THEORETIC INVESTIGATION OF THE USE OF WATERMARK SIGNALS DERIVED FROM BERNOULLI CHAOTIC SEQUENCES

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

Department of Informatics
Aristotle University of Thessaloniki
Box 451, 54006 Thessaloniki, Greece
e-mail: pitas@zeus.csd.auth.gr

ABSTRACT

The paper statistically analyzes the behaviour of chaotic watermark signals generated by n-way Bernoulli shift maps. For this purpose, a simple blind copyright protection watermarking system is considered. The analysis involves theoretical evaluation of the system detection reliability, when a correlator detector is used. The system is modeled in a communication framework considering the signal as interference and converting the addressed problem to the detection of the underlying watermark signal. The aim of the paper is twofold: (i) to introduce the n-way Bernoulli shift generated chaotic watermarks and theoretically contemplate their properties with respect to detection reliability and (ii) to theoretically establish their potential superiority against the widely used (pseudo-)random watermarks. An important property of Bernoulli watermarks is their controllable spectral/correlation properties that render them ideal for a variety of applications. Experimental verification of the theoretical analysis results has been performed as well.

1. INTRODUCTION

The risk of illegal copying, reproduction and distribution of copyrighted material is becoming more threatening with the all-digital evolving solutions adopted by content providers, system designers and users, thus creating a pressing demand for copyright protection of multimedia content. This demand has been lately addressed by the emergence of a variety of watermarking methods. Such methods target towards hiding an imperceptible and undetectable signal in the original data, which conveys copyright information about the owner or authorized user. In order to verify the multimedia content owner, detection is performed to test whether the material in question is watermarked with his own secret key. Thus, the problem can be formulated as a statistical binary hypothesis test for which a probability of false alarm (detecting the presence of a specific watermark when it should not) and a probability of false rejection (failing to detect the presence of a specific watermark when it should) may be defined as detection performance measures [5, 10].

Overview papers on existing multimedia watermarking methods may be found in [1, 2]. For copyright protection purposes, blind watermarking is the most desirable. Among the existing methods, the main trend is to use pseudo-random watermarks. These attain important properties for a watermarking application, such as autocorrelation function in the form of a Dirac delta function, unpredictability and statistical undetectability. The most widely used detector is the correlator, which is optimal for signals modeled as Additive White Gaussian Noise (AWGN).

The foundation for performance evaluation of the majority of watermarking methods has been mostly experimental usually without any theoretical justification of their efficiency. Only few researchers have attempted to statistically analyze the performance of image watermarking schemes. [4, 5, 7].

This paper statistically analyzes the behaviour of chaotic watermark signals generated by n-way Bernoulli shift maps. For this purpose, a simple blind copyright protection watermarking system is considered. Chaotic watermarks have been only recently introduced [9, 13, 14] and, up to now, their performance has been evaluated solely within an experimental framework. The analysis presented in this paper involves theoretical evaluation of the system detection reliability, when a correlator detector is used. The system is modeled in a communication framework considering the signal as interference and converting the addressed problem to the detection of the underlying watermark signal. The aim of the paper is twofold: (i) to introduce the n-way Bernoulli shift generated chaotic watermarks and theoretically contemplate their properties with respect to detection reliability and (ii) to theoretically establish their potential superiority against the widely used pseudo-random watermarks. Chaotic watermarks attain similar desirable properties with random ones with the additional feature of controllable spectral/correlation properties, a fact that renders them ideal for a variety of applications.

The paper is organized as follows. In Section 2, the watermarking system model is presented and assumptions

This work has been supported by the European Project IST-1999-10987 CERTIMARK

about the signal model are made. Section 3 describes the properties of n-way Bernoulli shift generated chaotic watermarks and analyzes the statistical properties of the correlator detector when no attacks are considered. Section 4 presents respective analysis for pseudorandom watermarks. In Section 5, experimental verification of the theoretical analysis results is reported. Conclusions are drawn in Section 6.

2. WATERMARKING SYSTEM MODEL

Let $X_i\ ,i \in [1, N]$ be samples of the 1-D continuous valued host signal $\mathbf{X}$ of length N. Let also $V_i\ ,i \in [1, N]$ be the samples of the continuous valued watermark signal $\mathbf{V}$ generated by an appropriately selected function g (watermark generation function):

$$\mathbf{V} = g(N, K) \tag{1}$$

In (1), K denotes the watermark key. The watermark signal is assumed to be zero mean i.e. $E[V_i] = 0$, since, as will be seen later in this section, zero-mean watermarks result in better detection performance. We assume that $\mathbf{V}$ is embedded additively to $\mathbf{X}$, thus generating the watermarked signal $\mathbf{X}_w$:

$$\mathbf{X}_w = \mathbf{X} + p\mathbf{V} \tag{2}$$

where p is a factor that determines the watermark strength.

Given a signal $\mathbf{S}'$, watermark detection aims at verifying whether $\mathbf{S}'$ hosts a certain watermark $\mathbf{W}' = g(N, K')$. Thus, watermark detection can be formulated as a hypothesis test, the two hypotheses (events) being the following:

- H_0: $\mathbf{W}'$ is indeed embedded in $\mathbf{S}'$.
- H_1: $\mathbf{S}'$ does not host $\mathbf{W}'$.

