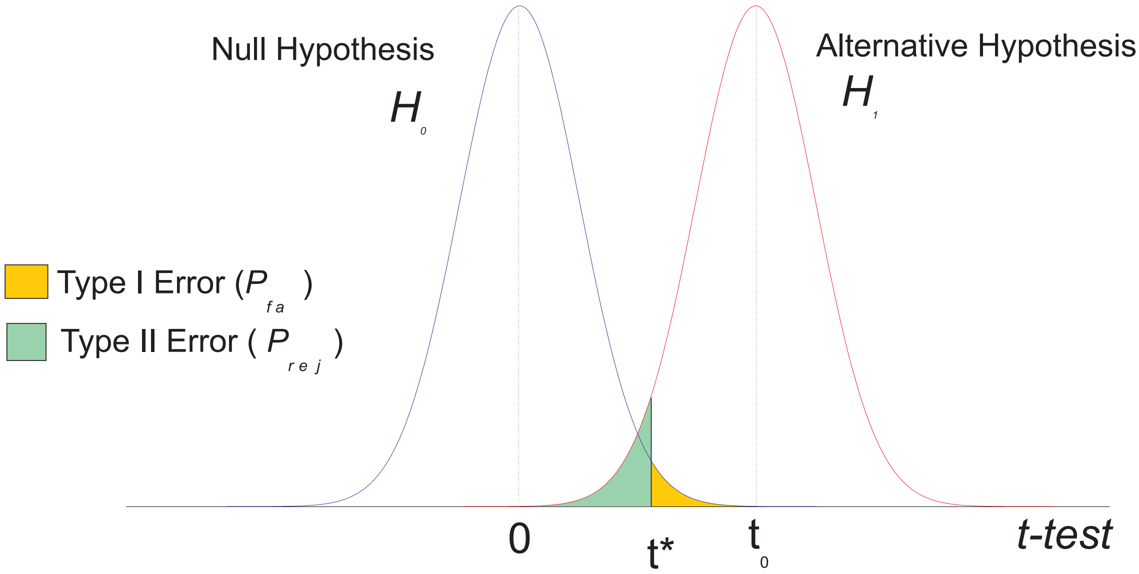

Figure 3: The distributions of the Null (watermark does not exist) and Alternative (watermark exists) hypotheses for the statistical detection based on the *t-test*. The certainty ($c = 1 - P_{fa}$) depends on the selection of the t-threshold (t^*).

A watermarking Example

Several already proposed watermarking schemes fall in this general framework. A a special case we present a watermarking scheme which is based on the above mentioned framework [14]. For illustration reasons, we summarize a simple version of the method and we apply it to the image "Lenna".

A. The bipolar $\{-1, 1\}$-valued watermark $W = \{w(i, j)$, presented in Figure 4 as a black and white image, is created by a watermark generation procedure $\mathcal{G}$ designed by using a chaotic system. The set of integer numbers is the watermarking key set. Each integer corresponds to a set of parameters for the chaotic system, through a well defined function. Therefore, each key represents a unique initial condition of the chaotic sequence and, therefore, sufficiently different watermarks are created for any different keys.

B. Let $I_0 = \{x(i, j)\}$ denotes the 8-bit luminance space of the original image (Figure 5a).The watermarked image I_w, having the same size as the original, is formed

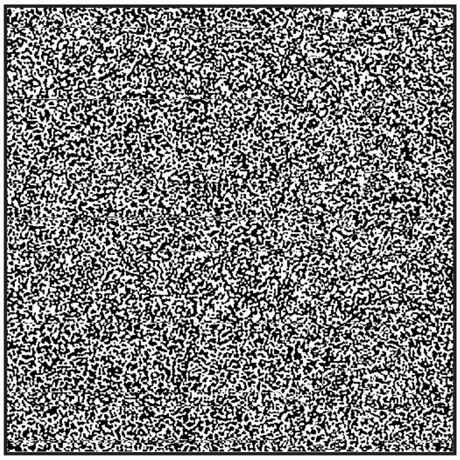

Figure 4: A chaotic binary watermark for embedding in a digital image

by applying (8) and by using a constant embedding mask ($h_{ij} = h = const$) and $\oplus$ is the usual addition operator that accounts appropriate truncations:

$$x_w(i,j) \;=\; \begin{cases} 0 & \text{if } x(i,j) + h\,w(i,j) < 0 \\ 255 & \text{if } x(i,j) + h\,w(i,j) > 255 \\ x(i,j) + h\,w(i,j) & \text{otherwise} \end{cases} \tag{12}$$

