Statistical Analysis of a Watermarking System based on 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

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

*Corresponding Author, Tel.:+30-31-996304, Fax: +30-31-996304, *e-mail: pitas@zeus.csd.auth.gr*

Abstract

The paper deals with the statistical analysis of the behaviour of a blind copyright protection watermarking system based on chaotic watermark signals generated by n-way Bernoulli shift maps. The analysis involves theoretical evaluation of the system detection reliability, when a correlator detector is used. The effect of distortions (lowpass filtering, noise corruption of the watermarked data) on the detection reliability is also theoretically investigated. 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 two-fold: (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 renders them ideal for a variety of applications. Bernoulli watermarks can be generated with lowpass spectral properties to withstand lowpass attacks. When no distortions are to be inflicted, white spectrum Bernoulli watermarks can be generated so that their performance converges to that of random watermarks. Experimental verification of the theoretical analysis results has been performed as well.

Keywords

Statistical analysis, watermarking, copyright protection, Bernoulli shift chaotic map

I. 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. Data hiding usually involves the use of secret keys possessed only by owners or authorized users. In order to verify the multimedia content owner and thus protect his copyrights, 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 [1]-[3].

The basic requirements of an efficient copyright protection watermarking system are numerous and equally vital [3], [4]. The first requirement is watermark imperceptibility which is translated to signal quality preservation. The system should further attain robustness against a variety of attacks, intentional or not, which still preserve sufficient signal quality. It is generally agreed that imperceptibility and robustness are two conflicting requirements. Furthermore, watermarks should be secure, meaning that only the owner or authorized user should be able to detect the watermark. Statistical watermark removal or detection by unauthorized persons should be impossible. Finally, the system should be characterized by sufficient detection reliability, i.e., it should attain sufficiently small probabilities of false alarm and false rejection. Its non- or quasi-invertibility is also considered of significance [5]. In many cases, blind watermarking is also a requirement meaning that the original image should not be used during the detection phase.

Watermarking has recently become a very active research area, a fact established by the numerous methods dealing with the watermarking of audio [6], image [2], [7]-[11] or video content [12]-[16] that have appeared in the literature to date. They are distinguished in two classes, with respect to the embedding and detection domain, namely, the spatial-domain [2], [6], [7] and the transform-domain methods. In the latter case, embedding is performed in a number of transform domains, attempting to exploit their properties mainly for watermark imperceptibility and robustness: DCT [9], [12], [15], [17], DFT [18], [19], Fourier-Mellin [20], [21], DWT [12], [16], [22]-[25] or fractal-based coding domain [26], [27]. Overview papers on existing multimedia watermarking methods may be found in [28], [29]. Many approaches adopt principles from spread spectrum communications in their watermarking system model [15], [30]. For copyright protection purposes, blind watermarking is the most desirable. Recent methods exploit principles of the human auditory/visual system (HAS, HVS) to attain improved watermark imperceptibility [4], [12], [23], [31]. Furthermore, the main trend is to use

pseudo-random number generators in order to construct (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. Gold or m-sequences are also used in watermarking systems due to their good correlation properties. Their main disadvantage is that only a small number of different watermarks can be generated. To make things worse, the watermark sequence can be reconstructed by a small number of samples using linear regression methods [32]. The most widely used detector is the correlator, which is optimal for signals modeled as Additive White Gaussian Noise (AWGN) [33], [34]. A final issue on watermarking systems is their robustness against a variety of unintentional or malicious attacks including lowpass/highpass distortions, compression, noise corruption, geometric distortions. An overview of possible attacks and the limitations of many current approaches is given in [5], [30], [35].

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 in terms of detection reliability by addressing the problem in a communication framework [1], [33], [36]. In these papers the statistic properties of correlator detectors, among others, are contemplated, under certain assumptions for the image model, when random watermarks are used. Specifically in [33], [36], the authors investigate the performance of both white and lowpass-filtered random watermarks concluding that the former are ideal when no distortions are inflicted on the image while the latter better withstand lowpass distortions. They also propose using a whitening filter prior to correlation to achieve optimum detection when the channel (image) cannot be modeled as AWGN.

