APPLICATIONS OF TORAL AUTOMORPHISMS IN IMAGE WATERMARKING

G.Voyatzis and I. Pitas

Department of Informatics
University of Thessaloniki
Thessaloniki 54006, Greece
E-mail: pitas@zeus.csd.auth.gr

ABSTRACT

Digital watermarking methods have been recently proposed for various purposes and especially for copyright protection of multimedia data. The digital watermark is embedded in a digital signal or an image and must be unrecognizable by unauthorized persons and detectable only by the legal copyright owner. In this paper we use toral automorphisms as chaotic 2-D integer vector generators in order to manipulate digital image watermarking. We propose also an embedding algorithm which provides robustness under filtering and compression.

1. INTRODUCTION

The embedding of an additional information in multimedia products can be met with several applications (tamper proofing, embedded captions, e.t.c.)[1]. Nowadays a very important application of the embedded information is to mark the ownership of the associated multimedia data [2].

A digital watermark (sometimes called digital signature) is a digital signal carrying out information about the copyright owner (e.g. an author's signature or a company logo) which is hidden in multimedia data in such a way that i) it is perceptually invisible ii) its existence can be detected only by an authorized person and iii) it is impossible to be removed without significant distortion of the total amount of data. The application of a watermark in digital images is a difficult problem since many filters for image processing have been developed in order to remove information which does not affect the visual perception of the image (e.g. compression keeping high quality) or to modify an image for various purposes. Another difficulty arises from the fact that a digital image provides a relatively short signal, where the additional information has to be included, and very slight modifications are permitted in order to avoid visually perceptible alterations.

The watermarking methods that have been proposed are classified in two main categories:

(a) Embedding in the frequency domain. A small subset of the frequency spectrum of particular blocks is modified. This subset belongs to the medium range of the spectrum so that to combine perceptual invisibility and robustness to JPEG compression and other image processing [1,3,4].

(b) Embedding in the spatial domain. A pseudorandom set of pixels is selected and the least significant bits of their intensity levels are modified in such way that to form a statistical property which describes only a specific set of pixels (the watermark). This method is very fast and reliable [2,5]. A robust version of this method under filtering, cropping and compression algorithms is represented in [6].

In this paper we propose a spatial embedding of a watermark which is assumed to be a bitmap logo i.e. an image which consists of a small number of pixels which are described by 0's and 1's. Our watermarking method is described in section 3 and is based on a family of chaotic tranformations which are called toral automorphisms. Some of their properties are discussed in the next section.

2. TWO-DIMENSIONAL TORAL AUTOMORPHISMS

A two-dimensional "torus automorphism" can be considered as a spatial transformation of planar regions which belong in a square two- dimensional area. It is defined in the subset $U = [0,1) \times [0,1) \subset R^2$ by the following formula [7]:

$$\mathbf{r}' = \mathbf{A}\,\mathbf{r}\,,\ \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a_{11}\ a_{12} \\ a_{21}\ a_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}\ (mod\,1) \quad (1)$$

where $a_{ij} \in Z$, $det\mathbf{A} = 1$ and $\lambda_{1,2} \in R - \{-1, 0, 1\}$ are the eigenvalues of $\mathbf{A}$. Iterated actions of $\mathbf{A}$ on a point

$\mathbf{r}_0$ form a dynamical system which can be expressed like a map

$$\mathbf{r}_{n+1} = \mathbf{A}^n \mathbf{r}_0 \ (mod\ 1) \quad or \quad \mathbf{r}_{n+1} = \mathbf{A}\mathbf{r}_n \ (mod\ 1) \quad (2)$$

where $n = 0, 1, 2, ...$ The set of points $\{\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, ...\}$ is an orbit of the system. It can be shown that $\mathbf{r}_i \in U, \forall i$ and for every $\mathbf{r}_0 \in U$ i.e. U remains invariant under the automorphism.

We consider the action of the system (2) on a subset $V_0 \subset U$. Then V_0 is transformed to a subset $V_1 \subset U$ which occupies the same area like V_0 since $det\mathbf{A} = 1$. n iterated transformations produce a subset V_n which is characterized as strongly chaotic. System (2) distorts any area element, that spreads over the entire available area. The subset V_n does not show significant correlations with its initial state V_0. Roughly speaking, this property is called "mixing". A famous automorphism in dynamics is the "cat map" ($a_{11} = 1, a_{12} = 1, a_{21} = 1, a_{22} = 2$).