The constant h should be small in order to guarantee the invisibility of the watermark in I_w. For $h = 2$ the watermarked image, presented at the left part of figure 5b, results. By using $h = 8$ the watermark embedding causes degradations shown in the right part of figure 5b.

C. We can apply detection on any image I of the same size. The watermark W is generated by using the specific key and the image I. The image pixels are divided in two subsets $\mathbf{A} = \{(i,j)|w_{ij} = 1\}$ and $\mathbf{B} = \{(i,j)|w_{ij} = -1\}$ having mean luminance values $\bar{A}$ and $\bar{B}$ respectively. We consider the following detection response:

$$R \;=\; \mathcal{D}(I,W) \;=\; \bar{A} \;-\; \bar{B} \tag{13}$$

We assume that x and w are statistically independent random variables. Thus, R should follow the normal distribution $N(\bar{R},\sigma)$, where is $\bar{R} = 2\,h$ when W exists in I and $\bar{R} = 0$ otherwise. When a watermarking image I_w is modified somehow (e.g. by lossy compression or filtering), we expect $R < 2\,h$. Watermark existence is assumed when $R > R_{thres}$. The constant R_{thres} is a threshold value associated with a certainty level c_{thres} for a positive detection. e.g. after numerical experiments we found that for $R_{thres} > 0.1$ the minimum detection certainty is 99.9%. Figure 6 shows the value of R obtained from I_w by using 1000 incorrect watermark keys. In the same figure we display also some labeled (blue) peaks of R's, which have been obtained from I_w and some compressed versions of it. The correct key is used for each one of these peaks. By decreasing R_{thres} watermark detection is possible even for high compression ratios (or, generally, large modification). However, in this case false alarms appear.

4 Basic demands for watermarking

The watermarking fundamental concepts, presented in the previous section, are efficient for protecting the copyright property if the following features characterize the elementary procedures $\mathcal{G}, \mathcal{E}$ and $\mathcal{D}$:

4.1 Perceptual quality preservation

When a watermark is embedded in a digital image/video or audio signal, their perceived quality should not be reduced. Such a requirement is directly satisfied when the watermark is invisible. Therefore, the human information perception should be taken into account. In the embedding scheme, described by (8), the proper choice of the embedding mask $H(\mathbf{k})$ guarantees invisibility (i.e. $|H(\mathbf{k})| < JND$ where JND denotes the Just Noticeable Distortion on the image). However, watermark invisibility implies potential watermark removal by lossy compression, and, possibly, by other processing operations. Small perceivable alterations, which can not be considered as distortions to the original, might be allowed. We note that only the watermarked image is available to the user.

4.2 Trustworthy Detection Process

The performance of a watermark detection procedure $\mathcal{D}$ can be evaluated by accounting the total error probability $P_{err} = P_{fa} + P_{rej}$. The contribution of the errors P_{fa} and P_{rej} to form the total detevtion error P_{err} is controlled by the certainty level c_{thres}. We distinguish the following choices:

- **Detection with low certainty**. False alarms are frequent. However, the probability to miss the detection of a watermarked image is very small. The provider can ascertain that the positive detection is reliable by searching his/her database and applying the matching process $\hat{m}$.

- **Detection with high certainty**. In this case $P_{fa} \to 0$ and the detector provides very reliable positive detection. However, the rejection probability may become quite significant. Watermark detection with insignificant false alarm probability may stand, in a court of law, as a sufficiently reliable evidence for proving legal ownership.