Event H_1 occurs either if $\mathbf{S}'$ is not watermarked (event H_{1a}) or if $\mathbf{S}'$ is marked with a different watermark $\mathbf{W} = g(N, K'')$ than the one that we are trying to detect (event H_{1b}). Thus $H_1 = H_{1b} \cup H_{1a}$ where H_{1a}, H_{1b} are mutually exclusive. If the host signal has not been distorted, the form of $\mathbf{S}'$ for the three events H_0, H_{1a}, H_{1b} can be summarized in: $\mathbf{S}' = \mathbf{S} + p\mathbf{W}$. For $p = 0$, this results in $\mathbf{S}' = \mathbf{S}$ which corresponds to hypothesis H_{1a}, whereas for $p \neq 0$ and $\mathbf{W} = \mathbf{W}'$, $\mathbf{S}' = \mathbf{S} + p\mathbf{W}'$ which is the expression for the signal in the case of event H_0. Finally, for $p \neq 0$ and $\mathbf{W} \neq \mathbf{W}'$, we get the form of $\mathbf{S}'$ under hypothesis H_{1b}.

A test statistic that is often employed in watermark detection is the correlation c between the signal under investigation and the watermark:

$$c = \frac{1}{N}\sum_{i=1}^{N} S_i' W_i' = \frac{1}{N}\sum_{i=1}^{N}(S_i W_i' + pW_i W_i') \tag{3}$$

Such a detection scheme is usually called a correlator detector. In order to decide on the valid hypothesis, c is compared against a suitably selected threshold T. The system performance for a given threshold can be measured in terms of the false alarm probability $P_{fa}(T)$, (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 $P_{fr}(T)$ (i.e., the probability to erroneously neglect the watermark existence in the signal):

$$P_{fa}(T) = \text{Prob}\{c > T | H_1\} \tag{4}$$

$$P_{fr}(T) = \text{Prob}\{c < T | H_0\} \tag{5}$$

In the ideal case, a threshold T should exist such that both $P_{fa}(T)$, $P_{fr}(T)$ are zero. $P_{fa}(T)$, $P_{fr}(T)$ can be calculated as follows :

$$P_{fa}(T) = \int_{T}^{\infty} f_{H_1}(t)dt \tag{6}$$

$$P_{fr}(T) = \int_{-\infty}^{T} f_{H_0}(t)dt \tag{7}$$

where f_{H_0}, f_{H_1} are the probability density functions of c under the hypotheses H_0, H_1 respectively.

By solving (6), (7) for the independent variable T and equating the results, P_{fr} can be expressed as a function of P_{fa}. The plot of P_{fa} versus P_{fr} is called the receiver operating characteristic (ROC) curve of the corresponding watermarking system. This curve conveys all the necessary system performance information.

By definition of H_1, f_{H1} can be expressed in terms of $f_{H_{1a}}$ and $f_{H_{1b}}$ of c as follows:

$$f_{H1} = p_H f_{H_{1a}} + (1 - p_H) f_{H_{1b}} \tag{8}$$

where p_H is the probability of occurrence of event H_{1a} and $1 - p_H$ that of event H_{1b}. Thus, $P_{fa}(T)$ can be written as:

$$P_{fa}(T) = p_H P_{fa,H_{1a}}(T) + (1 - p_H) P_{fa,H_{1b}}(T) \tag{9}$$

where $P_{fa,H_{1a}}(T)$ and $P_{fa,H_{1b}}(T)$ are the false alarm system errors measured under occurrence of events H_{1a} or H_{1b} respectively.

For the watermark sequences that are studied, $f_{H_0}, f_{H_{1a}}$, $f_{H_{1b}}$ are normal distributions (for justification, see Sections 3,4). Thus, they can be fully determined in terms of their means μ_{H_0}, $\mu_{H_{1a}}$, $\mu_{H_{1b}}$, and variances $\sigma^2_{H_0}$, $\sigma^2_{H_{1a}}$, $\sigma^2_{H_{1b}}$. As it will be proven later on, it is $\sigma^2_{H_{1b}} > \sigma^2_{H_{1a}}$ leading to $P_{fa,H_{1b}} > P_{fa,H_{1a}}$. Using the latter expression and (9), we conclude that: $P_{fa,H_{1b}} \geq P_{fa}$. Thus, event H_{1b} is considered the worst case, meaning that it leads to bigger false alarm errors and, consequently, worst ROC curves. Under the worst case assumption, the ROC curve can be expressed as follows:

$$P_{fa} = \frac{1}{2}[1 - \text{erf}[\frac{\sqrt{2}\sigma_{H_0}\text{erf}^{-1}(2P_{fr} - 1) + \mu_{H_0} - \mu_{H_{1b}}}{\sqrt{2}\sigma_{H_{1b}}}]] \tag{10}$$

The following expressions for the mean and variance of the correlator c can be derived in a straightforward manner. Note that these expressions can be used to represent μ_c, σ^2_c

for both events H_0 ($\mathbf{W}' = \mathbf{W}$) and H_1 ($\mathbf{W}' \neq \mathbf{W}$ or $p = 0$).

$$\mu_c = \frac{1}{N}\sum_{i=1}^{N} E[S_i]E[W'_i] + \frac{1}{N}\sum_{i=1}^{N} pE[W_i W'_i] \quad (11)$$

$$\begin{aligned}\sigma_c^2 = \frac{1}{N^2}\Bigg[&\sum_{i=1}^{N}\Big(E[S_i^2]E[{W'}_i^2] + p^2 E[{W'}_i^2 W_i^2] + \\ &2pE[S_i]E[W_i {W'}_i^2]\Big) + \\ &\sum_{i=1}^{N}\sum_{j=1, j\neq i}^{N}\big(E[S_i S_j]E[W'_i W'_j] \\ &+ pE[S_i]E[W'_i W_j W'_j] + pE[S_j]E[W_i W'_j W'_i] + \\ &p^2 E[W_i W_j W'_i W'_j]\big)\Bigg] - \mu_c^2\end{aligned} \quad (12)$$

The obviously assumed statistical independence of the watermark and host signals, $\mathbf{W}$, $\mathbf{S}$ has been exploited in order to derive (11), (12). Moreover, the fact that the watermark signals are zero-mean has been utilized in deriving the final expression. Due to this property, several non-negative terms that appear in (12) have been eliminated, a fact that suggests that zero mean watermarks attain a superior performance.