Although the automorphisms are strongly chaotic they possess a dense set of periodic orbits which correspond to the points with rational coordinates. For any point $\mathbf{r}_o = (p_1/q_1, p_2/q_2) \subset U$ with $p_i, q_i \in Z^+$ coprimes, there exists a "period" T, which depends on $\mathbf{r}_o$ such that $\mathbf{A}^T \mathbf{r}_o = \mathbf{r}_o \ (mod\ 1)$. We consider the discrete subset W of U which is defined as

$$W = \{(x, y) | x = k/N, y = l/N, k, l \in \{0, 1, .., N-1\}\ \}$$

where N is the least common multiple of q_1, q_2. $\mathbf{r}_0$ belongs to W which remains invariant under the action of an automorphism, i.e. all the points of an orbit belong to W. Thus, the evolution of the orbits in W under the automorphism (1) is equivalent to the evolution of orbits in an integer lattice $L = \{(k, l), 0 \leq k, l < N\}$ under an automorphism where the periodic condition $(mod\ 1)$ is replaced by $(mod\ N)$.

All the periodic orbits are unstable and their points are distributed irregulary in L. Thus the automorphisms can be directly applied on the space of a digital image in order to produce a chaotic mixing. We mention also that the dynamics of the chaotic orbits can be described exactly without numerical errors, because computations are performed by using integer arithmetic.

The evolution of the orbits in L depends exclusively on the one of the eigenvalues (say λ_1) of the automorphism, since $\lambda_2 = 1/\lambda_1$, and it is described by the congruent [8] :

$$\xi' \equiv \lambda_1 \xi \ (mod\ N) \quad (3)$$

where ξ', ξ are quadratic integers which correspond to integer vectors $(k, l) \in L$. Since λ_1 is a function of $t = tr(A) = a_{11} + a_{22}$, we obtain a one-parameter family of toral automorphisms $\mathcal{T}$. A great subset of $\mathcal{T}$ is represented by the family of one-parameter systems $A_N(k) : L \rightarrow L$ which is defined as follows :

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \ (mod\ N) \quad (4)$$

where $(x_n, y_n) \in L = [0, N-1] \times [0, N-1]$. For the $N-1$ integer values of k in the domain $[1, N)$ we obtain a finite family of systems $A_N(k)$. The greatest eigenvalue is $\lambda_1 = 1 + 0.5(k + (k^2 + 2k)^{1/2})$ and is real for every $k > 0$.

An extended study of the periodic orbits of automorphisms can be found in [8,9]. All the orbits of system (4) are unstable periodic orbits with periods T which depend on k,N and the initial point of the orbit. We state the following corollary :
For any integer lattice L of size N there is an integer $P = P(k, N)$ such that

$$A_N^P(k)\mathbf{r} = \mathbf{r}\ (mod N)\ , \ \forall \mathbf{r} \in L \quad (5)$$

We call the integer P *recurrence time*. Thus, any lattice point is a fixed point under the action of $A_N^P(k)$. The behaviour of the function $P = P(N, k)$ is quite irregular and this is caused by the complication of the integer arithmetic rather than by the chaotic properties of the automorphism. An orbit itself usually displays an unstable behaviour and a chaotic distribution in the lattice.

3. EMBEDDING AND RECONSTRUCTING A WATERMARK

A digital image can be understood as a rectangular mesh of size $M_1 \times M_2$. Each point of the mesh (a pixel) is characterized by its grey level or by the three intensity levels of red, green and blue colour. Next we consider a grey level image which is represented as :

$$I = \{x_{ij}, (i, j) \in L, x_{ij} \in \{0, 1, .., G-1\}\} \quad (6)$$

where L is an $M_1 \times M_2$ lattice of grid size 1 and G is the total number of intensity levels.

3.1. Embedding

In image (6) we want to embed a watermark which is a bitmap image of the form:

$$S = \{y_{ij}, (i, j) \in L_s, y_{ij} \in \{0, 1\}\} \quad (7)$$

where L_s is an $S_1 \times S_2$ lattice of grid size 1 such that $S_1 \ll M_1$ and $S_2 \ll M_2$. The watermark S is located in