The capability of $\mathcal{G}$ to produce an enormous watermark set $\mathbf{W}$, consisting of well distinguishable elements, is a necessary condition for achieving very low false alarm probabilities. Therefore, rich *complexity* should characterize watermark signals (e.g. see Figure 4).

4.3 Watermarking computational efficiency of the overall watermarking system

Watermark casting and detection are two separate algorithms. They should be easy to use, applicable for any digital image and trustworthy. Watermark casting is applied on the particular products that belong to the provider only once. However, detection should be applied to a large set of publicly exposed images. Therefore, a very fast watermark detection is desirable.

The knowledge of the private key and the digital image should be sufficient to proceed the watermark detection. Watermarks could be combined with an automated search procedure that searches any publicly accessible domain in a network environment for illegal copies (web crawling). A necessary condition, for developing such a system, is to avoid the use of the original product or any other information associated with it, in the detection algorithm.

4.4 Robustness to digital processing

An original digital image I may be modified by any provider or user for improving quality, data compression, digital editing etc. Copyright protection is desirable for products with sufficient quality. Preservation of image quality implies preservation of perceptual similarity.

Usually, we demand watermark robustness to the following image processing operations:

- **Lossy Compression**. It is the most widely used procedure for storing and transmitting digital images/video and audio. JPEG and MPEG algorithms are widely used and provide high compression ratio and desired quality. Compression algorithms tend to remove invisible information that can be related to the watermark. Therefore, watermarks should combine invisibility and robustness simultaneously.

- **Filtering**. Filtering is applied to remove noise or to improve the perceptual quality. It can remove watermarks as well. Attackers may also develop filters specified for watermark removal. Filters are usually lowpass and, thus, watermarks should possess lowpass characteristics.

- **Geometric modifications**. For digital images, such modifications, usually, include scaling, rotation, cropping, reflection and line/column extraction or insertion. Watermark detection in geometrically modified products and without resorting to the original product, is not easily manipulated.

- **Different image presentations** A watermarked digital image I_w can be printed or presented on slides. Afterwards a digital copy I'_w can be created by rescanning. Watermark should be still detected in I'_w when the above procedures do not reduce the image quality significantly.

- **Color correction and contrast enhancement**. Usually, watermarks are embedded in the luminance component in order to resist to compression.

5 Attacks and watermarking system efficiency

5.1 Intentional attacks

The watermarking scheme may be attacked indirectly and its capacity to indicate legal ownership may be reduced. In the following, we discuss possible attacks and ways for defense. We remind the reader that we do not allow the use of originals in the detection procedure.

Extraction of counterfeit watermarks [11]. The pirate knows the principle of the public watermarking detection algorithm and, subsequently, may form a signal W', for a particular product X, which forces the detector to output a positive answer. Therefore W' is a watermark signal that had never been embedded in X and the pirate uses it as his/her own watermark. However, W' should be associated with a key $K \in \mathbf{K}$ through the watermark generation procedure $\mathcal{G}$, which, generally, is not invertible and, therefore, such attack seems extremely difficult. Non-invertibility of $\mathcal{G}$ is usually inherited by the procedure $\mathcal{R}$.

Detection of false positives. A pirate, after a trial and error procedure, should find a key K^* that provides a positive answer and he can claim that K^* indicates his/her ownership. However such a key can be found approximately after $1/P_{fa}$ applications of $\mathcal{D}$, where P_{fa} is the minimum acceptable false alarm probability. Watermark detection with relatively significant P_{fa} becomes quite reliable when the provider registers his/her keys to a trusted authority. In such case, the probability that the counterfeit key K^* coincides with the pirate's registered key is extremely small.

Statistical watermark extraction [12]. The possession of a great number of digital images, all watermarked with the same key, should not dispose the watermark by applying statistical methods (e.g. averaging). Therefore, watermarks should not be statistically recoverable. An efficient solution to such an attack is to use watermarks that depend on the particular image. This requirement has been accounted for by introducing the procedure $\mathcal{T}$ during watermark generation.

