CHAOTIC MIXING OF DIGITAL IMAGES AND APPLICATIONS TO WATERMARKING

G.Voyatzis and I.Pitas

Department of Informatics
University of Thessaloniki
54006 Thessaloniki
GREECE
fax: +3031-996304, email: voyatzis@zeus.csd.auth.gr

ABSTRACT

This paper presents a method for embedding watermarks (some call them signatures) in digital pictures. The signatures are considered to be digital images with few grey levels, which are embedded in digital grey or color pictures. The extraction of the watermark, by an unauthorized person, is impossible since a chaotic mixing of the code takes place. Our study is based on the theory of toral automorphisms which may be proved to be a useful tool in digital copyright protection.

1. INTRODUCTION

Nowadays, the use of multimedia services over computer networks is rapidly increasing. But, also, the problems associated with enforcing copyright protection on these services become more and more significant. The use of watermarks (or digital signatures) has been proposed as a particular, but efficient solution to the above mentioned problem [1-3]. A digital watermark is a code which is embedded into digital data for copyright protection.If the data represent an image, then the visual perception of the image must remain unaltered after embedding. The watermark completely characterizes the owner and proves the ownership of the image.

There are some requirements which must be satisfied by a watermarking algorithm such as visual and statistical invisibility and resistance to compression. It is desirable that the algorithm is described by a standard procedure employing a set of parameters which is the key for embedding and detection of the watermark. Generally speaking, the algorithm consists of two independent procedures :

1. Selection of the secret code being embedded into an image.
2. Embedding by a superposition law which alters the intensity levels of some pixels of the image.

The watermark embedding takes place at the first procedure, by a suitable chosen encryption of the original code, and/or at the second procedure, by the use of a nonlinear superposition law.

In this paper we use as a watermark an $N \times N$ image S embedded in an original $M_1 \times M_2$ image I to be protected. We propose a spatial transformation of S such that only the knowledge of a specific set of numbers can lead to the extraction of S from I. We use *toral automorphisms* which are strongly chaotic (mixing) systems [4,5]. We consider a digital image as a set of pixels which form a two dimensional integer lattice. Toral automorphisms are characterised by special properties when they act on such lattices. In section 2 we point some main definitions from the theory of toral automorphisms, we state the "recurrence" property and we suggest a simple system which produces chaotic spatial transformations of images. In section 3 we describe a watermarking algorithm.

2. TORUS AUTOMORPHISMS ON INTEGER LATTICES

A two-dimensional "torus automorphism" can be considered like a spatial transformation of planar regions which belong in a square two- dimensional area. The heart of the transformation is a 2×2 matrix with constant elements. The term torus automorphism, usually, refers to this matrix. Let $U = [0,1) \times [0,1) \subset R^2$ is the domain where an automorphism is applied and $\mathbf{r}= (x, y)$ a point on U.The action of the automorphism on $\mathbf{r}$ gives the $\mathbf{r}' = (x', y')$ by the following formula [4,5]:

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

where (i) $a_{ij} \in Z$, (ii) $det\mathbf{A} = 1$ and (iii) $\mathbf{A}$ has eigenvalues $\lambda_{1,2} \in R - \{-1, 0, 1\}$.

The conditions (i) and (ii) ensure the existence of the inverse automorphism which is represented by the matrix $\mathbf{A}^{-1}$. The condition (iii) stands for "hyperbolicity" which is a neccesary property for a *chaotic* behaviour. By using (ii), the relation $\lambda_1 = 1/\lambda_2$ is proved. Iterated actions of $\mathbf{A}$ on a point $\mathbf{r}_0$ form a dynamical system which can be expressed like a map

$$\mathbf{r}_{n+1} = \mathbf{A}^n \mathbf{r}_0 \ \ (mod\ 1) \quad or \quad \mathbf{r}_{n+1} = \mathbf{A}\mathbf{r}_n \ \ (mod\ 1)\ , \ \ n = 0, 1, 2, ... \tag{2}$$

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 $det\mathbf{A} = 1$. The transormation of V_0 is characterized by the two directions which corespond to the directions of the eigenvectors $\mathbf{u}(\lambda_1)$, and $\mathbf{u}(\lambda_2)$ of $\mathbf{A}$. Suppose that $\lambda_1 > 1$, then $\lambda_2 = 1/\lambda_1 < 1$ and the V_0 is stretched to the direction of $\mathbf{u}(\lambda_1)$ and is shrinked to the direction of $\mathbf{u}(\lambda_2)$. Those directions exist at every point of U and they form a "hyperbolic set". As a consequence of such hyperbolicity is the chaotic evolution of the orbits and the spreading of small subsets of U in all the space of U. Roughly speaking, this property is called "mixing". A famous automorphism in dynamics is the "cat map" which is

Figure 1: Chaotic mixing of the "cat" by system (3).

defined as [5]

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \quad (mod\ 1) \tag{3}$$

In figure 1, the action of system (3) on the "cat" (figure 1a) is represented. At the first iteration (figure 2b) we observe the directions of shrinking (**e1**) and stretching (**e2**). The points of the "cat", which tend to leave the square, are repositioned due to the modulo operation. After some iterations the "cat" spreads in all the region of the square (figure 1c) and we get a "mixed cat".