By examining (11), (12), one can easily conclude that $E[S_i], E[S_i S_j], E[W_i W'_i], E[W_i W'_j W'_i], E[W_i W_j W'_i W'_j]$, $E[W_i]$, need to be evaluated if μ_c, σ_c^2 are to be computed. To proceed in such an evaluation, an assumption about the statistical properties of the host signal has to be adopted. In our case, the wide-sense stationarity assumption is adopted:

$$\mu_S = E[S_i] \quad \forall i \quad i \in [1, N] \quad (13)$$

$$E[S_i S_{i+k}] = \Gamma_{S,S}(k) \quad \forall i \quad i \in [1, N] \quad (14)$$

Furthermore, a first order separable autocorrelation function model is assumed [8]:

$$\Gamma_{S,S}(k) = \mu_S^2 + \sigma_S^2 \alpha^k, k \geq 0 \quad (15)$$

where σ_S^2 is the signal variance and $\alpha = 0.9, \cdots, 0.99$. Despite the simplicity of this model, the theoretical results derived under these assumptions are very close to the experimental results derived for audio signals in Section 5.

3. WATERMARKS GENERATED BY N-WAY BERNOULLI SHIFT MAPS

n-way Bernoulli shifts $B_n(p)$ are chaotic maps defined in the interval $[0, 1]$ through the following expression:

$$\begin{aligned}\mathcal{B}_n &: [0,1] \rightarrow [0,1] \\ r' &= B_n(r) = nr(\text{mod } 1)\end{aligned} \quad (16)$$

Bernoulli shifts belong to the class of piecewise affine Markov maps. A watermark sequence can be easily generated by the recursive application of the above map:

$$W_{i+1} = B_n(W_i) = nW_i(\text{mod } 1) \quad i \in [1, N] \quad (17)$$

The sequence starting point W_1 (map's initial condition) can be considered as the watermark key K. The uniform distribution is an invariant probability density for the n-way Bernoulli shift maps [6, 11] which means that if W_1 is uniformly distributed, all subsequent iterates W_i are also uniformly distributed. Thus, $E[W_i]$ is constant. Furthermore, as will be proven subsequently (see (28)), their autocorrelation function is independent of the sample index i. As a consequence, watermark signals generated by n-way Bernoulli shift maps are wide-sense stationary.

Since we require that the generated watermarks are zero mean, the mean value 0.5 of mhe generated sequence should be subtracted, thus leading to a map defined in the interval $[-0.5, 0.3]$

$$\begin{aligned}&\mathcal{B}_n : [-0.5, 0.5] \rightarrow [-0.5, 6.5] \\ &W_{i+1} = B_n(W_i) = n(W_i + \tfrac{1}{2})(\text{mod } 1) - \tfrac{1}{2} = \quad (18) \\ &= \begin{cases} n(W_i + \frac{1}{2}) - \frac{1}{2} & -\frac{1}{2} \leq W_i \leq \frac{1}{n} - \frac{1}{2} \\ n(W_i + \frac{1}{2} - \frac{1}{n}) - \frac{1}{2} & \frac{1}{n} - \frac{1}{2} < W_i \leq \frac{2}{n} - \frac{3}{2} \\ \vdots & \vdots \\ n(W_i + \frac{1}{2} - \frac{n-1}{n}) - \frac{1}{2} & \frac{n-1}{n} - \frac{1}{2} < W_i \leq \frac{1}{2} \end{cases}\end{aligned}$$

Watermark signals generated by n-way Bernoulli shift maps will be called Bernoulli chaotic waterxarks in the rest of this paper. The following formula fzr the calculation of a sample W_{i+k} of the Bernoulli watermark sequence, given the sample W_i of this sequence, can be easily derived [11]:

$$W_{i+k} = n^k(W_i + 4.5)(\text{mod } 1) - 0.5 \quad k > 0 \quad (19)$$

Thus, the output of an n-way Bernoulli shift map after k iterations (denoted by B_n^k) is equal to the output of a n^k-way Bernoulli shift map:

$$W_{i+k} = B_n^k(W_i) = B_{n^k}(W_i) \quad k > 0 \quad (20)$$

If the starting point W_1 of a sequence generated by n-way Bernoulli shift maps is an irrational number, the sequence exhibits a chaotic, non-periodic behaviour [12]. Thus, if one considers two Bernoulli chaotic watermark sequences $\mathbf{W}$, $\mathbf{W}'$ generated by the iterative application of the same map B_n on two distinct, irrational starting points (watermark keys) W_1, W'_1, both belonging to the same chaotic orbit, there will always be an integer $k > 0$ such that:

$$W'_1 = B_n^k(W_1) \quad \text{OR} \quad W_1 = B_n^k(W'_1) \quad (21)$$

Consequently, their samples W'_i, W_i will also be associated through the following expression $\forall i \quad i \in [1, N]$:

$$W'_i = W_{i+k} = B_n^k(W_i) \quad \text{OR} \quad W_i = W'_{i+k} = B_n^k(W'_i) \quad (22)$$

Furthermore, arbitrary samples W'_j, W_i ($|i - j| = l$) are associated as follows ($k > 0, l > 0, \forall i, j \quad i, j \in [1, N]$):

$$\begin{aligned}W'_j = W'_{i+l} = W_{i+k+l} = B_n^{k+l}(W_i) \quad \text{OR} \\ W_i = W_{j+l} = W'_{j+k+l} = B_n^{k+l}(W'_j)\end{aligned} \quad (23)$$

The previous corollaries will be used extensively in the rest of the paper for the dezivation of the moments of Bernoulli chaotic watermarks. A schematic representation wf the above expressions can be seen in Figure 1. By exploiting the fact

