Chaotic Watermarks for Embedding in the Spatial Digital Image Domain

G. Voyatzis and I. Pitas
Department of Informatics, University of Thessaloniki
Thessaloniki 54006, Greece
e-mail: {voyatzis,pitas}@zeus.csd.auth.gr

Abstract

Binary (bi-valued) digital signals, which are suitable watermarks for digital images, are presented. They are generated by using chaotic dynamical systems that provide sufficient watermark complexity and controlled lowpass characteristics. Watermark detection is performed without resorting to the original image and its reliability is studied. Efficient robustness under lossy compression, lowpass filtering and other image processing can be achieved. Possible watermark detection after geometrical transformations is discussed.

1 Introduction

Transmission and exposure of digital products like digital images, video, audio and, extensively, multimedia applications, is quite insecure. Piracy that aims to violate the intellectual property rights is an easy task and effective solutions are intensively looked for. Imperceptible watermarking of the digital media, mentioned above, has been proposed as a particular solution to protect the copyright property of the legal owners or providers [1].

In this paper, we refer to the watermarking of digital images. Watermarks may be defined as two dimensional signals superimposed on the main data. Watermarking algorithms that are applied directly to the pixel intensity (or luminance) have been proposed [2]. Their watermarks are formed by binary (or bi-valued) signals which are superimposed on the digital data. Their advantage is their simplicity and the fast calculation. However, such watermarks are not robust to digital processing e.g. lossy compression. Robust watermarks may be produced by performing alterations to the DCT components of the middle-band of the image spread spectrum [3] or by constraining the DCT components in particular image blocks [4]. When geometrical modifications are performed (e.g. scaling and cropping), watermark detection becomes a very difficult problem if the original image is not accounted for.

In this paper, we present a form of bipolar ($\{-1,1\}$) signals used as image dependent watermarks for still images or video frames. Such watermarks show lowpass characteristics and, subsequently, are robust to lossy compression and low-pass filtering. The reliability of detection is studied by examining the possible false alarms. The watermark resistance to geometrical distortion is discussed.

2 Watermarking scheme and basic demands

A watermarking scheme consists of two components: a casting algorithm and a detection algorithm. The copyright owner casts a private watermark W into his/her product X. By using an automatic *search/detection* algorithm, the owner can monitor the digital products exposed publicly in the global digital network and check the existence of his/her personal watermark. Positive detection on a particular product indicates (strongly or weakly) copyright ownership.

Our watermarking scheme is defined as the *six-tuple* $(\mathbf{X}, \mathbf{W}, \mathbf{K}, \mathcal{G}, \mathcal{E}, \mathcal{D})$:

1. $\mathbf{X}$ denotes the set of grayscale digital images, to be protected, of any size $N \times M$. Color images can be presented in $\mathbf{X}$ if their luminance component is used for watermarking.

2. $\mathbf{W}$ is the set of the watermark signals:

$$W = \{w_{ij} \in \{-1,1\} \mid 0 \le i < N, 0 \le j < M\} \quad (1)$$

3. $\mathbf{K}$ is a sufficiently large set of ID numbers, e.g. integer parameters that called watermark keys.

4. $\mathcal{G}$ denotes the watermark generation algorithm defined as follows:

$$\mathcal{G} : \mathbf{X} \times \mathbf{K} \to \mathbf{W} \ , \ W = \mathcal{G}(X,K) \quad (2)$$

   where $K \in \mathbf{K}$ is the watermark key and $X \in \mathbf{X}$ is the image where the watermark will be embedded.

5. $\mathcal{E}$ is the embedding algorithm defined by general superposition and multiplication operators $(\oplus, \otimes)$ and an *embedding mask* $H = \{h_{ij} \in I\!R\}$:

$$\mathcal{E} : \mathbf{X} \times \mathbf{W} \times I\!R \to \mathbf{X} \quad , \quad x_w(i,j) \; = \; x_o(i,j) \oplus h_{ij} \otimes w_{ij} \tag{3}$$

where $X_o = \{x_o(i,j)\}$ denotes the original image and $X_w = \{x_w(i,j)\}$ is the watermarked one.