The set of torus automorphisms is a special subset of Anosov diffeomorphisms which exhibit strongly chaotic motion i.e. local instability, ergodicity and mixing and decay of correlations. Every Anosov diffeomorphism is structurally stable and it is topological conjugate to some torus automorphism [4,5]. The orbits $\mathcal{O} = \{\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, ...\}$ of all automorphisms are classified in two main categories according to their initial point $\mathbf{r}_0 = (x_0, y_0)$:

a) x_0 and/or y_0 are irrational. The orbit $\mathcal{O}$ visits any neighbourhood of every point of U as $n \to \infty$ (ergodicity) and the set $\mathcal{O}$ is infinite and dense in U.

b) x_0 and y_0 are rational. In this case $\exists n \neq 0$ such that $\mathbf{r}_n = \mathbf{r}_0$. The orbit is periodic and the set $\mathcal{O}$ is finite. The number of the elements of $\mathcal{O}$ is the period of the orbit.

Let $\mathbf{r}_0 = (p_1/q_1, p_2/q_2)$ be a point of U with $p_i, q_i \in Z^+$ coprimes and N the least common multiple of q_1, q_2. We consider the descrete subset W of U which is defined as

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

$\mathbf{r}_0$ 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 equivelant 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 $(mod\ N)$.

The evolution of the orbits in L depends exclusively on the one of the eigenvalues (say λ_1) of the automorphism and it is described by the congruent [6]

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

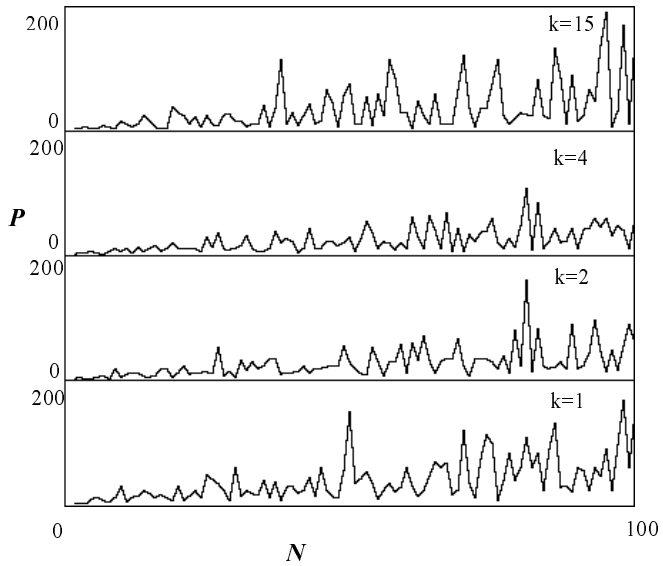

Figure 2: Recurrence time P versus the size N of the lattice for the system (4) and for some parameters k.

where ξ', ξ are quadratic integers which corespond 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 which is defined as follows :

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

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 [6-9]. All the orbits of system (4) are unstable periodic orbits with periods T which depend on the parameters k and N and the initial point of the orbit. We can state the following corollary :

For any integer lattice L of size N there is an integer $P = P(k, N)$ such that

$$A_N^P(k)\xi = \xi\ (mod N)\ ,\ \ \forall \xi \in L \tag{3}$$

We call the integer P "recurrence time". Thus any lattice point is a fixed point under the action of $A_N^P(k)$ and also the periodicity condition $A_N^{i+jP}(k)\xi = A^i(k)\xi$ holds, for all positive integers i, j and for all $\xi \in L$.

Figure 2 shows the recurrence time as a function of N and for some parameter values k of system (4). In most cases and for N prime number, P is equal to $N-1$ or $N+1$ and it is a common period for all periodic orbits in the lattice.The irregular character of $P = P(N, k)$ 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 "random" distribution in the lattice.

The automorphism (4) is *mixing*. It distorts any area element of the torus, that it is spread over the entire available area. If the automorphism acts on a sublattice $L' \subseteq L$, which contains a finite number of points, then L' disperses under the action of $A_N^n(k)$ and its image contains points which are distributed irregularly in L. For $n = P$ we obtain a complete recurrence and the subset L' is reconstructed. We mentioned that the dynamics of the chaotic orbits of automorphisms, can be described exactly without numerical errors, because computations are performed by using integer arithmetic.