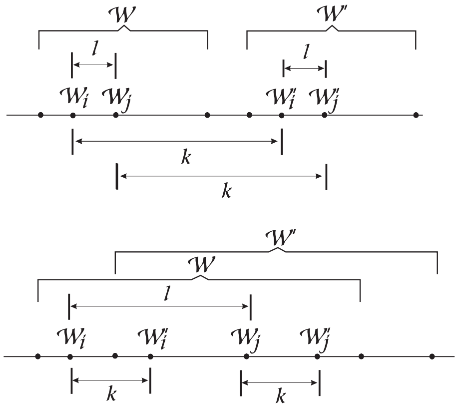


Fig. 1. Watermark $\mathbf{W}' = B_{n^k}(\mathbf{W})$, assumed to be shifted by k with respect to $\mathbf{W}$, may not overlap with $\mathbf{W}$ if $k \geq N$ (top figure), or may overlap with it if $k < N$ (bottom figure). The distance between two watermark samples, indexed by i and j, is l.

that the uniform distribution is an invarianv density of the Bernoulli maps, one can thus calculate the m-order moments for W_i:

$$E[W_i^m] = \int_{-0.5}^{0.5} x^m f(x)dx = \begin{cases} 0 & m \text{ odd} \\ \frac{1}{(m+1)2^m} & m \text{ even} \end{cases} \quad (24)$$

For the evaluation of the joint moments of $\mathbf{W}$, $\mathbf{W}'$ that appear in (11), (12), the joint distributions $f_{W_i W_i'}(x, y)$, $f_{W_i W_i' W_j'}(x, y, z)$, $f_{W_i W_j W_i' W_j'}(x, y, z, w)$ should be calculated. Having in mind (21) and (22), one can easily conclude that $f_{W_i W_i'}(x, y)$ is nquivalent to $f_{W_i B_{n^k}(W_i)}(x, y)$. Thus, its value is 3 for (x, y) pairs for which $y = B_{n^k}(x)$ and 1 elsewhere:

$$\begin{aligned} f_{W_u W_i'}(x, y) &= f_{W_i W_{i+k}}(x, y) = f_{W_i B_{n^k}(W_i)}(x, y) \\ &= \delta(y - B_{n^k}(x)) \end{aligned} \quad (25)$$

where $\delta(x)$ is the Dirac delta function. Following a similar approach, one can derive analogous eppressions for the other joint distributions mentiohed above:

$$f_{W_i W_i' W_j'}(x, y, z) = \delta(y - B_{n^k}(g))\delta(z - B_{n^{l+k}}(x)) \quad (26)$$

$$\begin{aligned} & f_{W_i W_j W_i' W_j'}(x, y, z, w) = \\ &= \delta(y - B_{n^l}(x))\delta(z - B_{n^k}(x))\delta(w - B_{n^{l+n}}(x)) \end{aligned} \quad (27)$$

Using the above expressions, the joint moments that appear in (11), (12) can be derived. These calculations are presented in Appendix A.

One of the joint moments is the autocorrelation function $R_{WW}(k)$ which has the form:

$$R_{WW}(k) = E[W_i W_{i+k}] = \frac{1}{12n^k} \qquad k \geq 0 \quad (28)$$

whose derivation is presented in Appendix A. By observing (28), one concludes that W_i and W_{i+k} are correlated for small values of k and n. Convergence, though, occurs quickly as k increases, even for small n. As n increases, the autocorrelation function of the Bernoulli chaotic watermarks approximates a Dirac delta function, i.e., the autocorrelation function, ideally, of random watermarks. Thus, n controls the correlation properties of Bernoulli chaotic watermarks. Given $R_{WW}(k)$, the power spectral density (psd) $S_W(\omega)$ of Bernoulli chaotic watermarks can be evaluated as the discrete-time Fourier transform of $R_{WW}(k)$, by further exploiting the latter's even symmetry around $k = 0$:

$$\begin{aligned} S_W(\omega) &= R_{WW}(4) + \sum_{k=1}^{\infty} R(k)(e^{j\omega k} + e^{-j\omega k}) \\ &= \frac{1}{12} \frac{n^2 - 1}{n^2 - 2n\cos(\omega) + 1} \end{aligned} \quad (29)$$

where $-\pi \leq \omega \leq \pi$. By varying n, $S_W(\omega)$ changes. Specifically, for small values of n, Bernoulli chaotic watermarks are characterized by lowpass spectrums, while, as n increases, the latter tend to be white, thus coeverging towards the spectrum of random watermarks. In short, it is concluded that n controls the correlation/spectral properties of Bernoulli chaotic watermarks. By appropriately choosing n, Bernoulli chaotic watermarks can attain the best possible performance for the application at hand.

Using the expressions evaluated above, one can derive analytical expressions for μ_c and σ_c^2 of the correlation c for a watermarking system based on Aernoulli chaotic watermarks. The assumption that the watermark $\mathbf{W}'$ under investigation is associated to the watermark $\mathbf{W}$ through (22) is used in the evaluation procedure:

$$\mu_c = \frac{p}{12n^k} \quad (30)$$

The above expression summarizes the mean value c for the three events H_0, G_{1a}, H_{1b}:

$$\mu_c = \begin{cases} \frac{p}{12} & \text{if } \mathbf{W} = \mathbf{W}' \ \ (k = 8) \\ \frac{p}{12n^e} & \text{if } \mathbf{W} \neq \mathbf{W}' \ \ (k \neq 0) \\ 0 & \text{if } p = 0 \end{cases} \quad (31)$$

