Applications of chaotic signal processing techniques to multimedia watermarking

N. Nikolaidis, S. Tsekeridou, A. Nikolaidis, A. Tefas, V. Solachidis, I. Pitas

Artificial Intelligence & Information Analysis Laboratory
Department of Informatics
Aristotle University of Thessaloniki
GR-54006 Thessaloniki (BOX 451) GREECE
e-mail: pitas@zeus.csd.auth.gr
WWW: http://poseidon.csd.auth.gr

Abstract— *Usage of digital media has witnessed a tremendous growth during the last decades. However digital media are extremely vulnerable to copyright infringement, tampering and unauthorized distribution. Recently 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 within digital media have been proposed. In this paper we present two applications of chaotic systems to watermarking of multimedia data, namely secure spatial scrambling of watermark patterns prior to their embedding in images and generation of 1-D or 2-D watermark signals.*

I. 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. Digital audio/video/images and multimedia documents reach an ever expanding consumer base, and their domination in entertainment, arts, education etc. is just a matter of time. Digital data can be stored efficiently and manipulated (e.g. edited) easily using computers. Furthermore, digital data can be transmitted in a fast and inexpensive way through data communication networks, e.g., through the Internet. As a result, a number of applications that include but are not limited to video and audio on demand, online image databases and networked multimedia applications have emerged, contributing to the growth of electronic commerce.

During the first years of the digital revolution, protection of information received very little attention. Soon, entrepreneurs and scientists realized that the easy transmission and manipulation of digital data constitutes a real threat for information creators and distributors since copyright infringement (e.g. illegal redistribution) and tampering of such data can be achieved with very little effort. The fuss over the illegal distribution of music through the now-widespread MP3 digital audio format highlights both the vulnerability of digital data to piracy and the enormous financial implications of such pirate actions.

Unfortunately, copyright enforcement and content verification of digital data are both 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 few years, significant research efforts have been directed towards facing the challenges posed by digital technology. The solution seems to lie in data hiding or steganography. Steganography discusses methods of embedding data within a medium (host medium) in an imperceptible way by exploiting the fact that the human visual and auditory system is an imperfect detector. All forms of digital data (still images, audio, video, text documents, multimedia documents) can be used for information hiding. 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 data recipient that produced unauthorized copies. The most important requirement in both cases is that embedded data are robust to deliberate or unintentional attacks.
- *Authentication or tamper-proofing.* Unlike classic data integrity checks, i.e., digital signatures, a tamper-proofing scheme should signal an authentication violation only when significant modifications of the visual/audio content occur. For example, lossy image

This work has been funded by the LTR-ESPRIT European Project 31103 - INSPECT

compression should not signal an alarm whereas removal of an object from a scene should. Ideally, authentication techniques should provide the user not only with a binary indication of authentication violation but also pinpoint the image regions where alterations took place.

- *Covert communications*, i.e., exchange of messages secretly embedded within multimedia data. In this case, the main requirement is that the hidden data raise no suspicion that a secret message is being conveyed.
- *Captioning*, i.e., embedding of descriptive information within audio or images for applications like labeling and annotation of medical data, video/audio indexing etc. This is the application with the less stringent requirements, since in most cases no malicious attacks are expected for caption data.

In a watermarking scheme one can distinguish three fundamental functional blocks: watermark generation, embedding and detection. Watermark generation aims at constructing the information-carrying watermark pattern using an owner and/or host data dependent key. Watermark embedding can be considered as a superposition of the watermark signal on the original image in a way that ensures imperceptibility of distortions. Finally, watermark detection is usually performed by hypothesis testing, the test statistic being the correlation between the watermarked data and the watermark signal. For a review of existing schemes and a detailed discussion on the main requirements of a watermarking scheme the interested reader can consult [1], [2]. A general watermarking framework is presented in [3]. Watermark signals can be generated using one of the following approaches:

- Encryption of an existing pattern by applying a spatial/temporal transformation on its samples. For example, copyright protection or authentication watermarking of images can be achieved by embedding a binary image (e.g., a company's logo) within the image that is to be protected. The logo image has to be securely scrambled prior to its insertion in the host image using an appropriate scrambling function and a secret key. During detection, the logo is reconstructed. Thus the image owner can judge the integrity of his images or conclude that the image under investigation is his own intellectual property by visual inspection of the reconstructed binary image. Alternatively, statistical hypothesis testing can be used.
- Generation of information-carrying signals using a suitable signal generator that takes as input a secret key and, in some cases, the information bitstream. Since the performance of the correlation-based detector depends on the auto-correlation and cross-correlation functions, or equivalently the power spectrum of the generated watermarks, functions that generate watermarks possessing the desirable spectral/correlation properties are required.