3. CHAOTIC MIXING AND WATERMARK EMBEDDING

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

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

where L is an $N \times N$ lattice of grid size 1 and G is the total number of intensity levels. A torus automorphism $A_N(k)$ is applied on an image $I = I_0$. The result is a new image I_1 with a chaotic reallocation of pixels without effect on their intensity levels.

$$I_1 = A^n{}_N(k) I_0 \text{ such that } (i_1, j_1) = A_N(k)(i_0, j_0)\ ,\ x_{i_1 j_1} = x_{i_0 j_0}$$

By repeating the action of $A_N(k)$ on I_0 we obtain a set of images $I_i, i = 1, .., P-1$, where P is the recurrence time.

In figure 3, the automorphism (4) is applied on the 256×256 image "Lena". Mixing is observed after some iterations. Some background patterns, which show some order (e.g. the diagonal lines in case c) do not provide any information about the original structure of the image. The original image I_0 is reconstructed from an image I_n, either by the inverse system A_N^{-n} or by the system itself after $P - n$ iterations. In any case the reconstruction of a mixed image requires the knowledge of the parameter of the automorphism and the number of iterations.

Next we consider as watermark an $N \times N$ image S (e.g. the signature of the manufacturer) which is embedded into an $M_1 \times M_2$ image I_0 ($M_1 \geq N$ and $M_2 \geq N$). From the embedding, we get a signed image I_s such that i) its visual perception remain unaltered and ii) S can be detected only if the watermark parameters are known. The second requirement is satisfied when a mixing of S (say S') is embedded in I_0.The first one can be satisfied by an appropriate superposition of S' on I_0. We propose an embedding of a watermark S with few grey levels into an original grey level image I_0. The procedure is also applicable for colour images.

The images S, I_0 are represented as

$$S = \{s_{ij}, i, j \in \{0, .., N-1\}, s_{ij} \in \{0, 1, 2\}\}$$
$$I_0 = \{x_{ij}, i \in \{0, .., M-1\}, j \in \{0, .., M-1\}, x_{ij} \in \{0, .., G-1\}, G \gg 1\}$$

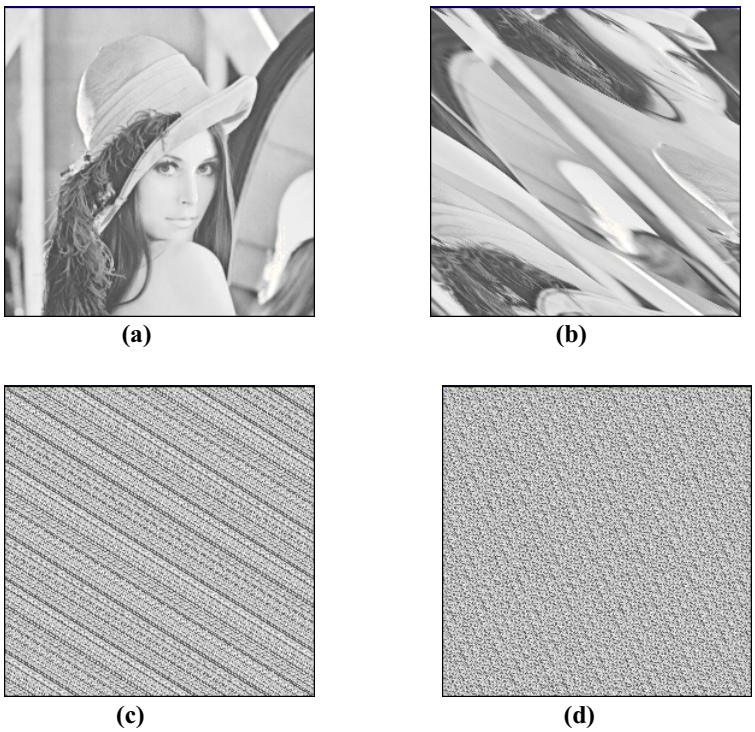

Figure 3: Mixing of "Lena" by $A^n_{256}(1)$ for b)$n = 1$, c) $n = 5$ and d) $n = 10$. For $n = P = 192$ "Lena" is reconstructed.