This paper deals with the statistical analysis of the behaviour of a blind copyright protection watermarking system based on chaotic watermark signals generated by n-way Bernoulli shift maps. Chaotic watermarks have been only recently introduced [37], [38], [39] 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 effect

of distortions (lowpass filtering, noise corruption of the watermarked data) on the detection reliability is also theoretically investigated. 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 two-fold: (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 white ones with the additional feature of controllable spectral/correlation properties, a fact that renders them ideal for a variety of applications. Bernoulli watermarks can be generated with lowpass spectral properties to withstand lowpass attacks. When no distortions are to be inflicted, white spectrum Bernoulli watermarks can be generated so that their performance converges to that of random watermarks.

The paper is organized as follows. In Section II, the watermarking system model is presented in terms of embedding and detection procedures and assumptions about the signal model are made. Section III 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 IV presents respective analysis for random white watermarks. Section V is devoted to the investigation of the influence of simple attacks, such as noise addition or linear lowpass filtering, on the system detection reliability, when watermarks generated by n-way Bernoulli shifts as well as pseudorandom watermarks are used. In Section VI, experimental verification of the theoretical analysis results is reported. Section VII summarizes the conclusions drawn by the presented statistical analysis and comments on potential future research efforts.

II. Watermarking system model

Let X_i , $i = 1, 2, ..., N$, be samples of the 1-D continuous valued host signal $\mathbf{X}$ of length N. Let also V_i , $i = 1, 2, ..., N$, 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 the previous formula, K denotes the watermark key that should be known only to the person that generates the watermark, i.e., the copyright owner. The watermark signal is assumed to be zero mean, i.e., $E[V_i] = 0$. This assumption ensures that the watermark embedding does not change the host signal mean value, thus providing watermark imperceptibility and additional robustness against unauthorized detection. Furthermore, as will be seen later in this section, zero-mean watermarks result in better detection performance. We assume that the watermark $\mathbf{V}$ is embedded additively to the host signal $\mathbf{X}$, 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: the watermark $\mathbf{W}'$ is indeed embedded in the signal $\mathbf{S}'$ under investigation.
- H_1: the signal under investigation does not host the watermark $\mathbf{W}'$.

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 $H_1 = H_{1a} \cup H_{1b}$ 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} mentioned above can be summarized in the following formula:

$$\mathbf{S}' = \mathbf{S} + p\mathbf{W} \tag{3}$$

For $p = 0$, expression (3) 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 $\mathbf{W} \neq \mathbf{W}'$, expression (3) represents 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:

$$c = \frac{1}{N}\sum_{i=1}^{N} S_i' W_i' = \frac{1}{N}\sum_{i=1}^{N}(S_i W_i' + p W_i W_i') \tag{4}$$

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):

$$P_{fa}(T) = \text{Prob}\{c > T | H_1\} \tag{5}$$

$$P_{fr}(T) = \text{Prob}\{c < T | H_0\} \tag{6}$$

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 :

$$P_{fa}(T) = \int_{T}^{\infty} f_{H_1}(t)dt \tag{7}$$

$$P_{fr}(T) = \int_{-\infty}^{T} f_{H_0}(t)dt \tag{8}$$

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

By solving (7), (8) 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, the probability density function f_{H1} can be expressed in terms of the probability density functions $f_{H_{1a}}$ and $f_{H_{1b}}$ of c as follows:

$$f_{H1} = p_H f_{H_{1a}} + (1 - p_H) f_{H_{1b}} \tag{9}$$

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

$$P_{fa}(T) = p_H P_{fa,H_{1a}}(T) + (1-p_H) P_{fa,H_{1b}}(T) \tag{10}$$

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 will be studied in this paper, i.e., the sequences generated by n-way Bernoulli shift maps and the pseudorandom sequences, f_{H_0}, $f_{H_{1a}}$, $f_{H_{1b}}$ are normal distributions (for justification, see Sections III,IV). 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 (10), 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:

$$P_{fa} = \frac{1}{2}\left[1 - \mathrm{erf}\left[\frac{\sqrt{2}\sigma_{H_0}\mathrm{erf}^{-1}(2P_{fr}-1) + \mu_{H_0} - \mu_{H_{1b}}}{\sqrt{2}\sigma_{H_{1b}}}\right]\right] \tag{11}$$

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_c^2 for both events H_0 ($\mathbf{W}' = \mathbf{W}$) and H_1 ($\mathbf{W}' \neq \mathbf{W}$ or $p = 0$).