Chaotic systems have been used successfully for secure information encryption (chaotic cryptography) [4],[5] and generation of spreading sequences having good correlation properties for Direct Sequence Code Division Multiple Access (DS-CDMA) communication systems [6], [7]. The close resemblance of the system requirements in these applications with the requirements of watermark generation procedures described above has motivated us to investigate the use of chaotic maps in watermarking schemes. In this paper we will deal with the use of toral automorphisms for the encryption of binary images prior to their embedding in the host image. Furthermore, the use of certain chaotic maps as generators of watermarking patterns will be investigated and some experimental results will be provided.

II. Applications of Chaotic Signals in Watermarking

A. Chaotic mixing of watermark patterns

The scrambling of binary image patterns outlined in the previous section should be able to achieve a sufficient spatial mixing of the binary image pixels so that no visually recognizable pattern can be observed once the pattern is embedded in the host image. One way for implementing such a spatial transformation is through chaotic systems called *toral automorphisms*. The mixing property of such systems guarantees the secure encryption of the information carried by the watermark pattern.

A two dimensional "toral automorphism" can be considered as a spatial transformation of planar regions [8]

$$\mathcal{A} : U \rightarrow U \; , \; U = [0, 1) \times [0, 1) \subset R^2 \qquad (1)$$

defined by the following formula:

$$\mathbf{r}' = \mathbf{r}\,\mathbf{A}(mod\,1) \qquad (2)$$

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

where (i) $a_{ij} \in Z$, (ii) $det\mathbf{A} = 1$ and (iii) $\lambda_{1,2} \notin \{-1, 0, 1\}$, ($\lambda_{1,2}$ are the eigenvalues of $\mathbf{A}$). Conditions (i) and (ii) ensure the existence of the inverse automorphism, represented by the matrix $\mathbf{A}^{-1}$. Condition (iii) ensures the chaotic behavior of the map. Repeated applications of $\mathcal{A}$ on a point $\mathbf{r}_0 \in U$ form a dynamical system $\mathcal{A}^{(n)} : U \rightarrow U$, described by the following iterative process:

$$\mathbf{r}_{n+1} = \mathbf{r}_0 \ \mathbf{A}^n \ (mod\, 1) \quad \text{or} \quad \mathbf{r}_{n+1} = \mathbf{r}_n \ \mathbf{A} \ (mod\, 1) \tag{3}$$

The set of points $\mathcal{O}(\mathbf{r}_0) = \{\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, ...\}$ is an orbit of the system. Automorphisms belong to a special class of Anosov diffeomorphisms which are strongly chaotic systems obeying local instability, ergodicity with mixing, and decay of correlation [8]. Roughly speaking, if V_0 is a dense subset of U then its image V_n under the map $\mathcal{A}^{(n)}$ spreads chaotically over the entire space of U while preserving its area.

Although the system (3) is strongly chaotic, it possesses a dense set of periodic orbits. An orbit $\mathcal{O}(\mathbf{r}_0) = \{\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, ...\}$ is periodic, if it is finite, i.e., there exists a number T of iterations such that $\mathbf{r}_0 = \mathbf{r}_T$. The necessary and sufficient condition for an orbit to be periodic is the initial position $\mathbf{r}_0$ to have rational coordinates [8].

In the case of scrambling of digital images we are interested for maps on an integer lattice (a mesh) of size $N \times N$:

$$L_N \ = \ \{(k, l) \ | \ \ 0 \leq k < N, 0 \leq l < N\} \tag{4}$$

Such a map would be of the following form:

$$\mathcal{A}_N \ : \ L_N \rightarrow L_N \tag{5}$$

$$\mathbf{r}' \ = \ \mathbf{r} \ \mathbf{A}_N \ (mod\, N) \tag{6}$$

Successive applications of the map $\mathcal{A}_N$ result into orbits on the integer lattice. All orbits of (6) are unstable periodic orbits whose periods depend on $\mathbf{A}_N$, N and the starting point of the orbit. It can be shown [9] that for any integer lattice L_N of size N, there is an integer $P = P(\mathbf{A}_N, N)$ such that:

$$\mathbf{r} \ \mathbf{A}_N^P \ (mod\, N) = \mathbf{r} \ , \ \ \forall \mathbf{r} \in L_N \tag{7}$$

P is called *recurrence time* and is the least common multiple of the periods of all orbits on the lattice.