6. Finally, $\mathcal{D}$ denotes the detection algorithm defined as follows:

$$\mathcal{D} \; : \; \mathbf{X} \times \mathbf{K} \to \{0,1\} \tag{4}$$

$$\mathcal{D}(X,W) = \mathcal{D}(X, \mathcal{G}(X,K)) = \begin{cases} 1 & \text{if } W \text{ exists in } X \\ 0 & \text{otherwise} \end{cases}$$

We proceed also to the following definitions:

Perceptual similarity: if $X, Y \in \mathbf{X}$ then the notation $X \sim Y$ denotes that the digital products X and Y are perceptually similar. $X \not\sim Y$ denotes that Y shows quality reduction in respect to X.
Watermark similarity: $W_1 \simeq W_2$ (W_1 is similar to W_2) when:

$$\mathcal{D}(X, W_1) = 1 \; \Rightarrow \; \mathcal{D}(X, W_2) = 1$$

The operators $\sim$ and $\simeq$ are commutative.

The following watermark properties are necessary in order the above scheme to be effective for copyright protection:

1. *Perceptual invisibility*: $X_0 \sim X_w$. X_w should not show perceptual distortions, therefore, the values h_{ij} should be relatively small ($H < JND$).

2. *Key uniqueness*: $K_1 \neq K_2 \;\; \Rightarrow \;\; W_1 \not\simeq W_2 \;\; \forall X \in \mathbf{X}$ and $W_i \; = \; \mathcal{G}(X, K_i)$.

3. *Watermark validity*: $W \in \mathbf{W}$ is a valid watermark for a product $X \in \mathbf{X}$ if and only if $\exists K \in \mathbf{K}$ such that $\mathcal{G}(X,K) = W$.

4. *Non-invertibility.* $G_{X^*}(K) \; = \; \mathcal{G}(X^*, K)$ is not invertible. A sufficient condition is to consider $\mathcal{C}(\mathbf{W}) >> \mathcal{C}(\mathbf{K})$, where $\mathcal{C}(\mathbf{A})$ denotes the cardinality of the set $\mathbf{A}$.

5. *Image dependency*: For any particular key $K \in \mathbf{K}$ and for any $X_1, X_2 \in \mathbf{X}$:

$$X_1 \not\sim X_2 \; \Rightarrow \; W_1 \not\simeq W_2$$

where is $W_i \; = \; \mathcal{G}(X_i, K)$.

6. *Multiple watermarking* $X \; \in \; \mathbf{X} \quad \Rightarrow \quad X_w \; \in \; \mathbf{X}$. Thus watermarking of X_w is possible. If $X_{w_i} = \mathcal{E}(X_{w_{i-1}}, W_i), i = 1, 2, ...,$ then:

$$\mathcal{D}(X_{w_i}, W_1) = 1 \quad \forall \, i \leq n$$

where n is a sufficient number of coexisting watermarks such that if $X_{w_n} \sim X_0$ then $X_{w_{n+1}} \not\sim X_0$.

7. *Reliable detection* : If P_{fa} denotes the detection false alarm probability then

$$\mathcal{D}(X,W) = 1 \; \Rightarrow \; P_{fa} < P_{thres}$$

where P_{thres} is a sufficient threshold value for effective detection.

8. *Robustness.* When X_w is modified by some processing then the product X'_w results and for $X'_w \sim X_w (\sim X_o)$ the following condition should be satisfied :

$$\mathcal{D}(X_w, W) = 1 \; \Rightarrow \; \mathcal{D}(X'_w, W) = 1$$

The above scheme provides efficient security to various intentional attacks (see e.g. [8]) like generation of counterfeit watermarks, statistical watermark extraction, multiple ownership claims, taking advantage of false positives etc. [5].