$$\mu_c = E[c] = E\left[\frac{1}{N}\sum_{i=1}^{N}(S_i W_i' + p W_i W_i')\right] = \frac{1}{N}\sum_{i=1}^{N} E[S_i]E[W_i'] + \frac{1}{N}\sum_{i=1}^{N} pE[W_i W_i'] \tag{12}$$

$$\begin{aligned}
\sigma_c^2 &= E[c^2] - E[c]^2 = E\left[\left(\frac{1}{N}\sum_{i=1}^{N}(S_i W_i' + p W_i' W_i)\right)^2\right] - \mu_c^2 \qquad (13)\\
&= \frac{1}{N^2}E\left[\sum_{i=1}^{N}(S_i W_i' + p W_i' W_i)^2 + \sum_{i=1}^{N}\sum_{j=1, j\neq i}^{N}(S_i W_i' + p W_i' W_i)(S_j W_j' + p W_j' W_j)\right] - \mu_c^2\\
&= \frac{1}{N^2}\left[\sum_{i=1}^{N}\left(E[S_i^2]E[{W'}_i^2] + p^2 E[{W'}_i^2 W_i^2] + 2pE[S_i]E[W_i {W'}_i^2]\right) + \sum_{i=1}^{N}\sum_{j=1, j\neq i}^{N}\Big(E[S_i S_j]E[W_i' W_j']\right.\\
&\quad \left. + pE[S_i]E[W_i' W_j W_j'] + pE[S_j]E[W_i W_j' W_i'] + p^2 E[W_i W_j W_i' W_j']\Big)\right] - \mu_c^2
\end{aligned}$$

The obviously assumed statistical independence of the watermark and host signals, $\mathbf{W}$, $\mathbf{S}$ has been exploited in order to derive the previous formulas. 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 (13) have been eliminated, a fact that suggests that zero mean watermarks attain a superior performance.

By examining (12), (13), one can easily conclude that the moments $E[S_i]$, $E[S_iS_j]$, $E[W_i]$, $E[W_iW_i']$, $E[W_iW_j'W_i']$, $E[W_iW_jW_i'W_j']$ 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 will be adopted:

$$\mu_S = E[S_i] \quad \forall i \quad i = 1 \dots N \tag{14}$$

$$E[S_iS_{i+k}] = \Gamma_{S,S}(k) \quad \forall i \quad i = 1 \dots N \tag{15}$$

Furthermore, a first order separable autocorrelation function model will be assumed [40]:

$$\Gamma_{S,S}(k) = \mu_S^2 + \sigma_S^2 \alpha^k, k \geq 0 \tag{16}$$

where σ_S^2 is the signal variance:

$$\sigma_S^2 = E[S_i^2] - E[S_i]^2 \tag{17}$$

and α a real-valued constant typically equal to $\alpha = 0.9, \cdots, 0.99$. 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 VI.

III. Watermarks generated by n-way Bernoulli shift maps

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

$$\mathcal{B}_n : [0, 1] \to [0, 1]$$

$$r' = B_n(r) = nr (\text{mod } 1) \tag{18}$$

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:

$$W_{i+1} = B_n(W_i) = nW_i (\text{mod } 1) \quad i = 1 \dots N \tag{19}$$

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 [41], [42] 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 (30)), 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 the generated sequence should be subtracted, thus leading to a map defined in the interval $[-0.5, 0.5]$

$$\mathcal{B}_n : [-0.5, 0.5] \rightarrow [-0.5, 0.5]$$

$$W_{i+1} = B_n(W_i) = n(W_i + 0.5)(\text{mod } 1) - 0.5 = \tag{20}$$

$$= \begin{cases} n(W_i + 0.5) - 0.5 & -0.5 \leq W_i \leq \frac{1}{n} - 0.5 \\ n(W_i + 0.5 - \frac{1}{n}) - 0.5 & \frac{1}{n} - 0.5 < W_i \leq \frac{2}{n} - 0.5 \\ \vdots & \vdots \\ n(W_i + 0.5 - \frac{n-1}{n}) - 0.5 & \frac{n-1}{n} - 0.5 < W_i \leq 0.5 \end{cases}$$

The n-way Bernoulli shift maps for $n = 3$ and 12 are shown in Figure 1a. Watermark signals generated by n-way Bernoulli shift maps will be called Bernoulli chaotic watermarks in the rest of this paper. The following formula for 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 [42]:

$$W_{i+k} = n^k(W_i + 0.5)(\text{mod } 1) - 0.5 \quad k > 0 \tag{21}$$

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:

$$W_{i+k} = B_n^k(W_i) = B_{n^k}(W_i) \quad k > 0 \tag{22}$$

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 [8], [43], [44]. 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 any two randomly-chosen distinct, irrational starting points (watermark keys), then one of the following three cases may occur:

- *Case 1*: The two watermarks are parts of the same chaotic orbit. This happens, if the starting points belong to the same chaotic orbit themselves. Due to this, a certain degree of correlation exists between $\mathbf{W}$ and $\mathbf{W}'$. Furthermore, crosscorrelation expressions between $\mathbf{W}$ and $\mathbf{W}'$ become autocorrelation ones.
- *Case 2*: The two watermarks belong to different chaotic orbits. In this case, they may be assumed independent, just as two distinct pseudorandom watermarks are. However, samples W_i of the same watermark $\mathbf{W}$ are correlated with each other, since they are produced by iterating the same map on the same initial condition, a statement which is not valid for samples belonging to the same pseudorandom sequence.
- *Case 3*: The two watermarks belong to eventually the same chaotic orbit. This happens when the map is initialized with two distinct irrational numbers, not belonging to the same chaotic orbit, but the map iteration on those eventually leads to the same chaotic orbit after a certain number of iterations. Then, partial correlation may be observed between different watermarks. There might be seldom cases of two different watermarks differing only in the first few samples.

If two different watermarks are derived by initiating the map with two randomly chosen irrational numbers, there is no apriori knowledge on which of the above three cases will be valid. Since there is no possibility to control the occurrence of Cases 2 and 3 above, by appropriately selecting initial points during the watermark generation process, while this possibility exists for Case 1 (we just have to initialize the map with two irrational numbers belonging to the same chaotic orbit), extensive system performance analysis will be pursued for this case only. However, to give the reader a better picture of a watermarking system based on Bernoulli chaotic watermarks, both other cases will be briefly

commented in this Section.

Starting the analysis with Case 1, 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 W_1, W_1', both belonging to the same chaotic orbit, there will always be an integer $k > 0$ such that:

$$W_1' = B_n^k(W_1) \quad \text{OR} \quad W_1 = B_n^k(W_1') \tag{23}$$

Consequently, their samples W_i', W_i will also be associated through the following expression:

$$W_i' = W_{i+k} = B_n^k(W_i) \quad \text{OR} \quad W_i = W_{i+k}' = B_n^k(W_i'), \quad \forall i \quad i = 1 \dots N \tag{24}$$

Furthermore, arbitrary samples W_j', W_i ($|i-j| = l$) are associated as follows ($k > 0$, $l > 0$):

$$W_j' = W_{i+l}' = W_{i+k+l} = B_n^{k+l}(W_i) \quad \text{OR} \quad W_i = W_{j+l} = W_{j+k+l}' = B_n^{k+l}(W_j') \quad \forall i,\ j \quad i,j = 1 \dots N \tag{25}$$

The previous corollaries will be used extensively in the rest of the paper for the derivation of the moments of Bernoulli chaotic watermarks. A schematic representation of the above expressions can be seen in Figure 1b. By exploiting the fact that the uniform distribution is an invariant density of the Bernoulli maps, one can thus calculate the m-order moments for W_i:

$$E[W_i^m] = \int_{-0.5}^{0.5} x^m f(x) dx = \begin{cases} 0 & m \quad odd \\ \frac{1}{(m+1)2^m} & m \quad even \end{cases} \tag{26}$$

For the evaluation of the joint moments of two watermark signals $\mathbf{W}$, $\mathbf{W}'$ that appear in expressions (12), (13), 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 equations (23) and (24), one can easily conclude that the joint distribution $f_{W_i W_i'}(x,y)$ is equivalent to the joint distribution $f_{W_i B_{n^k}(W_i)}(x,y)$. Thus, the value of the joint distribution is 1 for (x,y) pairs for which $y = B_{n^k}(x)$ and 0 elsewhere:

$$f_{W_i W_i'}(x,y) = f_{W_i W_{i+k}}(x,y) = f_{W_i B_{n^k}(W_i)}(x,y) = \delta(y - B_{n^k}(x)) \tag{27}$$

where $\delta(x)$ is the Dirac delta function. Following a similar approach, one can derive analogous ex-

pressions for the other joint distributions mentioned above:

$$f_{W_i W_i' W_j'}(x,y,z) = f_{W_i W_{i+k} W_{i+k+l}}(x,y,z) = \delta(y - B_{n^k}(x))\delta(z - B_{n^{l+k}}(x)) \tag{28}$$

$$f_{W_i W_j W_i' W_j'}(x,y,z,w) = f_{W_i W_{i+l} W_{i+k} W_{i+k+l}}(x,y,z,w) = \delta(y - B_{n^l}(x))\delta(z - B_{n^k}(x))\delta(w - B_{n^{l+k}}(x)) \tag{29}$$