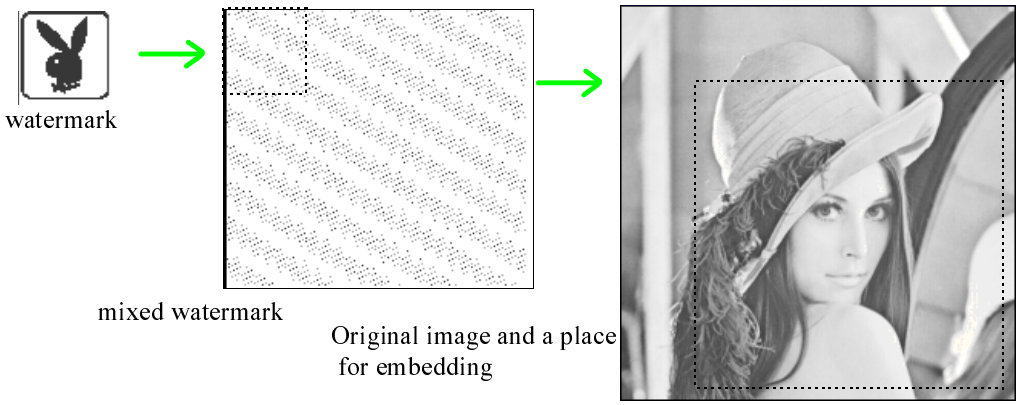

Figure 1: Embedding of the logo "rabbit" in "Lena" (original image)

an empty box $\mathcal{B}$ of size $N \times N$ where $N \leq min(M_1, M_2)$. The automorphism $A_N(k)$ is applied n times by choosing a parameter k. The result is a mixed watermark S' with a chaotic reallocation of pixels without effect on their bitmap intensity.

Let I' be an $N \times N$ subset of I which is determined by its size N and its position in I, say e.g. the upper-left corner (p_1, p_2). We correspond the pixels of $\mathcal{B}$ to the pixels of I' by a 1-1 map μ

$$\mathcal{B} \ni \mathbf{r} = (i,j) \overset{A_N^n(k)}{\longleftrightarrow} (k,l) \overset{\mu}{\longleftrightarrow} \mathbf{r}' = (k+p_1, l+p_2)$$

or symbolically

$$\mathbf{r}' = f(\mathbf{r}) \tag{8}$$

Now we embed the watermark S by altering the intensity levels of the pixels of image I and we get the signed image

$$I_s = \{x'_{\mathbf{r}'}, \mathbf{r}' \in L, x'_{\mathbf{r}'} \in \{0,1,..,G-1\}\} \tag{9}$$

where

$$\begin{aligned} x'_{\mathbf{r}'} &= g(x_{\mathbf{r}'}) \text{ if } \mathbf{r} = f^{-1}(\mathbf{r}') \in L_s \\ x'_{\mathbf{r}'} &= x_{\mathbf{r}'} \text{ if } \mathbf{r} = f^{-1}(\mathbf{r}') \notin L_s \end{aligned}$$

The "embedding" function g is selected in such a way that to be able to determine a "detection" function D with the following output :

$$\begin{aligned} D(x'_{\mathbf{r}'}) &= 1 \text{ if } \mathbf{r} = f^{-1}(\mathbf{r}') \in L_s \text{ and } y_{\mathbf{r}} = 1 \\ D(x'_{\mathbf{r}'}) &= 0 \text{ if } \mathbf{r} = f^{-1}(\mathbf{r}') \in L_s \text{ and } y_{\mathbf{r}} = 0 \\ D(x'_{\mathbf{r}'}) &= 0 \text{ or } 1 \text{ if } \mathbf{r} = f^{-1}(\mathbf{r}') \notin L_s \end{aligned}$$

Several superposition techniques can be applied by choosing appropriate functions g and D. Also they may depent on the pixels arround the signed pixel $x'_{\mathbf{r}'}$ so that the method to be robust.

Watermark embedding is described by the the size N of $\mathcal{B}$, the position (p_1, p_2) of I' in I, the parameter k of the automorphism and the number of iterations n for mixing. An examble of the embedding procedure is given in Figure 1. The watermark "rabbit" is spread chaotically by the automorphism $A_{186}^{30}(15)$ in a 186×186 area (the $\mathcal{B}$) and is embedded in 256×256 "Lena" at the position (65,65).

3.2. Watermark detection

For a given I_s, the watermark detection demands the knowledge of the numbers N, p_1, p_2, k and n (the key). We extract the subset I' from I_s which is determined by p_1, p_2 and N. For every pixel $\mathbf{r}'$ in I' we calculate the corresponding average $A_{\mathbf{r}'}$ and we form the following $N \times N$ bitmap set :

$$U = \{z_{\mathbf{r}'}, \mathbf{r}' \in \mathcal{B}, z_{\mathbf{r}'} \in \{0,1\}\} \tag{10}$$

where

$$z_{\mathbf{r}'} = D(x'_{\mathbf{r}'})$$

U contains the mixed watermark S'. By applying the automorphism $A_N(k)$ $P-n$ times on U (i.e. $A_N^{P-n}(k)$), where P is the recurrence time, the pixels which belong to S' are reallocated and they form the initial watermark S. The rest of the pixels in U show a "random" distribution. In Figure 2 the reconstruction of the watermark is illustrated. Figure 2a presents the watermarked image of "Lena". The set U is shown in Figure 2b. By applying the automorphism $A_{186}(15)$ 18 times (the recurrence time for $k = 15$ and $N = 186$ is 48) the watermark is reconstructed (Figure 2c).