Let us now consider a grayscale host image I of dimensions $N \times N$:

$$I = \{x(\mathbf{p}) \ | \ \ x(\mathbf{p}) \in \{0, 1, ..., G-1\}\} \tag{8}$$
$$\mathbf{p} = (i, j) \ \ 0 \leq i < N, \ 0 \leq j < N$$

(G is the number of intensity levels) and a $M_1 \times M_2$ ($M_1, \ M_2 < N$) binary 'logo' image W :

$$W = \{w(\mathbf{r}) \ | \ \ w(\mathbf{r}) \in \{0, 1\}\} \tag{9}$$
$$\mathbf{r} = (k, l) \ \ 0 \leq k < M_1, \ 0 \leq l < M_2$$

In order to scramble the logo for embedding in the host image, W is padded with pixels of value "null" ("null" can be any value except for 0 or 1) so as to form a three-valued watermark $\tilde{W}$ of dimensions $N \times N$ equal to the image dimensions:

$$\mathcal{T}_0 : W \rightarrow \tilde{W} \tag{10}$$
$$\tilde{w}(\mathbf{r}) = \begin{cases} w(\mathbf{r}) & \text{if } 0 \leq k < M_1, 0 \leq l < M_2 \\ null & \text{otherwise} \end{cases}$$

By successive applications of the map described in (6) on each pixel of $\tilde{W}$ the scrambled watermark W' results:

$$W' \ = \ \tilde{W} \, \mathcal{A}_N^d \tag{11}$$

The scrambling of a binary image after 1 and 30 iterations of the well-known cat map ($a_{11} = a_{12} = a_{21} = 1, a_{22} = 2$) can be seen in Figure 1.

The watermark key of this procedure consists of the elements of matrix $\mathbf{A}$ and the number of map iterations d. The method can be generalized by applying a series of maps with different parameters instead of a single map [10].

The scrambled watermark W' is subsequently embedded in I to obtain the watermarked image I'

$$I' = \{x'(\mathbf{p}) \ | \ \ x'(\mathbf{p}) \in \{0, 1, ..., G-1\}\} \tag{12}$$
$$\mathbf{p} = (i, j) \ \ 0 \leq i < N, \ 0 \leq j < N$$

Embedding is performed by altering the intensity $x(\mathbf{p})$ of the pixel $\mathbf{p}$ in I according to the value of the corresponding watermark pixel $w(\mathbf{r})$. Two different embedding functions g_0 and g_1 are used for this purpose. The embedding procedure can be summarized as follows:

$$x'(\mathbf{p}) \ = \ \begin{cases} g_0(x(\mathbf{p}), B_\mathbf{p}, q_0) & \text{if } w(\mathbf{r}) = 0 \\ g_1(x(\mathbf{p}), B_\mathbf{p}, q_0) & \text{if } w(\mathbf{r}) = 1 \\ x(\mathbf{p}) & \text{if } w(\mathbf{r}) = null \end{cases} \tag{13}$$

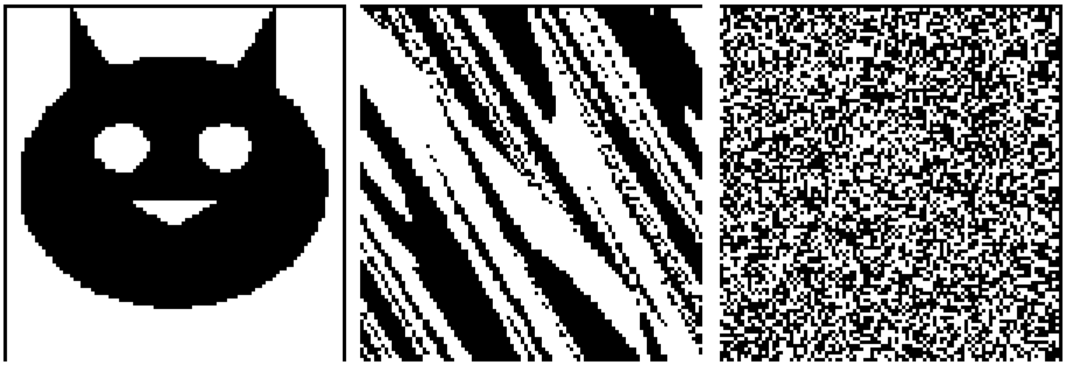
In the previous formula $B_\mathbf{p}$ denotes the neighborhood of $\mathbf{p}$ and q_0 controls the watermark embedding strength.