Using the above expressions, the joint moments that appear in expressions (12), (13) 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:

$$R_{WW}(k) = E[W_i W_{i+k}] = \frac{1}{12n^k} \quad k \geq 0 \tag{30}$$

whose derivation is presented in Appendix A. By observing (30), 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 $k = 0$:

$$S_W(\omega) = \sum_{k=-\infty}^{\infty} R_{WW}(k)e^{-j\omega k} = R_{WW}(0) + \sum_{k=1}^{\infty} R_{WW}(k)(e^{j\omega k} + e^{-j\omega k}) = \frac{1}{12}\frac{n^2 - 1}{n^2 - 2n\cos(\omega) + 1} \tag{31}$$

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 converging 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 the mean and the variance of the correlation c for a watermarking system based on Bernoulli chaotic watermarks. The

assumption that the watermark $\mathbf{W}'$ under investigation is associated to the watermark $\mathbf{W}$ through equation (24) is used in the evaluation procedure:

$$\mu_c = E[c] = \frac{1}{N}\sum_{i=1}^{N} E[S_i]E[W_i'] + \frac{1}{N}\sum_{i=1}^{N} pE[W_i W_i'] = \frac{p}{12n^k} \tag{32}$$

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

$$\mu_c = \begin{cases} \frac{p}{12} & \text{if } \mathbf{W} = \mathbf{W}' \ \ (k=0) \\ \frac{p}{12n^k} & \text{if } \mathbf{W} \neq \mathbf{W}' \ \ (k \neq 0) \\ 0 & \text{if } p = 0 \end{cases} \tag{33}$$

The variance σ_c^2 of the correlation c can be evaluated using a similar procedure:

$$\sigma_c^2 = \begin{cases} \frac{1}{12N}\left[\sigma_S^2 + \mu_S^2 + p^2(\frac{1}{12} - \frac{1}{60n^{2k}})\right] + \frac{p^2 k}{144N^2}(\frac{1}{n^2})^k(2N-(k+1)) + \\ \frac{\mu_S^2}{6N^2(n-1)}\left[(N - k(\frac{1}{n})^k - (N-k)(\frac{1}{n})^{N-1}) - \right. \\ \qquad \left. \frac{n}{n-1}(1 - k(\frac{1}{n})^k + k(\frac{1}{n})^{k+1} - (N-k)(\frac{1}{n})^{N-1} + (N-k-1)(\frac{1}{n})^N)\right] + \\ \frac{\alpha\sigma_S^2}{6N^2(n-\alpha)}\left[(N - k(\frac{\alpha}{n})^k - (N-k)(\frac{\alpha}{n})^{N-1}) - \right. \\ \qquad \left. \frac{n}{n-\alpha}(1 - k(\frac{\alpha}{n})^k + k(\frac{\alpha}{n})^{k+1} - (N-k)(\frac{\alpha}{n})^{N-1} + (N-k-1)(\frac{\alpha}{n})^N)\right] + \\ \frac{p^2}{12N^2(n^2-1)}(\frac{-1}{5n^{2k}})\left[(N - k(\frac{1}{n^2})^k - (N-k)(\frac{1}{n^2})^{N-1}) - \right. \\ \qquad \left. \frac{n^2}{n^2-1}(1 - k(\frac{1}{n^2})^k + k(\frac{1}{n^2})^{k+1} - (N-k)(\frac{1}{n^2})^{N-1} + (N-k-1)(\frac{1}{n^2})^N)\right] + \\ \frac{p^2}{72N^2(n^2-1)}\left[(N(1 + (\frac{1}{n^2})^k) - 2k(\frac{1}{n^2})^k - 2(N-k)(\frac{1}{n^2})^{N-1}) - \right. \\ \qquad \left. \frac{n^2}{n^2-1}(1 - (k-1)(\frac{1}{n^2})^k + k(\frac{1}{n^2})^{k+1} - 2(N-k)(\frac{1}{n^2})^{N-1} + 2(N-k-1)(\frac{1}{n^2})^N)\right], \quad k \leq N-1 \\ \\ \frac{1}{12N}\left[\sigma_S^2 + \mu_S^2 + p^2(\frac{1}{12} + \frac{N}{12n^{2k}} - \frac{1}{10n^{2k}})\right] + \\ \frac{\mu_S^2}{6N^2(n-1)}\left[N(1 - (\frac{1}{n})^{N-1}) - \frac{n}{n-1}(1 - N(\frac{1}{n})^{N-1} + (N-1)(\frac{1}{n})^N)\right] + \\ \frac{p^2}{12N^2(n^2-1)}(\frac{-1}{5n^{2k}} + \frac{1}{6})\left[N(1 - (\frac{1}{n^2})^{N-1}) - \frac{n^2}{n^2-1}(1 - N(\frac{1}{n^2})^{N-1} + (N-1)(\frac{1}{n^2})^N)\right] + \\ \frac{\alpha\sigma_S^2}{6N^2(n-\alpha)}\left[N(1 - (\frac{\alpha}{n})^{N-1}) - \frac{n}{n-\alpha}(1 - N(\frac{\alpha}{n})^{N-1} + (N-1)(\frac{\alpha}{n})^N)\right], \quad k > N-1 \end{cases} \tag{34}$$