The grey level 0 of S correspond to watermark that should not reconstructed necessarily. Also, the levels 1 and 2 can be transformed to desired grey levels. We act the automorphism $A^n_N(k)$ on S and we get a mixed image S'

$$S' = \{s'_{ij}, i, j \in \{0, .., N-1\}, s'_{ij} \in \{0, 1, 2\}\}$$

S' is superimposed on a connected $N \times N$ subset I_N of I_0. I_N is determined by its size N and its position in I_0 (say e. g. the upper-left corner (p_1, p_2)). Then, we change the grey level parity of the pixels of I_N as follows :

$$x'_{ij} = s'_{ij} \oplus x_{ij} = \begin{cases} {y^1}_{ij} & \text{if } s'_{ij} = 1 \\ {y^2}_{ij} & \text{if } s'_{ij} = 2 \\ x_{ij} & \text{if } s'_{ij} = 0 \end{cases}$$

where

$${y^1}_{ij} = \begin{cases} x_{ij} & \text{if } x_{ij} \text{ odd} \\ x_{ij} \pm 1 & \text{if } x_{ij} \text{ even} \end{cases} \quad \text{and} \quad {y^2}_{ij} = \begin{cases} x_{ij} & \text{if } x_{ij} \text{ even} \\ x_{ij} \pm 1 & \text{if } x_{ij} \text{ odd} \end{cases}$$

The signed image I_s is represented as

$$I_s = \{y_{ij}, i \in \{0, .., M-1\}, j \in \{0, .., M-1\}, y_{ij} \in \{0, .., G-1\}\}$$

where $y_{ij} = x_{ij}$ if $x_{ij} \notin I_N$ and $y_{ij} = x'_{ij}$ if $x_{ij} \in I_N$. It is remarkable that only a part of the pixels of $I_N \subseteq I_0$ is affected by the operation $\oplus$. The grey levels of the rest of

(a) **(b)**

Figure 4: (a) signed "Lena" and (b) the reconstruction of the watermark "Playboy".

the pixels in I_N change slightly so that the visual perception of I_s is same as that of I_0.

watermark's embedding is described by the size N of I_N, the position (p_1, p_2) of I_N in I_0, the parameter k of the automorphism and the number of iterations n for mixing.

watermark's detection in I_s is achieved as follows :

i) Act the automorphism $A_N^{n-P}(k)$ on I_N, where P the recurrence time.
ii) Replace the grey level of pixels (i, j) in I_N by the grey level X if y_{ij} is even and by Y if y_{ij} is odd.

The watermark S appears like a two grey level image on a two grey level "chaotic" pattern. An example of the above procedure is illustrated in figure 4 where the watermark "Playboy" is embedded in a 41×41 box at position $(197, 202)$ in "Lena". The watermark has been mixed by using the parameters $k = 17$ and $n = 10$.

4. CONCLUSIONS

In this paper we introduced 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 to remain the same. The reconstruction of the watermark from the signed image is succeded by applying the same system and by using a specific set of parameters which characterizes the watermark embedding.

Since the set of values for the parameter k of the automorphism is finite and small $(0 < k < N)$, a "trial and error" procedure can lead to the reconstruction of the original image (or a watermark). Also, the composition of some automorphisms $A_N^n(k_i)$ belongs to the general form (1) where the values of the four integer parameters a_{ij} are restricted by the parameter N and by the property $det\mathbf{A} = 1$. A more complex system, possessing many independent parameters, can arise if we use different automorphisms on sublattices having different sizes.

The embedding procedure which is presented in section 3 is based on a simple superposition law which however does not imply robustness. Compression of the image and additive noise destroy the watermark. If the watermark consists of a small number of pixels (compared to the total size of the image) then we can use a superposition law which corresponds any pixel of the watermark to a special intensity alteration of a set of pixels. We mention that the mixing of the watermark can take place in specific sublattices of the image. Such alterations can create a hidden pattern with specific attributes such that i) the decision that a pixel belongs to a watermark depends on the attribute of its neighbourhood pattern and ii) the attributes resist under compession and noise. The satisfaction of these criteria needs further investigation which is in progress.

5. REFERENCES

[1] I. Pitas and T. Kaskalis, "Applying Signatures on Digital Images" in proceedings "1995 IEEE workshop on Nonlinear Signal and Image processing", I.Pitas (ed) , Vol I, p.460, 1995.

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

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

[4] Ya.G.Sinai (ed), "Dynamical systems II", Springer,Berlin 1988

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

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

[7] F.Vivaldi, "Arithmetical theory of Anosov diffeomorphisms", Proc.R.Soc. 413, p.97-107, 1987.

[8] M.Bartuccelli and F.Vivaldi, "Ideal orbits of toral automorphisms", Physica 39D, p.194-204, 1989.

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

[10] R.Z. Sagdeev, D.A.Usikov and G.M.Zaslavsky, "Nonlinear Physics", Harwood Academic publ. 1988.