3 Watermark generation

We consider an one-dimensional (1D) discrete map $\mathbf{F} : U \to U$, $U \subset I\!R$, which provides sequences of real numbers (trajectories) :

$$z(n+1) \; = \; \mathbf{F}(z(n), \lambda) \;\; , \;\; z(n) \in U, \; \lambda \in I\!R \tag{5}$$

where $n \; = \; 0, 1, 2, ...$ denotes map iterations and λ is a control parameter (or a set of parameters) for the system. For a particular value of λ, the finite space U consists of two subsets U_{reg} and U_{ch} so that if $z(0) \in U_{reg}$ the produced sequence is periodic or quasiperiodic (regular) and chaotic otherwise. In such systems, the trajectories, genericly, oscillate in a subdomain $[z_{min}, z_{max}] \subset U$ that depends on λ. For any λ we define a level $z^* \in [z_{min}, z_{max}]$ and a bipolar sequence $s(n) \in \{-1, 1\}$ is created by "thresholding" $z(n)$. Uniqueness and complexity of $s(n)$ are necessary conditions in order to proceed to the watermark formation. Therefore $s(n)$, or equivalently $z(n)$ should be chaotic sequences. Also we demand the parameter(s) λ to control the frequency of trajectory oscillations, and subsequently, the mean frequency of the -1,1 exchanges in $s(n)$. It is convenient to use strongly chaotic systems where the measure of U_{reg} in U is zero. We can use 1D maps on the circle [6] where λ is the Liapounov exponent of the trajectories. Thus, for $\lambda > 1$ chaos is obtained, almost everywhere. When λ is close to 1 the values change rarely in $s(n)$ and, subsequently, lowpass characteristics are obtained. For, the particular system used in this paper, about $\lambda > 2$, $s(n)$ is like a pseudorandom sequence (Fig. 1a). In any case we select a threshold value z^* such that, in a sufficient large sequence, the number of -1s and 1s to be approximately equal.

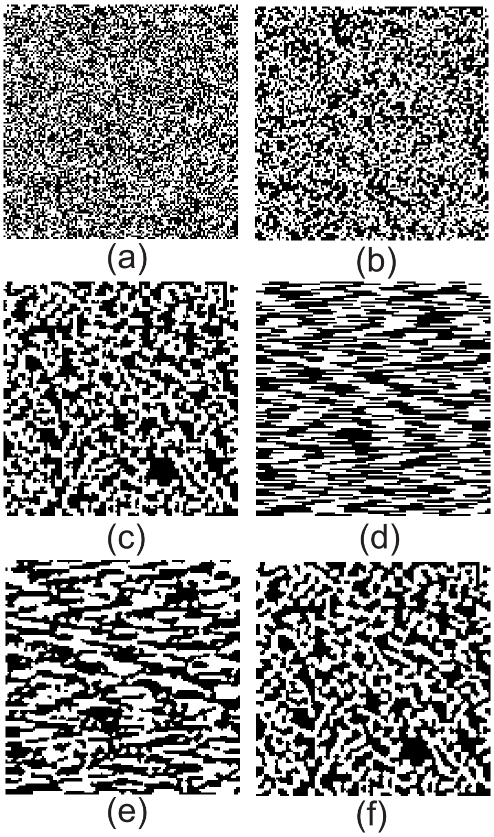

Figure 1: Watermarks presented in binary form (128×128) and created by the same key and by using a) $\lambda = 2.0$, b) $\lambda = 1.3$ and Peano scan, c) $\lambda = 1.1$ and Peano scan, d) $\lambda = 1.1$ and raster scan order, e) $\lambda = 1.1$ and cellular smoothing and f) $\lambda = 1.1$, Peano scan and cellular smoothing.