The above formula can be used to obtain the variance of c for the events H_0 ($\mathbf{W} = \mathbf{W}'$) by setting $k = 0$, H_{1b} ($\mathbf{W} \neq \mathbf{W}'$) by setting $k \neq 0$ and H_{1a} by setting $p = 0$. The variance of c for event H_{1b} proves to be greater than that for event H_{1a}. Its mean value 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_1.

Although Bernoulli chaotic watermarks, generated as described in Case 1, prove to be correlated for small $k > 0$ (see (30) bearing in mind that $\mathbf{W}'$ is a shifted version of $\mathbf{W}$), the Central Limit Theorem for random variables with small dependency [45] may be used in order to establish that c of (4) attains a Gaussian distribution, even for the event H_{1b} (assuming that N is sufficiently large). Furthermore, under the worst case assumption, both μ_c and σ_c^2, given by (32) and (34) respectively, converge to a constant value for large k. For such k, $R_{WW}(k) = 0$ meaning that $E[W_i W_j] = E[W_i]E[W_j] = 0$. Thus, the terms of the sum (4) 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, $P_{fa,H_{1b}}$ 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 evaluated from (11).

Now, let's assume occurrence of Case 2, i.e. two watermarks $\mathbf{W}$, $\mathbf{W}'$ belong to different chaotic orbits. Then, they may be assumed independent (e.g. $E[W_i W'_j] = E[W_i]E[W'_j] = 0$), and the watermarking system performance is independent of k, which now has no actual meaning. Although this case might be considered similar with that of pseudorandom watermarks, there is still a significant difference. Samples W_i of the same watermark $\mathbf{W}$ are actually correlated to each other, since they are derived from the iterative application of the same map on the same initial condition. Thus, their autocorrelation function will be given by (30), if k is substituted by l, i.e. the relative shift of the iterate indices between two samples of the same watermark. Consequently, their psd, $S_W(\omega)$, will be given again by (31). Also, the joint distributions between samples of the same watermark will have the same form as the ones given above (e.g. (27)), if W' terms are substituted by W and the indices differ. This could be further applied to the autocorrelation expressions of any order, summarized in Appendix A. In short, all the analytical expressions for the autocorrelations of any order will be valid for samples belonging to the same watermark. For example, $E[W_i^2 W_j^2] = \frac{1}{144} + \frac{1}{180n^{2l}}$, relevant to $E[W_i^2 W_i'^2]$, given in the Appendix. Joint moments between samples of different watermarks (crosscorrelation expressions) are derived in a straightforward manner, based on their independence. On the basis of

all these remarks, analytical expressions for μ_c and σ_c^2, for all events H_0 ($\mathbf{W}' = \mathbf{W}$), H_{1b} ($\mathbf{W}' \neq \mathbf{W}$) and H_{1a} ($p = 0$), can be easily derived by appropriately replacing the joint moment terms appearing in (12) and (13):