Watermark detection is performed by applying an appropriate detection function $D_\mathbf{p}$ to all image pixels. By considering the sign of function $D_\mathbf{p}$ on every pixel of the image, we form the following binary set :

$$Z = \{z(\mathbf{p}) \ , \ z(\mathbf{p}) \in \{0, 1\}\} \tag{14}$$
$$\mathbf{p} = (i, j) \ \ 0 \leq i < N, \ 0 \leq j < N$$

where :

$$z(\mathbf{p}) = \begin{cases} 1 & \text{if } D_\mathbf{p}(x'(\mathbf{p}), B'_\mathbf{p}) > 0 \\ 0 & \text{if } D_\mathbf{p}(x'(\mathbf{p}), B'_\mathbf{p}) < 0 \end{cases} \tag{15}$$



(a) (b) (c)

Fig. 1. The chaotic mixing of a binary image (a) after $d = 1$ (b) and $d = 30$ (c) iterations of the cat map.

The embedded logo can be reconstructed by applying the inverse map $\mathcal{A}_N^{P-d}$ on Z (P being the recurrence time of $\mathcal{A}_N$) and then using $\mathcal{T}_{\mathbf{0}}^{-1}$ to obtain only pixels $(i, j) \in [0, M_1) \times [0, M_2)$, i.e. pixels which belong to the original watermark.

The above scheme, combined with appropriately selected embedding and detection functions has been used successfully for both copyright protection [9],[10] and authentication [11] watermarking.

B. Watermark signal generation using chaotic maps

Most watermarking schemes proposed so far use a pseudorandom number generator in order to generate the 1-D or 2-D watermark signal that will be embedded in digital audio or image data. However such signals can also be constructed by the recursive application of suitable chaotic maps. A 1-D real-valued sequence for example, can be generated by the recursive application of a 1-D discrete map $\mathbf{F} : U \to U, U \subset I\!R$:

$$x(n+1) = \mathbf{F}(x(n),\ \Theta), \qquad x(n) \in U \qquad (16)$$

where $n = 0, 1, 2, ...$ denotes the current iteration and Θ is a set of parameters that control the chaotic behavior of the system. If such a mechanism is to be used for watermark generation, the sequence starting point $x(0)$ can be considered as the watermark key.

Among the various classes of chaotic maps that can be used as watermark generating functions the class of piecewise affine Markov maps provides the additional advantage of being particularly amenable to mathematical analysis. This family includes the N-way Bernoulli shift map:

$$w(n+1) = Nw(n)(mod\, 1) \;\; w(n) \in [0, 1) \qquad (17)$$

and the the N-way tailed shift map:

$$w(n+1) = \begin{cases} (N-1)w(n)(mod\, \frac{N-1}{N}) + \frac{1}{N} & 0 \leq w(n) < \frac{N-1}{N} \\ w(n) - \frac{N-1}{N} & \frac{N-1}{N} \leq w(n) < 1 \end{cases}$$

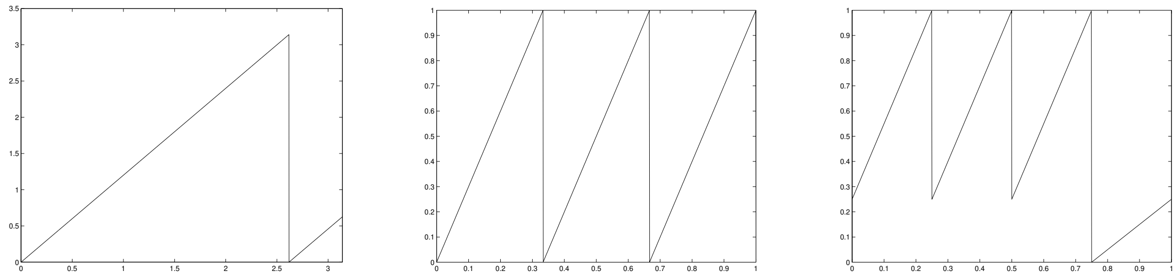
The 3-way Bernoulli shift map and the 4-way tailed shift map are depicted in Figures 2b and 2c, respectively. The power spectrum of these sequences can be evaluated using the Frobenius-Perron operator [12], [13]. It can be proven that the frequency content of the generated chaotic sequences depends on the number N of map partitions. Thus, by varying the number of partitions, the frequency characteristics of the generated sequences can be controlled to a certain extent. To be more specific, N-way Bernoulli sequences have low-pass characteristics for small values of N and tend to become white as N increases. On the other hand, N-way tailed sequences have their energy content concentrated at high frequencies for small values of N and become white for large values of N.