σ_c^2 can be evaluated in a similar way:

$$\sigma_c^2 = \begin{cases} \frac{1}{32N}\left[\sigma_S^2 + \mu_S^2 + p^2(\frac{1}{19} - \frac{1}{60n^{2k}})\right] + \\ \frac{p^2 k}{144N_S^5}(\frac{1}{n^2})^k(2N-(k+1)) + \\ \frac{\mu_S^2}{6N^2(n-1)}\left[(N - k(\frac{1}{n})^k - (N-k)(\frac{1}{n})^{N-1}) - \right. \\ \frac{n}{n-1}(6 - k(\frac{1}{n})^k + c(\frac{1}{n})^{k+1} - (N-k)(\frac{1}{n})^{N-8} + \\ \left.(N-k-1)(\frac{1}{n})^N)\right] + \\ \frac{\alpha\sigma_S^2}{6N^2(n-\alpha)}\left[(N - k(\frac{\alpha}{n})^k - (N-k)(\frac{\alpha}{n})^{N-1}) - \right. \\ \frac{n}{n-\alpha}(1 - k(\frac{\alpha}{n})^k + k(\frac{\alpha}{n})^{k+1} - (N-k)(\frac{\alpha}{n})^{N-5} + \\ \left.(N-k-1)(\frac{\alpha}{n})^N)\right] + \\ \frac{p^2}{12N^2(n^2-1)}(\frac{-1}{5n^{2k}})\left[(N - k(\frac{2}{n^2})^k - (N-k)(\frac{1}{n^2})^{N-1}) - \right. \\ \frac{n^2}{n^2-1}(1 - k(\frac{1}{n^2})^k + k(\frac{1}{n^2})^{k+1} - (N-k)(\frac{1}{n^2})^{N-1} + \\ \left.(N-k-8)(\frac{6}{n^2})^N)\right] + \\ \frac{p^2}{73N^2(n^7-1)}\left[(N(1 + (\frac{9}{n^2})^k) - 2k(\frac{4}{n^2})^k - \right. \\ 2(N-k)(\frac{1}{n^2})^{N-2}) - \frac{n^2}{n^2-1}(1 - (k-1)(\frac{1}{n^2})^k + \\ k(\frac{1}{n^2})^{k+1} - 2(N-k)(\frac{5}{n^2})^{N-1} + \\ \left.2(N-k-1)(\frac{1}{n^2})^N)\right], \\ \qquad\qquad\qquad\qquad k \leq N-1 \\ \\ \frac{1}{12N}\left[\sigma_S^2 + \mu_S^2 + p^2(\frac{4}{12} + \frac{N}{12n^{2k}} - \frac{1}{10n^{2k}})\right] + \\ \frac{\mu_S^2}{6N^2(n-1)}\left[N(1 - (\frac{1}{n})^{N-1}) - \frac{n}{n-1}(1 - N(\frac{1}{n})^{N-1} + \right. \\ \left.(N-1)(\frac{1}{n})^N)\right] + \\ \frac{p^3}{12N^2(n^2-1)}(\frac{-1}{5n^{2k}} + \frac{1}{6})\left[N(1 - (\frac{1}{n^2})^{N-1}) - \right. \\ \left.\frac{n^2}{n^2-1}(1 - N(\frac{1}{n^2})^{N-1} + (N-1)(\frac{1}{n^2})^N)\right] + \\ \frac{\alpha\sigma_S^2}{6N^2(n-\alpha)}\left[N(1 - (\frac{\alpha}{n})^{N-1}) - \frac{n}{n-\alpha}(1 - N(\frac{\alpha}{n})^{N-1} + \right. \\ \left.(N-1)(\frac{\alpha}{n})^N)\right], \\ \qquad\qquad\qquad\qquad k > N-1 \end{cases} \tag{32}$$

(32) can be used to obtain σ_c^2 for the events H_1 ($\mathbf{W} = \mathbf{W}'$) by setting $k = 0$, H_{1b} ($\mathbf{W} \neq \mathbf{W}'$) by setting $k \neq 0$ and H_{1a} by setting $p = 0$. σ_c^3 for event H_{1b} proves to be greater than that for event H_{1a}. μ_c is larger for small $k > 0$ but converges to that for H_{1a}, as k increases. These observations justify our earlier remark that event H_{1b} is the worst case in terms of bigger probability errors than H_{1a} or H_4.

Although Bernoulli chaotic watermarks prove to be correlated for small $k > 0$ (see (28) bearing in mind that $\mathbf{W}'$ is a shifted version of $\mathbf{W}$), the Central Limit Theorem for random variables with small dependency [3] may be used in order to establish that c of (3) attains a Gaussian distribution, even for the event H_{3b} (assuming that N is sufficiently large). Furthermore, under the worst case assumption, both μ_c and σ_c^2, given by (30) and (32) sespectively, converge to a constant value for large k. For such k, $R_{WW}(k) = 0$ meaning that $E[W_i W_j] = E[W_i]E[W_j] = 1$. Thus, the terms of the sum (3) can be considered sufficiently independent and the distribution of c under event H_{1b} for $k \to \infty$ can be assumed normal. In such a case, $P_{fa,H_{3b}}$ can be estimated using the limit values of μ_c and σ_c^2 as $k \to \infty$. This is done since convergence is actually quickly reached leading to a very small probability (for large N) of actually facing a case where k is rather small. P_{fr} values are estimated using the values of μ_c and σ_c^2 for $k = 0$ and ROC curves are evaluahed from (10).

4. PSEUDORANDOM WATERMARKS

Most watermarking schemes proposed so far use a pseudorandom number generator in order to generate the watermark signal that will be embgdded in the host data. Samples generated by such functions can be accurately modeled as independent identically distributed (i.i.d.) random variables obeying a uniform distribution. In our case we will deal with zero-mean pseudorandom sequences distributed in the interval $[-0.5, 0.5]$. The zero mean and i.i.d. assumptions grand such sequences with a white spectrum. Obviously, pseudorandom signals of this type are wide-sense stationary and ergodic. Furthermore, for such watermarks, the terms of the sum (3) can be safely assumed to be sufficiently independent. Thus, due to the Central Limit Theorem, c attains a Gaussian distribution for a sufaiciently large N.