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

$$\sigma_c^2 = \begin{cases} \frac{1}{12N}\left[\sigma_S^2 + \mu_S^2 + \frac{p^2}{15}\right] + \\ \frac{\mu_S^2}{6N^2(n-1)}\left[N(1-(\frac{1}{n})^{N-1}) - \frac{n}{n-1}(1 - N(\frac{1}{n})^{N-1} + (N-1)(\frac{1}{n})^N)\right] + \\ \frac{p^2}{90N^2(n^2-1)}\left[N(1-(\frac{1}{n^2})^{N-1}) - \frac{n^2}{n^2-1}(1 - N(\frac{1}{n^2})^{N-1} + (N-1)(\frac{1}{n^2})^N)\right] + \\ \frac{\alpha\sigma_S^2}{6N^2(n-\alpha)}\left[N(1-(\frac{\alpha}{n})^{N-1}) - \frac{n}{n-\alpha}(1 - N(\frac{\alpha}{n})^{N-1} + (N-1)(\frac{\alpha}{n})^N)\right], & \mathbf{W} = \mathbf{W}' \\ \\ \frac{1}{12N}\left[\sigma_S^2 + \mu_S^2 + \frac{p^2}{12}\right] + \\ \frac{\mu_S^2}{6N^2(n-1)}\left[N(1-(\frac{1}{n})^{N-1}) - \frac{n}{n-1}(1 - N(\frac{1}{n})^{N-1} + (N-1)(\frac{1}{n})^N)\right] + \\ \frac{p^2}{72N^2(n^2-1)}\left[N(1-(\frac{1}{n^2})^{N-1}) - \frac{n^2}{n^2-1}(1 - N(\frac{1}{n^2})^{N-1} + (N-1)(\frac{1}{n^2})^N)\right] + \\ \frac{\alpha\sigma_S^2}{6N^2(n-\alpha)}\left[N(1-(\frac{\alpha}{n})^{N-1}) - \frac{n}{n-\alpha}(1 - N(\frac{\alpha}{n})^{N-1} + (N-1)(\frac{\alpha}{n})^N)\right], & \mathbf{W} \neq \mathbf{W}' \\ \\ \frac{1}{12N}\left[\sigma_S^2 + \mu_S^2\right] + \\ \frac{\mu_S^2}{6N^2(n-1)}\left[N(1-(\frac{1}{n})^{N-1}) - \frac{n}{n-1}(1 - N(\frac{1}{n})^{N-1} + (N-1)(\frac{1}{n})^N)\right] + \\ \frac{\alpha\sigma_S^2}{6N^2(n-\alpha)}\left[N(1-(\frac{\alpha}{n})^{N-1}) - \frac{n}{n-\alpha}(1 - N(\frac{\alpha}{n})^{N-1} + (N-1)(\frac{\alpha}{n})^N)\right], & p = 0 \end{cases} \tag{36}$$

The careful observation of (33) and (34), in comparison with (35) and (36), leads to the conclusion that the latter expressions are derived from the former ones, by either setting $k = 0$, i.e. $\mathbf{W} = \mathbf{W}'$, or $k \to \infty$, i.e. $\mathbf{W} \neq \mathbf{W}'$ (limit values of the former expressions), or $p = 0$. Thus, by generating different watermarks as in Case 1, using an appropriately large value of k (convergence condition of Case 1), different watermarks may be assumed independent. As a result, we are led from Case 1 to Case 2 and (35), (36) hold.

If Case 3 occurs, then we might have the worst case to deal with. Different watermarks may be different by only a few initial samples, and, thus, the crosscorrelation between them will be significant.

Theoretical evaluation of the crosscorrelation expressions and the watermarking system performance is a rather difficult task in this case. It is noted though that, as in Cases 1 and 2, the derived expressions for the autocorrelation function, the psd and the joint distributions will apply here, as well, for samples belonging to the same watermark signal.

As already mentioned earlier, further analysis of the watermarking system performance, when Bernoulli chaotic watermarks are used, will be subsequently pursued under Case 1 occurrence assumption only. It is noted that, if a system designer was to design a watermarking system based on Bernoulli chaotic watermarks, then the optimal choice for watermark generation would be Case 1. The reasons are that, firstly, watermark generation can be directly controlled by appropriately choosing irrational starting points of the same chaotic orbit. Secondly, the system performance could be controlled to be identical with that exhibited under Case 2 occurrence (two distinct watermarks are considered independent), if initial points are selected to be appropriately far apart (k is chosen to be large).

IV. Pseudorandom watermarks

Most watermarking schemes proposed so far use a pseudorandom number generator in order to generate the watermark signal that will be embedded 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 (4) can be safely assumed to be sufficiently independent. Thus, due to the Central Limit Theorem, c attains a Gaussian distribution for a sufficiently large N.