The two-dimensional (2D) watermark W, of size $N \times M$, is formed by considering a sequence $s(n)$ of size NM and a *scan order*. However, when e.g. raster scanning is applied, the 2D formed pattern shows "line segments" for $\lambda \approx 1$ and, thus, the lowpass characteristics of the 1D sequence $s(n)$ become highpass in a 2D representation (Fig. 1d). We propose the following ways to minimize the above feature:

- *Cellular smoothing.* The pattern, derived by using raster scanning, is smoothed by applying rules of cellular automata, e.g. by moving the 1-valued pixels to directions so that to have more neighborhoods with the same value.
- *Peano Scan.* Instead of using raster scan, Peano curves are applied to fill the 2D area of W (Fig. 1c). By using Peano scan, watermarking becomes very fast in respect of using cellular automata.

The key K, associated with the watermark W, is the initial condition $z(0)$ of the chaotic trajectory $z(n)$. Very small variations from the initial condition lead to uncorellated sequences $s(n)$ and subsequently to non-similar watermarks. A very large and countable key set $\mathbf{K}$ can be formed. We note also the non-invertibility of the watermark generation. By possessing a watermark W, the determination of the corresponding key is impossible.

Watermarks should be image dependent in order to avoid intentional extraction (and removal) of a watermark by using statistical methods. However, the image adaptive watermark should preserve its lowpass characteristics formed before. Let X_0 be the original image and W_0 be the original watermark produced by using the key K. We consider a boolean condition $\mathcal{F}$ based on local and robust features of the image X_0 and on a parameter k associated with the watermark key K. Then $W = \{w(i,j)\}$ is derived from W_0 as follows:

$$w(i,j) \;=\; \begin{cases} -w_0(i,j) & \text{if } \mathcal{F}(X_0,i,j,k)\text{=true} \\ w_0(i,j) & \text{otherwise} \end{cases} \qquad (6)$$

In order to preserve lowpass characteristics, $\mathcal{F}$ should change smoothly by the pixel position (i,j). If X'_w is a modified version of the watermarked image X_w, then watermark robustness demands a sufficient approximation of the relation:

$$\mathcal{F}(X_0,i,j,k) = \mathcal{F}(X_w,i,j,k) = \mathcal{F}(X'_w,i,j,k)$$

Figure 2 shows such image dependent watermarks derived from the watermark of Fig. 1c.

Generally, the watermark generation procedure $\mathcal{G}$ can be decomposed in two procedures:

$$\mathcal{G} = \mathcal{T} \circ \mathcal{R} \;,\; \mathcal{R} : \mathbf{K} \to \mathbf{W} \;,\; \mathcal{T} : \mathbf{W} \times \mathbf{X} \to \mathbf{W} \quad (7)$$

$\mathcal{R}$ may be based on a pseudo-random number generator or, generally, on chaotic systems having parameters (initialization seed) the input key K. $\mathcal{T}$ modifies the signal $W_0 = \mathcal{R}(K)$ to obtain the final watermark that depends on the particular image. Therefore, watermarking non-invertibility and watermark image dependency are inherited from $\mathcal{R}$ and $\mathcal{T}$ respectively.

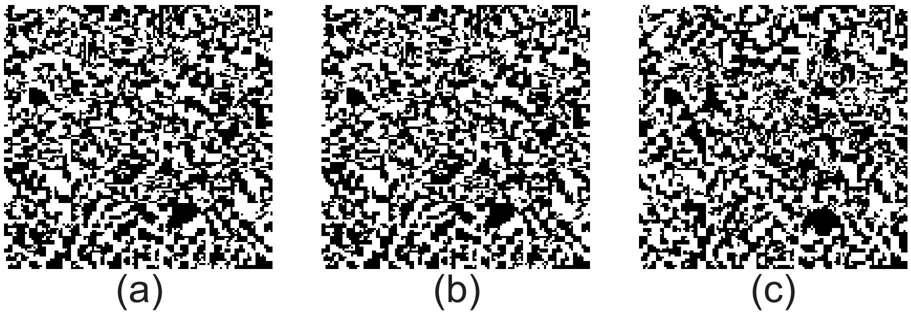

Figure 2: Image dependent watermarks (128×128). The watermark of Fig. 1c is transformed by a) the original "Lenna", b) "Lenna" of JPEG quality 30% and c) the "Baboon" image.