Multiple Watermarking [13]. Multiple watermarking may be proved useful when product resellers should embed their own watermark. However, an attacker may use this property to embed his/her own watermark. Both watermarks (the original and the piratical) can be detected by using the corresponding unique key. Generally speaking, the watermark embedded at a later stage is detected with greater certainty. However, we can not conclude which watermark has been embedded first because the pirate may use a sufficiently "distorted" watermark that is detected with the minimal required certainty. We remark that the *original owner* of the image under question is the only one who can dispose a copy containing *only* his/her watermark and, subsequently, he/she can prove legal ownership in cases of conflict.

Watermarking by using arbitrary keys. Malevolent users or providers may apply watermarking to any accessible images by using arbitrary keys ("watermark bombing"). If these products are publicly exposed, a great confusion may arise when the automated watermark searching procedure is applied. The negative consequences of such an attack are restricted by the fact that we demand an enormous set of watermark keys. An efficient solution to eliminate such an attack is to consider restrictions for the keys that can be used by the providers; i.e. each watermarking software package should provide just one key for watermark casting.

Private key loss/theft. The loss of the private key may cause the watermark removal by a pirate, from all the images that belong to the particular owner. Thus, the system becomes dangerously unstable. A solution to this serious problem might be given by combining secure *time-stamping* [2] and *time-dependent* watermarks. In this way, such an attack is restricted on a small number of products.

5.2 Product registration

Product registration to a trusted authority is a well established way for protecting intellectual property rights of various products, e.g. books, software packages etc. Registration information can be used to form indisputable proofs for original ownership and legal rights. A protection system based on product registration requires the following actions before product disposition:

1. The provider is registered in a trusted authority, which provides him/her with a watermarking key (or a set of keys) or, generally, with a private watermark embedding software package.

2. Watermark casting is applied by using the registered key or the private software.

3. The original product is included in the provider's library $\mathcal{L}$ and the watermarked one is registered to a trusted authority.

4. The provider proceeds to an automated watermark searching through the network sites. When low certainty searching level is used, the reliability of a positive result is reinstated by searching the library $\mathcal{L}$.

5. The demonstration of the registered copy in a court of law is the proof for copyright ownership.

Therefore, by including registration schemes in the protection system, the watermark contribution is restricted to the discovery of products used illegally in the network. Afterwards, the registration authority, must provide the final and reliable proof about legal ownership.

6 Conclusions

In this article we studied the copyright protection of digital still images through invisible watermarking. Watermarking schemes serve for searching in the global network for illegal copies of digital products and for providing reliable indications or proofs for copyright ownership.

Watermarks are efficient for copyright protection when basic demands are satisfied. However, the demand of watermark robustness under digital image processing has not been satisfied completely yet. Robustness to geometrical distortions is an essential problem when the originals are not used in the detection procedure. Furthermore, optimizations to current processing algorithms or the development of new ones should be accounted; e.g. more optimized future compression techniques must not destroy watermarks embedded at any time before. A watermarking scheme should be resistant to intentional attacks. A pirate will try always to violate the protection system either by creating forged proofs of ownership or by trying to show that the capacity of the watermarking scheme to indicate legal ownership is undetermined. A global scheme, for protecting effectively digital products, may be based on third trust parties, product registration and other feasible services, provided by the World Wide Web. We believe that watermarking will contribute essentially for assembling such a protection system.

References

[1] B. M. Macq and J. J. Quisquater. Cryptology for digital TV broadcasting. *Proceeding of the IEEE*, 83:944–957, June 1995.

[2] D. R. Stinson. *Cryptography, Theory and Practice.* CRC Press, New York, 1995.

[3] T. ELGamal. A public key cryptosystem and signature scheme base on discrete logarithms. *IEEE transactions on Information Theory*, 31:469–472, 1985.

[4] A. Z. Tirkel R. G. Schyndel and C. F. Osborne. A digital watermark. In *Proceedings of ICIP'94*, volume II, pages 86–90, 1994.

[5] N. F. Johnson and S. Jacodia. Exploring steganography: Seeing the unseen. *IEEE Computer*, pages 26–34, February 1998.

[6] W. Bender, D. Gruhl, and N. Morimoto. Techniques for data hiding. In *Proceedings of SPIE*, volume 2420, page 40, 1995.