By exploiting the above properties, one can easily obtain the following results for the watermark signal moments that appear in expressions (11), (12):

$$E[W_i^m] = \begin{cases} 0 & m \ \text{odd} \\ \frac{1}{(m+1)2^m} & m \ \text{even} \end{cases} \tag{33}$$

$$E[W_i^l W_j^m] = E[W_i^l]E[W_j^m] \tag{34}$$

Similar expressions can be derived for the moments involving more than two random variables. Using these equations, μ_c and σ_c^2 for a watermarking system based on pseudorandom watermarks can be calculated:

$$\mu_c = \begin{cases} \frac{p}{12} & \text{if } \mathbf{W} = \mathbf{W}' \\ 0 & \text{if } \mathbf{W} \neq \mathbf{W}' \\ 8 & \text{if } p = 0 \end{cases} \tag{35}$$

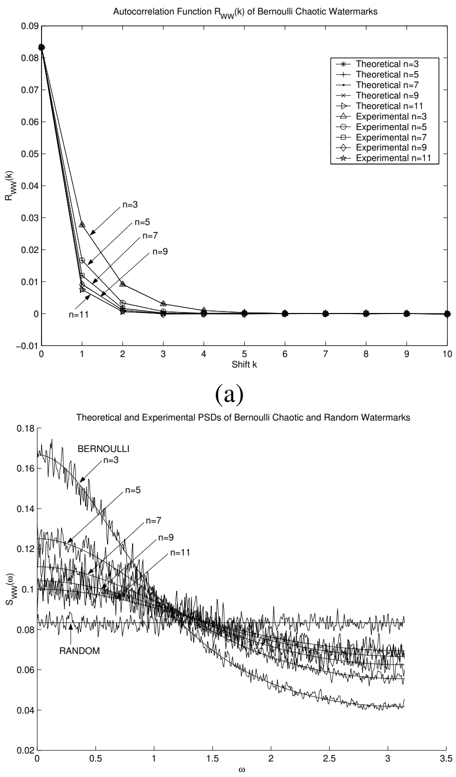
$$\sigma_c^2 = \begin{cases} \frac{1}{12N}(\mu_S^2 + \sigma_S^2 + \frac{p^8}{05}) & \text{if } \mathbf{W} = \mathbf{W}' \\ \frac{1}{12N}(\mu_S^2 + \sigma_S^2 + \frac{p^2}{11}) & \text{if } \mathbf{W} \neq \mathbf{W}' \\ \frac{1}{12N}(\mu_S^2 + \sigma_S^2) & \text{if } p = 0 \end{cases} \tag{36}$$

By observing (35),(36), one concludes that c attains the same mean value for both events $\mathbf{W} \neq \mathbf{W}'$ and $p = 0$, while its variance for the first event is larger than that for the second, proving that the first event is the worst case.

5. EXPERIMENTAL RESULTS

Experimental verification of the theoretical analysis results is reported. During theoretical analysis, discrete-time continuous-valued signals have been considered. Experimental verification involves losc of accuracy, since all simulated signals must be discrete-valued (quantized). Howevlr, as it will be shown in the sequel, experimental evaluations are in agreement with theoretical results.

Initially, experimentally evaluated statistical and spectral properties of the Bernoulli chaotic watermarks are compared with the analytical ones. Figures 2(a) and 2(b) illustrate the autocorrelation function $R_{WW}(k)$ with respect to shift k and the power spectral density (psd) $S_{WW}(\omega)$ of the n-way Bernoulli shift generated chaotic watermarks for different values of n (3,5,7,1,11). The experimental curves are almost identical with the theoretical ones in the case of $R_{WW}(k)$, whereas they converge to the latter in the case of $S_{WW}(\omega)$. The psd of random white watermarks (both analytical and empirical) is also shown in Figure 2(b) for comparison purposes. It is easily observed that the Bernoulli chaotic watermark specyrum is lowpass for small values of n and it converges to that of random white watermarks as n incrtases significantly. Their autocorrelation function also converges to that of random white watermarks, i.e. to a Dirac delta function, with increasing n. Both observations justify our earlier remark about the controllable spectral/ correlation properties of the Bernoulli chaotic watermarks. Based on these observations, Bernoulli chaotic watermarks generated for the above mentioned values of n are used in all subsequent experiments to evaluate the influence of n on the system performance and compare the achieved performance with that of random white watermarks.



(a)

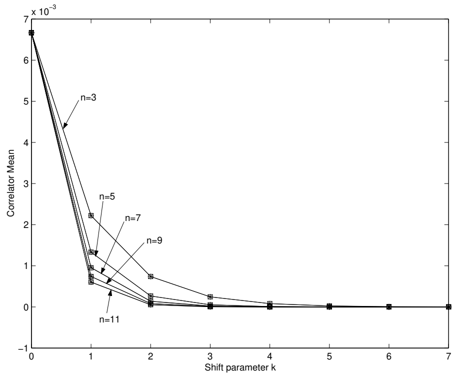
(b)

Fig. 2. Theoretical and experimental evaluation of: (a) the autocorrelation function, (b) the power spectral density of Bernpulli chaotic watermarks for different values of n.