4 Embedding and Detection Algorithms

Both applications for watermark embedding and detection require the watermark generation formerly.

Watermark Embedding

Let X_0 be an original grayscale or color image of size $N \times M$ and $x(i,j)$ denote the intensity or the luminance of the pixels (i,j). The watermarked image X_w, having the same size as the original, is formed by applying (3). The simplest case is to assume a constant embedding mask ($h_{ij} = h = const$) and as $\oplus$ the usual addition operator and accounting appropriate truncations:

$$x_w(i,j) \; = \; x(i,j) \; + \; h\,w(i,j) \qquad (8)$$

The constant h should be small in order to guarantee the invisibility of the watermark in X_w.

Watermark detection

Let $X \in \mathbf{X}$ be an image of size $N \times M$. The watermark W is generated by using the specific key and the image X. The image pixels are divided in two subsets $\mathbf{A} = \{(i,j)|w_{ij} = 1\}$ and $\mathbf{B} = \{(i,j)|w_{ij} = -1\}$ having N_A and N_B elements respectively. We consider the following detection response:

$$R(I,W) = \frac{1}{N_A} \sum_{(i,j)\in\mathbf{A}} x(i,j) - \frac{1}{N_B} \sum_{(i,j)\in\mathbf{B}} x(i,j) \quad (9)$$

We assume that x and w are statistically independent random variables. Thus, R should follow the normal distribution $N(\bar{R}, \sigma)$, where $\bar{R} = 2\,h$, when W exists in X and $\bar{R} = 0$ otherwise.

5 Robustness issues and Numerical experiments

When a watermarking image X_w is modified somehow (e.g. by lossy compression or filtering), we expect $R < 2\,h$. Therefore a threshold value R_{thres} should be set such that watermark existence is assumed when $R > R_{thres}$. A positive detection is associated with a false alarm probability P_{fa}.

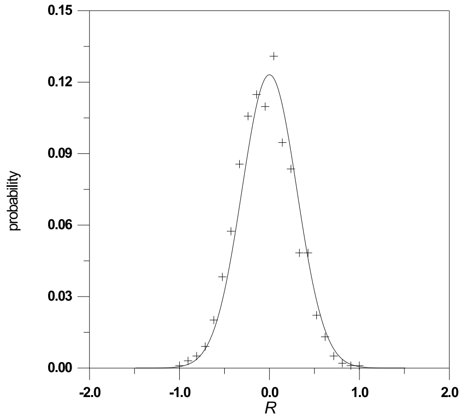

Figure 3: The $p.d.f$ of R calculated on original "Lenna" by using 1000 watermarks.

The watermarking algorithm has been tested on the gray-scale "Lenna" of size 512×512. The watermarks have been produced by using $\lambda = 1.2$. The embedding level was $h = 2$. Fig. 3 shows the probability distribution of R calculated from 1000 applications of the correlator to non-watermarked image "Lenna" and for watermarks created by choosing different keys. A threshold value $R_{thres} \approx 1.0$ provides detection certainty up to 99.9%. Fig. 4 presents the correlator's output R for the watermarked "Lenna" compressed with various JPEG quality factors. We can observe that $R > R_{thres}$ even for compression levels where extensive image degradation is produced.

Lowpass watermark characteristics, generally, leads to a loss of reliability [10]. The choice of higher threshold level R_{thres} is required, when W become more lowpass, in order to preserve high detection certainty. Fig. 5 presents the function R_{thres} as a function of

λ, which should be accounted for in order to detect watermarks with at least 99.9% certainty. However, on the other hand, lowpass watermarks are more robust to compression and other processing. Therefore, a control parameter $\lambda^*(X)$ may be defined for providing optimal detection performance.