[7] E. Koch and J. Zhao. Towards robust and hidden image copyright labeling. In *Proceedings of 1995 IEEE Workshop on Nonlinear Signal and Image Processing*, pages 452–455, 1995.

[8] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12):1673–1687, 12 1997.

[9] D. Kundur and D. Hatzinakos. A robust digital image watermarking method using wavelet-based fusion. In *Proceedings of ICIP'97*, volume I, pages 544–547, 1997.

[10] A. Papoulis. *Probability & Statistics.* Prentice Hall, 1991.

[11] S. Craver, N. Memon, B-L. Yeo, and M. Yeung. Resolving rightful ownerships with invisible watermarking techniques : Limitations, attacks and implications. *to appear in IEEE Journal of Selected Areas in Communications*, 1998.

[12] N. Nikolaidis and I. Pitas. Robust image watermarking in the spatial domain. *Signal Processing, sp.issue on Copyright Protection and Access control*, to appear in 1998.

[13] I. Pitas and T.H. Kaskalis. Applying signatures on digital images. In *Proceedings of 1995 IEEE Workshop on Nonlinear Signal and Image Processing*, pages 460–463, 1995.

[14] G. Voyatzis and I. Pitas. Chaotic Watermarks for Embedding in the Spatial Digital image Domain. In *Proceedings of ICIP'98*, 1998.

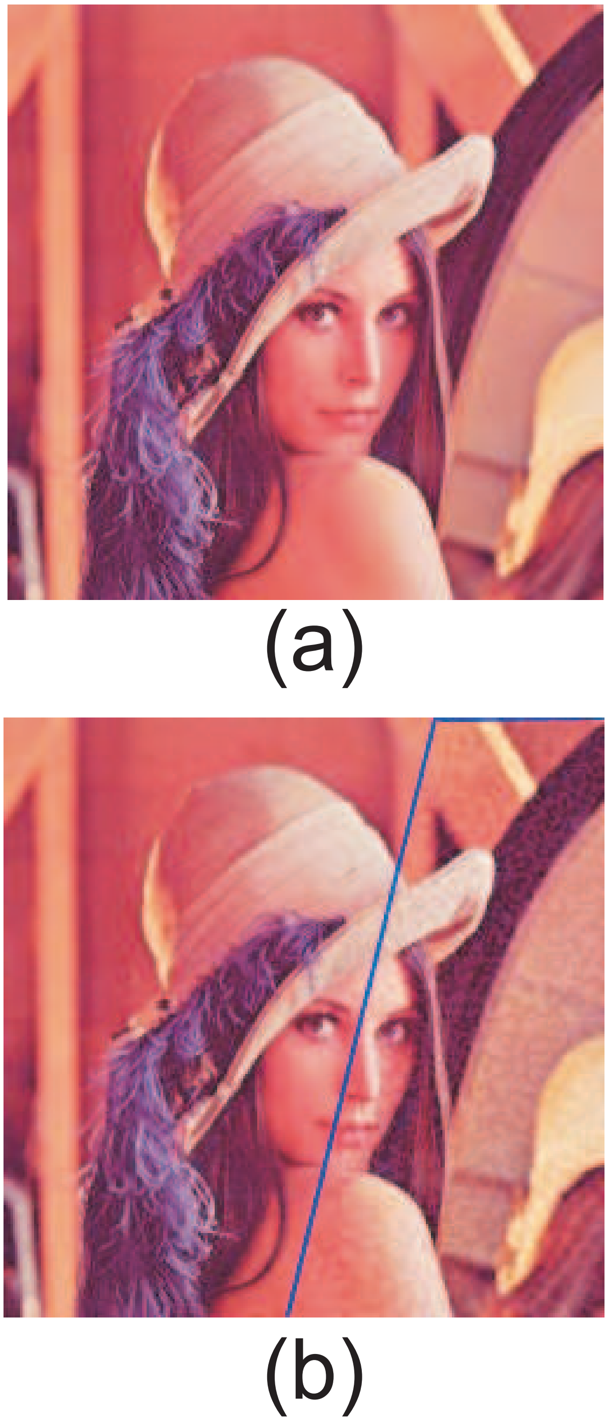

Figure 5: a) The original image Lenna b) Invisible watermarking of original Lenna by using $h = 2$ (left part) and watermarking that produces image degradation ($h = 8$ for the right part)

.