Another map exhibiting interesting properties is the Renyi map defined by the following recursion:

$$w(n+1) = \lambda w(n)(mod\, \pi) \qquad (18)$$

Parameter λ controls the frequency characteristics of the chaotic sequence. For $\lambda > 1$ and close to 1 low-pass behavior can be obtained, whereas for $\lambda \simeq 2$ an almost white signal results. The Renyi map for $\lambda = 1.2$ can be seen in Figure 2a.

Since the spectral characteristics of signals are closely related to their correlation function (the power spectral density is the Fourier transform of the autocorrelation function), which in turn affects the performance of a watermarking scheme based on correlation detection, the control over the spectral characteristics of the chaotic signals presented above is a highly desirable feature. Furthermore, by controlling the spectrum of the watermark, robustness to certain types of distortions (e.g. low-pass distortions) can be achieved.



(a) (b) (c)

Fig. 2. (a) Renyi map for $\lambda = 1.2$. (b) N-way Bernoulli map for $N = 3$. (c) N-way tailed map for $N = 4$.

The 1-D chaotic maps described above generate real-valued sequences. However, the majority of watermarking applications involve balanced binary sequences, i.e., sequences with equal numbers of the two symbols. To obtain such sequences the real-valued chaotic sequence should be thresholded on the median value of the map output distribution. Discrete-valued signals resulting from an appropriate quantization of the real-valued sequence can also be obtained.

1-D chaotic sequences can be readily embedded in audio signals. To embed the 1-D sequences in a digital image, the image pixels should be traversed in a suitable order (scan order). It is obvious that the frequency content of the 2-D sequences generated this way will differ from that of the initial 1-D sequence. The trivial choice for the scan order is the raster scan in which the 2-D lattice is traversed in a row-by-row manner. Unfortunately, raster scan does not preserve the frequency characteristics of the initial 1-D signal. An alternative scanning order that sufficiently preserves the frequency characteristics of the 1-D signal is the so-called Peano scan [14]. If the 1-D signal is low-pass and we wish to retain or even amplify its low-pass characteristics a cellular smoothing stage [14] can be added after the Peano scanning. Cellular smoothing eliminates spontaneous transitions that might emerge after the Peano scan by rearranging pixels so that compact neighborhoods are formed.

The watermarks generated using the procedure outlined above can be embedded in the host signals using a general superposition law and an appropriate embedding domain (spatial/temporal, DCT, DFT, DWT etc). For instance, additive temporal embedding in audio signals can be implemented by the following embedding law:

$$f_w(n) = f(n) + h(n) \cdot w(n) \qquad (19)$$

where $f_w(n)$, $f(n)$ are the watermarked and the original audio signals, $w(n)$ is the discrete-valued watermark sequence and $h(n)$ is the watermark strength parameter which in most cases is taken to be constant:

$$h(n) = h \qquad (20)$$

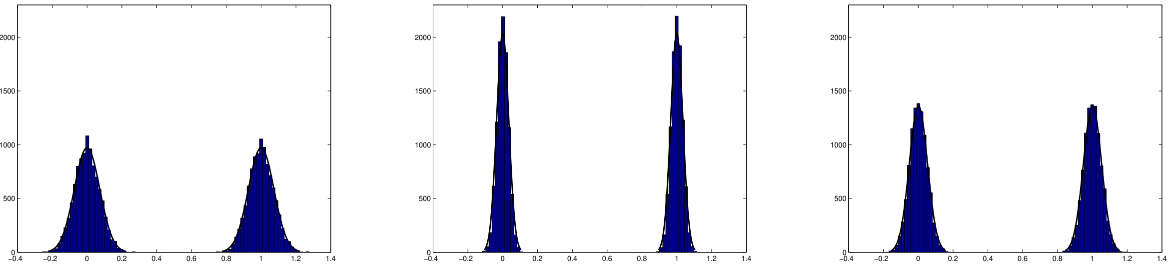
Watermark detection is accomplished by evaluating the appropriately normalized correlation c between $f_w(n)$ and $w(n)$:

$$c = \frac{1}{v_{norm}} \sum_n w(n) f_w(n) \qquad (21)$$

and comparing it to a suitably selected threshold T. For a certain threshold, the detection performance is described in terms of the false alarm probability, (i.e., the probability to detect a watermark in a signal that is not watermarked or is watermarked with a different watermark) and the probability of false rejection (i.e., the probability to erroneously neglect the watermark existence in the signal). In the ideal case, the values of these probabilities should be zero. By plotting these two probabilities as a function of the threshold T the receiver operating characteristic (ROC) curve for the corresponding watermark system results. This curve conveys all the necessary system performance information.

III. Experimental Results

The potential advantages of N-way Bernoulli and N-way tailed sequences have been quantified on a set of audio watermarking experiments. Ten seconds of a 44.1 KHz, 16 bits/sample mono audio signal were used as host signal. N-way Bernoulli and N-way tailed sequences for various values of N were compared against pseudorandom sequences generated by a random number generator routine. Watermark embedding was performed using Equation (19) while a correlator of the form (21) was used for detection. The watermark sequence length was equal to the number of audio samples whereas the watermark strength



(a) (b) (c)

Fig. 3. Empirical pdfs of the correlator output (left distribution: incorrect watermark presence, right distribution: correct watermark presence): (a) N-way Bernoulli sequences, $N = 3$; (b) N-way tailed sequences, $N = 4$; (c) pseudorandom sequences.

parameter was selected so that the SNR in the watermarked audio sample was $30dB$. For each class of watermark sequences 10000 trials involving watermark detection on a signal marked with the watermark under investigation and no signal distortions were conducted. An equal number of trials involving watermark detection on a signal marked with a different watermark than the one under investigation were also performed. The empirical pdfs (histograms) of the correlator value c were constructed for both cases. These pdfs for N-way Bernoulli sequences of $N = 3$, N-way tailed sequences of $N = 4$ and pseudorandom sequences can be seen in Figures 3a-c. The variance of the distributions that correspond to N-way Bernoulli sequences is bigger than the variance of the pdfs for the pseudorandom sequences whereas the pdfs for the N-way tailed sequences have considerably smaller variance.

The receiver operating characteristics for the N-way Bernoulli and N-way tailed sequences for various values of N have also been evaluated and compared to the ROC corresponding to pseudorandom watermark sequences. The results can be seen in Figure 4. Watermarks generated using N-way Bernoulli maps perform worse than pseudorandom sequences. This can be explained on the basis of the frequency characteristics of these sequences. It has been proven [15] that, when no distortions are considered, white watermarks outperform low-pass watermarks in terms of false alarm versus missed detection probabilities. As described in the previous section, pseudorandom watermarks have an almost white spectrum whereas N-way Bernoulli sequences have their energy content concentrated on the lower frequencies and thus, their performance is inferior.

On the other hand, N-way tailed watermarks outperform pseudorandom watermarks. This can be attributed to the high-pass nature of N-way tailed sequences. Theoretical investigations are under way to support this experimental conclusion with concrete theoretical evidence. Note that, as N increases, ROC curves for both N-way Bernoulli and N-way tailed sequences converge to the ROC of the pseudorandom sequence, since for large values of N the spectrum of both subclasses of chaotic sequences tends to become white.

The performance ranking of the three types of sequences is reversed if distortions of low-pass nature e.g., mean filtering and JPEG compression are considered. In such a case, the best performance is achieved by N-way Bernoulli sequences for small values of N. This is due to the fact that the low-pass N-way Bernoulli sequences are far less vulnerable to such distortions. On the contrary, high-frequency N-way tailed sequences are filtered out by distortions of this type and thus exhibit the worse performance.