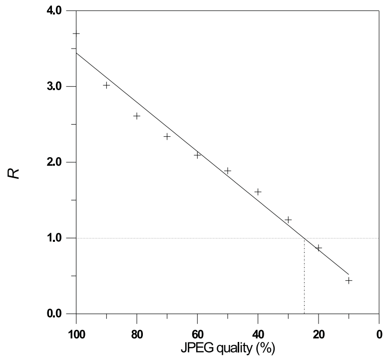

Figure 4: The response R after applying detection on JPEG versions of the watermarked "Lenna" and by using the correct key.

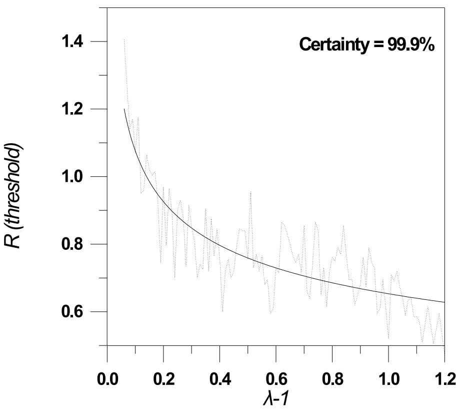

Figure 5: The R_{thres}, for minimum detection certainty 99.9%, as a function of the control parameter λ.

Most of the watermarks are not robust to possible image geometrical distortions. Some watermarks may resist to some elementary modifications [9], however is not known a "fully" efficient watermarking algorithm yet. A watermark of size $N \times M$ can be embedded into an image of size $N' \times M'$ by performing watermark scaling to the image size. By using watermarks of specific size, the correlator R is applied to a watermarked image of any size by performing image scaling to the watermark size. When cropping takes place, the correlator $R(k,l)$ should be calculated for all necessary shift (k,l). The maximum value of $R(k,l)$ should determine the position of the cropped image in the original one. Statistical detection reliability should be guaranteed before for each one of the above mentioned cases. Serious problems arise when both scaling and cropping took place. By watermarking internal robust segments in the image, an efficient solution to this problem is possible.

References

[1] A.Z. Tirkel, R.G. Schyndel and C.F. Osborne, "A digital Watermark", in *Proceedings of ICIP'94*, vol II, pp 86-90, 1994.

[2] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for data hiding", *IBM Systems Journal*, vol. 25, pp 313-335, 1996.

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

[4] E. Koch and J.Zhao, "Towards Robust and Hidden Image Copyright Labeling", *Proceedings IEEE workshop on Nonlinear Signal and Image processing*, Vol I, pp 452-455, 1995.

[5] G. Voyatzis, N.Nikolaidis and I.Pitas, "Digital Watermarking: An Overview", *Proceedings of EUSIPCO'98*, to appear, 1998.

[6] Devaney R.L. *An introduction to dynamical systems*, Penjamine/Cummings, Publ. 1986.

[7] Piva A., Barni M, Bartollini F and Cappellini V, "DCT-based Watermark Recovering without resorting to the uncorrupted original image", *Proceedings of ICIP'97*, vol I, pp 520-523, 1997.

[8] Zeng W and B.Liu, "On Resolving rightful ownerships of digital images by invisible watermarks", *Proceedings of ICIP'97*, vol I, pp 552-555, 1997.

[9] J.K. Ruanaidh and T. Pun, "Rotation, Scale and Translation Invariant Digital image watermarking", *Proceedings of ICIP'97*, vol I, pp 536-539, 1997.

[10] T, Kalker, J-P. Linnartz and G. Depovere, "On the reliability of detecting electronic watermarks in digital images", *Proceedings of EUSIPCO'98*, to appear, 1998.