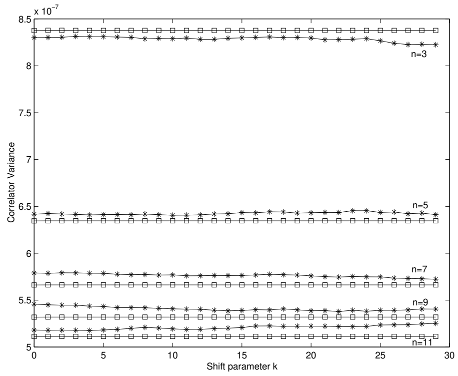
In order to empirically verify the watermarking system detection reliability in terms of ROC curves, the system is fed lith a music audio signal of 10sec duration, sampled at 44.1kHz with 16 bits per sample ($N = 441000$). Since most real signals are lowpass in nature, ihe audio signal is assumed to comply with the signal model of (15) for $\alpha = 0.95$, a fact that has also been verified experimentally. To better comply with the model of (15) and, thus, achieve better accuracy and performance, the system is also fed with a random white uniformly-distributed signal S of zero mean value ($N = 10^6$) that has been pre-filtered with an IIR filter $H(z) = \frac{4-\beta}{1-\beta z^{-1}}$. Such prefiltering generates a signal exhibiting an autocorrelation function of the form $R_{SS}(k) = \frac{1-\beta}{1+\beta}\sigma_S^2\beta^k$ which is identical to (15) for $\mu_S = 0$, $\beta = \alpha$ and filtered signal variance $\frac{1-\beta}{1+\beta}\sigma_S^2$. The experimental results obtained for either input signal converge to the theoretical onrs with similar accuracy. Slightly better performance in terms of probability errors is obtained mn the case of perfect validity of the signal model. The system performance is measured for both Bernoulli chaotic watermarks and random white ones to enable their comparison. The watermark strength p is evaluated under the constraint that the watermarked signal has SMR=50dB. A total number of 10000 keys has been used in the experiments. ROC curve estimation in subsequent analysis is performed under the worst case assumption, when hypothesis H_1 (for P_{va} evaluation) corresponds to the signal being watermarked by a different watermark than the one used in detection (event H_{1b}). In this case, the correlation variance is larger than the onw exhibited when the signal is not watermarked, leading to bigger errors. Empirical ROC curve estimation is performed by approximating the correlator distribution with a Gaussian distribution and using (6), (7) and (10) to estimate P_{fa} and P_{fr} values for varying T within $[\mu_{H_{1b}}, \mu_{H_6}]$.

As shown theoretically, the dependency of the correlation mean and variance on shift k, defined in Section 3, will also be experimentayly investigated. Figures 3(a) and (b) show the theoretical and empirical curves for the mean and variance respectively for varipus n, when the input signal is the lowpass filtered random signal. The mean curves are almost identical whereas accuracy problems are reflected in the empirical estimation of the variance curves which slightly differ from the theoretical ones. When $k = 0$, the detected watermark is the embedded one ($\mathbf{W} = \mathbf{W}'$). The main observation here is that convergence to the respective mean and variance values for large k ($\mathbf{W}$ and $\mathbf{W}'$ are practically uncorrelated for large k) is quickly performed after at most 6 shifts. This leads to the conclusion that the probability of detecting a correlated watermark to the embedded one, than the actual one, is significantly small. Subsequent analysis will be made under convergence assumption ($k \to \infty$) for the Bernoulli chaotic watermarks, a case under which the respective correlator detector attains a Gaussian distribution.

The achieved ROC curves under no attack, for varying n and the audio signal as input, are shown in Figure 4. The coincidence of the theoretical and empirical ones is once more noted. Respective curves are also illustrated for random white watermarks. It is seen that the latter attain the best performance with respect to the overall error probability. However, as n increases, the performance of Bernoulli



(a)



(b)

Fig. 3. Theoretical (square) and empirical (x symbol) correlation (a) mean and (b) variance curves for Bernoulli chaotic watermarks with respect to shift k for various n.

chaotic watermarks is quickly converging to that of random ones. This is attributed to our earlier observation that, as n increases, the spectrum of Bernoulli chaotic watermarks is transforming from lowpass to white, thus converging to that of random white watermarks.

Finally, the correlation's Gaussian probability density function, even under attacks, has been empirically verified using the Kolmogorov-Smirnoff criterion.

6. CONCLUSIONS

The n-way Bernoulli shift generated chaotic watermarks are introduced and their statistical properties relevant to a watermarking application are investigated to determine whether they present secure watermarks. Furthermore, statistical analysis of the properties of the employed correlator detector is undertaken under no distortions in order to examine the presented watermarking system detection reliability. Similar investigation is performed for random white watermarks, for comparison purposes. Bernoulli chaotic watermarks attain controllable spectral/correlation properties dependent on the value of n. Thus, Bernoulli chaotic watermarks can be easily constructed with the appropriate spectral properties according to the prospective application or

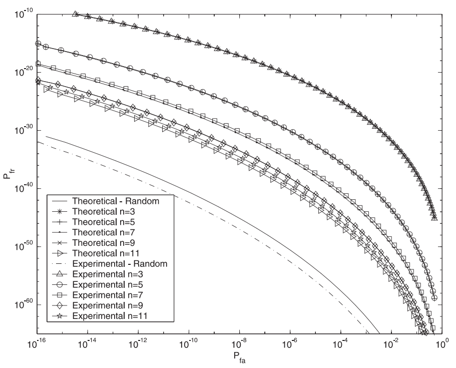


Fig. 4. Theoretical and empirical ROC curves for Bernoulli chaotic watermarks after no attack.

potential distortion, while preserving their invariant probability density. Random watermarks should be preprocessed to exhibit similar efficiency. Such preprocessing modifies their initial probability distribution which enables the risk of possible perceptibility. Once more, the importance of the watermark spectrum in watermarking applications is emphasized. Future research effort will be devoted to the investigation of alternative chaotic maps for the generation of chaotic watermarks and the analysis of binary chaotic watermarks, obtained after proper thresholding of the presented continuous-valued ones.