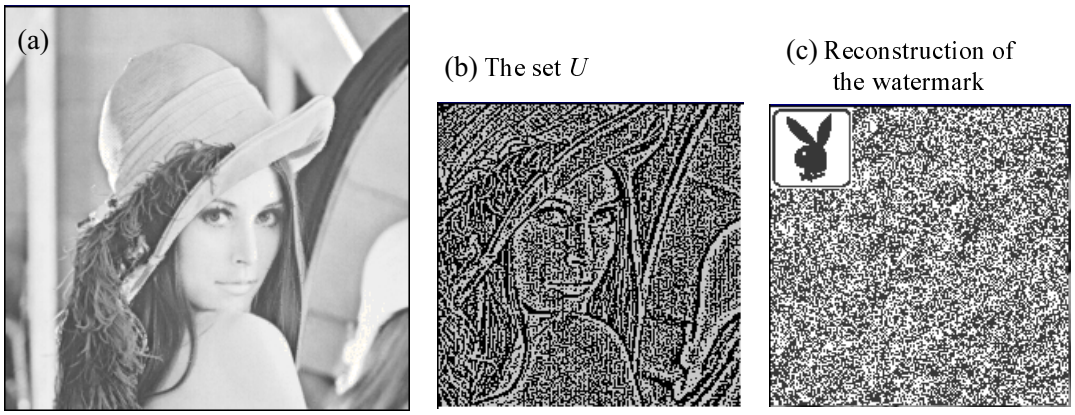

Figure 2: The reconstruction of the logo "rabbit" from "Lena" (watermarked image)

4. CONCLUSIONS

In this paper we introduce a chaotic transformation of images which is based on the mixing property of toral automorphisms and we proposed a method for embedding a watermark in a digital image. The watermark is mixed by the chaotic system (4) and is embedded in an image such that its visual perception remains the same. The watermark detection from the signed image is done by applying the same system and by using a specific set of parameters which characterizes the watermark embedding. A more complex mixing, possessing more independent parameters, can arise if we use different automorphisms on sublattices having different sizes.

The embedding procedure, which has been used to place the watermark "rabbit" in "Lena", takes into account the average value of the intensity levels of the pixels which belong in a neigbourhood of a pixel which is altered. This average is quite a robust under noise, filtering and compression. Numerical experiments show that the reconstructed watermark is recognized visibly if the watermarked image is affected by JPEG compression up to 6:1. By using signal detection methods we can get a reliable answer about the existence or not of a watermark even if the watermaked image has been affected quite strongly by filtering and JPEG compression greater than 10:1.

5. REFERENCES

[1] I.J.Cox, J.Kilian, T.Leighton and T.Shammoon "Secure Spread spectrum Watermarking for Multimedia", *Tech. Report*, NEC research Institute, 95-10, p.1.

[2] I. Pitas and T. Kaskalis, "Applying Signatures on Digital Images",*proc. IEEE Workshop on Nonlinear Signal and Image processing*, I.Pitas (ed) , Vol I, p.460, 1995.

[3] A.G.Bors and I.Pitas "Embedding parametric digital signatures in images" *proc. of EUSIPCO'94*, Trieste, Italy 10-13 Sep 1996 (accepted).

[4] E. Koch and J.Zhao, "Towards Robust and Hidden Image Copyright Labeling" *proc. IEEE workshop on Nonlinear Signal and Image processing*, I.Pitas (ed) , Vol I, p.452, 1995.

[5] O. Bruyndonckx, J-J.Quisquater and B. Macq "Spatial Method for Copyright Labeling of Digital Images" *proc. IEEE workshop on Nonlinear Signal and Image processing*, I.Pitas (ed) , Vol I, p.456, 1995.

[6] N.Nikolaidis and I.Pitas "Copyright protection of images using robust digital signatures" *proc. of ICASSP-96*, Atlanta, USA, May 1996 (accepted).

[7] D.K. Arrowsmith and C.M.Place, "An Introduction to Dynamical systems", Cambridge Univ. Press 1990.

[8] I. Percival and F.Vivaldi, "Arithmetical properties of strongly chaotic systems", *Physica 25D*, p.105-130, 1987.

[9] F.Vivaldi, "Geometry of linear maps over finite fields", *Nonlinearity 5*, p.133-147, 1992.