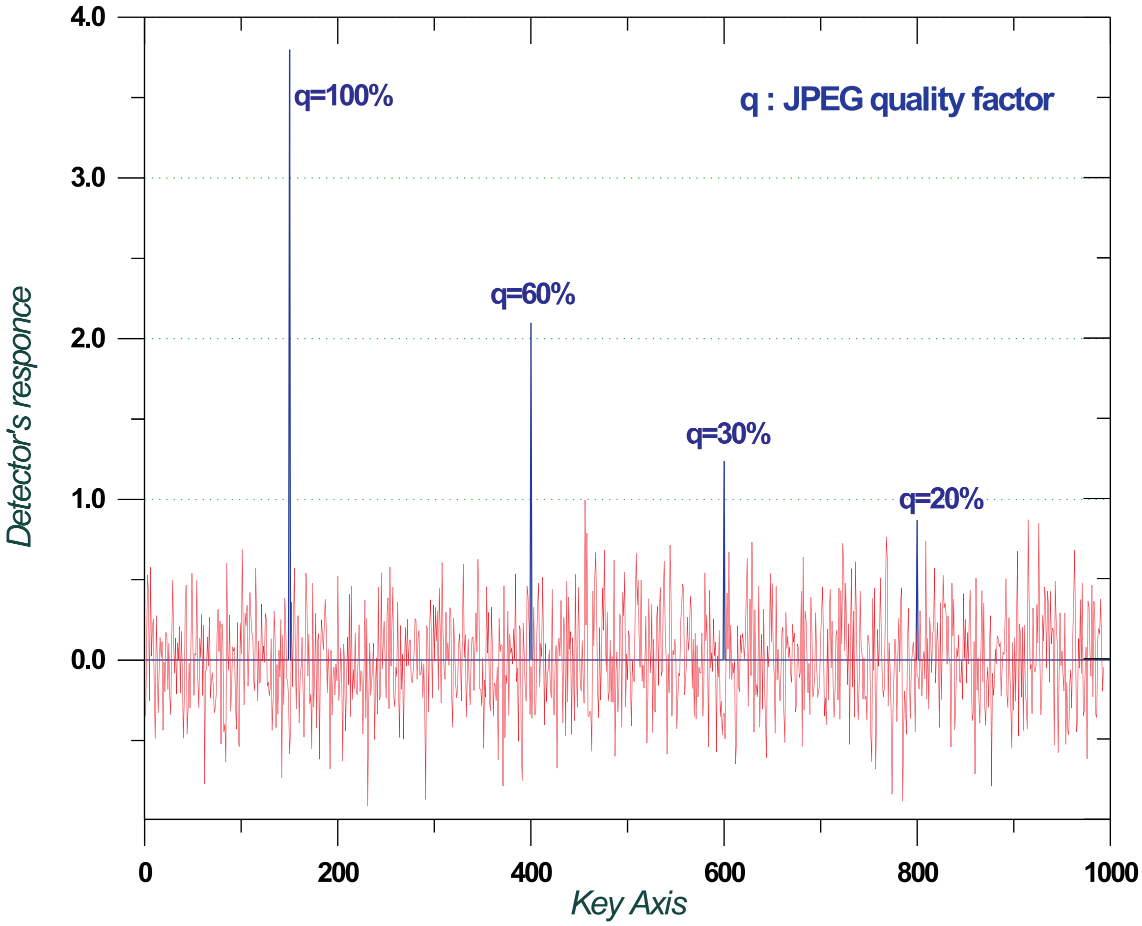

Figure 6: The responce of the detector (red peaks) for various not correct keys. The labeled peaks (blue ones) correspond to detection using the correct key. These peaks are easily distinguishable for the original watermarked Lenna and for high quality compressed versions of it