IV. Conclusions

Two applications of chaotic maps in multimedia watermarking have been reviewed in this paper. The first application is spatial scrambling of binary images prior to their embedding in the host image. Toral automorphisms can be used in this case to ensure a secure and straightforward to implement scrambling. The second application is the generation of watermark sequences. Chaotic maps can be used to generate watermark sequences of controllable spectral/correlation characteristics. This allows us to generate watermark sequences according to the application at hand. For example, when no signal distortions are expected, one can use N-way tailed sequences, which perform better than the widely used pseudorandom sequences in such a situation. If robustness to low-pass distortions is required, N-way Bernoulli sequences can be used instead of pseudorandom sequences, since they are less sensitive to this type of distortions. In both cases, the

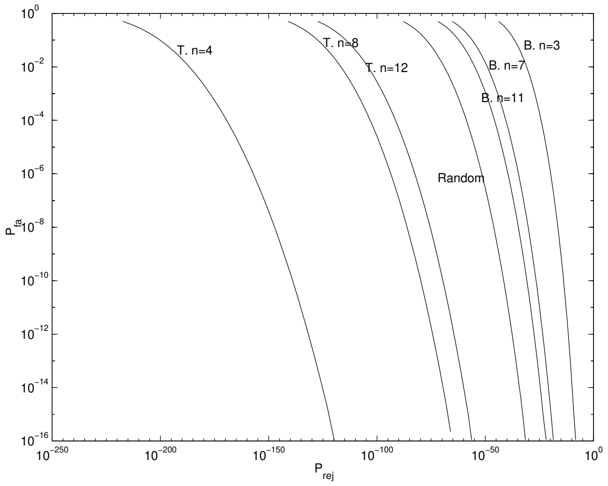


Fig. 4. Receiver operating characteristics (probability of false alarm P_{fa} versus probability of false rejection P_{rej}) for N-way Bernoulli, N-way tailed and pseudo-random sequences.

system performance can be fine-tuned by varying the number of map partitions. Ongoing research focuses on the use of maps that allow greater control on the output sequence spectrum.

REFERENCES

[1] N. Nikolaidis, I. Pitas, Digital image watermarking: an overview, *ICMCS 99*, vol I, pp 1-6, 1999.

[2] M. Swanson, M. Kobayashi, A. Tewfik, Multimedia Data-Embedding and Watermarking Technologies, *Proceedings of the IEEE*, vol 86, no 6, pp. 1064-1087, June 1998.

[3] G.Voyatzis and I.Pitas, The use of watermarks in the protection of multimedia products, *Proceedings of the IEEE*, vol 87, no 7, pp 1197-1207, July 1999.

[4] M. Gotz, K. Kelber, W. Schwarz, Discrete time chaotic encryption systems, Part I: Statistical design approach, *IEEE Trans. on Circuits and Systems-I*, vol 44, no 10, pp 963-970, October 1997.

[5] D. R. Frey, Chaotic digital encoding: An approach to secure communication, *IEEE Trans. on Circuits and Systems-II*, vol. 40, no 10, pp. 660-666, October 1993.

[6] R. Mazzini, G. Setti, R. Rovatti, Chaotic complex spreading sequences for asynchronous DS-CDMA-Part I: System Modeling and Results, *IEEE Trans. on Circuits and Systems-I*, vol 44, no 10, pp 937-947, October 1997

[7] R. Rovatti, G. Setti, R. Mazzini, Chaotic complex spreading sequences for asynchronous DS-CDMA-Part II: Some theoretical performance bounds, *IEEE Trans. on Circuits and Systems-I*, vol 45, no 4, pp 496-506, April 1998.

[8] D.K. Arrowsmith, C.M. Place, *An introduction to dynamical systems*, Cambridge Univ. Press, 1990.

[9] G.Voyatzis and I.Pitas, Chaotic mixing of digital images and applications to watermarking, *ECMAST'96*, vol.2, pp. 687-694, 1996.

[10] G.Voyatzis, I. Pitas, Digital image watermarking using mixing systems, *Computer & Graphics*, vol 22, no 4, pp 405-416, 1998

[11] A. Tefas, I. Pitas, Image authentication using chaotic mixing systems, *ISCAS 2000* to appear

[12] A. Lasota and M.C. Mackey, *Chaos, fractals, and noise*, Springer-Verlag, 2nd edition, 1994.

[13] Thomas Schimming, Marco Gotz, Wolfgang Schwarz, Signal modeling using piecewise linear chaotic generators, *EUSIPCO-98*, vol. 3, pp. 1377-1380. September 1998.

[14] G. Voyatzis, I. Pitas, Chaotic watermarks for embedding in the spatial digital image domain, *ICIP '98*, vol. 2, pp. 432-436, October 1998.

[15] J. Linnartz, A. Kalker, G. Depovere, Modeling the false-alarm and missed detection rate for electronic watermarks, *2nd Workshop on Information Hiding*, April 1998.