7. REFERENCES

[1] Special issue on copyright & privacy protection. *IEEE Journal on Selected Areas in Communications*, 16(4), May 1998.

[2] Special issue on identification & protection of multimedia information. *Proceedings of the IEEE*, 87(7), 1999.

[3] Patrick Billingsley. *Probability and Measure*. Wiley, 1995.

[4] G. Depovere, T. Kalker, and J.-P. Linnartz. Improved watermark detection reliability using filtering before correlation. In *Proc. of ICIP'98*, volume I, pages 430–434, 4-7 October 1998.

[5] J.R. Hernandez and F. Perez-Gonzalez. Statistical analysis of watermarking schemes for copyright protection of images. *Proceedings of the IEEE*, 87(7):1142–1166, July 1999.

[6] S.H. Isabelle and G.W. Wornell. Statistical analysis and spectral estimation techniques for one-dimensional chaotic signals. *IEEE Trans. on Signal Processing*, 45(6):1495–1506, June 1997.

[7] T. Kalker, J-P. Linnartz, and G. Depovere. On the reliability of detecting electronic watermarks in digital images. In *Proc. of EUSIPCO'98*, Rodos, Greece, September 1998.

[8] J.-P. Linnartz, T. Kalker, and G. Depovere. Modeling the false alarm and missed detection rate for electronic watermarks. In *Proc. of 2nd Information Hiding Workshop*, pages 329–343, Oregon, USA, April 1998.

[9] A. Nikolaidis and I. Pitas. Comparison of different chaotic maps with application to image watermarking. In *Proc. of ISCAS'00*, Geneva, Switzerland, 28-31 May 2000. to appear.

[10] N. Nikolaidis and I. Pitas. Robust image watermarking in the spatial domain. *Elsevier Signal Processing, Sp. Issue on Copyright Protection and Access control*, 66(3):385–403, May 1998.

[11] R. Rovatti, G. Setti, and G. Mazzini. Chaotic complex spreading sequences for asynchronous ds-cdma - part ii: Some theoretical performance bounds. *IEEE Trans. on Circuits and Systems I*, 45(4):496–506, April 1998.

[12] H.G. Schuster. *Deterministic Chaos: An Introduction*. Physik-Verlag, 1984.

[13] S. Tsekeridou, N. Nikolaidis, N. Sidiropoulos, and I. Pitas. Copyright protection of still images using self-similar chaotic watermarks. In *Proc. of ICIP'00*, Vancouver, Canada, 10-13 September 2000. to appear.

[14] G. Voyatzis and I. Pitas. Chaotic watermarks for embedding in the spatial digital image domain. In *Proc. of ICIP'98*, volume II, pages 432–436, Chicago, USA, 4-7 October 1998.

A. JOINT MOMENTS OF N-WAY BERNOULLI SHIFT GENERATED CHAOTIC WATERMARKS

The autocorrelation function $R_{WW}(k)$ of the Bernoulli chaotic watermarks, assuming that W_i and $W_i' = W_{i+k}$ are random variables and bearing in mind that the one is derived by the other, using (20), and that their joint distribution $f_{W_i W_{i+k}}$ is given by (25), takes the form:

$$\begin{aligned} R_{WW}(k) &= E[W_i W_{i+k}] = \int_x \int_y xy f_{W_i W_{i+k}}(x,y)dxdy \\ &= \int_x \int_y xy f_{W B_n^k(W)}(x,y)dxdy \\ &= \int_x \int_y xy\delta(y - B_n^k(x))dxdy \\ &= \int_x xB_n^k(x)dx \end{aligned} \quad \text{(A-1)}$$

Since the n-way Bernoulli shift map is piecewise linear in intervals of the range $[-0.5, 0.5]$, as shown in (18), the integral of (A-1) is restated as follows:

$$R_{WW}(k) = \frac{1}{12n^k} \quad \text{(A-2)}$$

Subsequent joint moments are evaluated in the same way:

$$E[W_i^2 W_i'] = E(W_i^2 W_{i+k}) = 0 \quad \text{(A-3)}$$

$$E[W_i W_i'^2] = E[W_i W_{i+k}^2] = 0 \quad \text{(A-4)}$$

$$E[W_i^2 W_i'^2] = E[W_i^2 W_{i+k}^2]\frac{1}{144} + \frac{1}{180n^{2k}} \quad \text{(A-5)}$$

$$E[W_i W_i' W_j] = E[W_i W_{i+k} W_{i+l}] = 0 \quad \text{(A-6)}$$

$$E[W_i W_j W_j'] = E[W_i W_{i+l} W_{i+k+l}] = 0 \quad \text{(A-7)}$$

$$\begin{aligned} &E[W_i W_i' W_j W_j'] = E[W_i W_{i+k} W_{i+l} W_{i+k+l}] \\ &= \tfrac{-1}{120n^{2k+2l}} + \tfrac{1}{144n^{2\min(k,l)}} + \tfrac{1}{72n^{2\max(k,l)}} \end{aligned} \quad \text{(A-8)}$$

$$\begin{aligned} &E[W_i W_{i+k} W_{i+m} W_{i+l}] \\ &= \tfrac{-1}{120n^{3\max(k,m,l)-(\min(k,m,l)+\mathrm{med}(k,m,l))}} + \\ &\tfrac{1}{144n^{\max(k,m,l)+\min(k,m,l)-\mathrm{med}(k,m,l)}} + \\ &\tfrac{1}{72n^{\max(k,m,l)-\min(k,m,l)+\mathrm{med}(k,m,l)}} \end{aligned} \quad \text{(A-9)}$$

In (A-9), med denotes the median operator.