By exploiting the above properties, one can easily obtain the following results for the watermark

signal moments that appear in expressions (12), (13):

$$E[W_i^m] = \begin{cases} 0 & m \quad odd \\ \frac{1}{(m+1)2^m} & m \quad even \end{cases} \tag{37}$$

$$E[W_i^l W_j^m] = E[W_i^l]E[W_j^m] \tag{38}$$

Similar expressions can be derived for the moments involving more than two random variables. Using these equations, the mean value and the variance of the correlation c for a watermarking system based on pseudorandom watermarks can be calculated as follows:

$$\mu_c = \begin{cases} \frac{p}{12} & \text{if } \mathbf{W} = \mathbf{W}' \\ 0 & \text{if } \mathbf{W} \neq \mathbf{W}' \\ 0 & \text{if } p = 0 \end{cases} \tag{39}$$

$$\sigma_c^2 = \begin{cases} \frac{1}{12N}(\mu_S^2 + \sigma_S^2 + \frac{p^2}{15}) & \text{if } \mathbf{W} = \mathbf{W}' \\ \frac{1}{12N}(\mu_S^2 + \sigma_S^2 + \frac{p^2}{12}) & \text{if } \mathbf{W} \neq \mathbf{W}' \\ \frac{1}{12N}(\mu_S^2 + \sigma_S^2) & \text{if } p = 0 \end{cases} \tag{40}$$

By observing (39) and (40), 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.

V. Attacks

Attacks are operations, intentional or not, that limit the detection reliability of a watermarking system. A theoretical investigation of the influence of simple attacks, such as additive noise corruption or linear lowpass filtering, on the detection reliability of the presented watermarking system is further undertaken. For comparison purposes, similar analysis is performed when random white watermarks are used.

A. Noise Addition

The possibly watermarked signal $\mathbf{S}' = \mathbf{S} + p\mathbf{W}$ is assumed to be corrupted by additive random white i.i.d. noise ϵ uniformly distributed in the interval $[-\epsilon_r, \epsilon_r]$. ϵ has zero mean value $\mu_\epsilon = 0$ and

variance equal to $\sigma_\epsilon^2 = \epsilon_r^2/3$. $\mathbf{W}$ may be either a chaotic watermark or a random one. The case of noise corruption has been considered, since noise may be unintentionally inserted in a signal due to channel noise during transmission, or intentionally inserted aiming at destroying evidence of the embedded watermark and, thus, of copyright information, or increasing the artistic quality of the data. Detection, in the general case, involves estimation of the correlation between the noise corrupted and possibly watermarked signal $\mathbf{S}' + \epsilon$ and a watermark $\mathbf{W}'$ (equal to $\mathbf{W}$ or not), i.e.:

$$c_\epsilon = \frac{1}{N}\sum_{i=1}^{N}(S_i' + \epsilon_i)W_i' \tag{41}$$

The noise signal does not modify the correlator's Gaussian distribution since it is independent of the other signals. In order to determine the influence of noise addition on the system's detection reliability measured by (11), the mean value μ_{c_ϵ} and variance $\sigma_{c_\epsilon}^2$ of c_ϵ must be estimated:

$$\mu_{c_\epsilon} = E[c_\epsilon] = \frac{1}{N}\left[\sum_{i=1}^{N} E[S_i]E[W_i'] + \sum_{i=1}^{N} E[\epsilon_i]E[W_i'] + \sum_{i=1}^{N} pE[W_iW_i']\right] \tag{42}$$

For Bernoulli chaotic watermarks, (42) leads to:

$$\mu_{c_\epsilon} = \frac{p}{12n^k} \tag{43}$$

For random watermarks, we obtain:

$$\mu_{c_\epsilon} = \begin{cases} \frac{p}{12}, & \text{if } \mathbf{W} = \mathbf{W}' \\ 0, & \text{if } \mathbf{W} \neq \mathbf{W}' \text{ or } p = 0 \end{cases} \tag{44}$$

Its variance $\sigma_{c_\epsilon}^2$ is evaluated by:

$$\begin{aligned} \sigma_{c_\epsilon}^2 &= \frac{1}{N^2}E\left[\sum_{i=1}^{N}((S_i + pW_i + \epsilon_i)W_i')^2 + \sum_{i=1}^{N}\sum_{j=1, j\neq i}^{N}((S_i + pW_i + \epsilon_i)W_i')((S_j + pW_j + \epsilon_j)W_j')\right] - \mu_{c_\epsilon}^2 \\ &= \sigma_c^2 + \frac{\epsilon_r^2}{36} \end{aligned} \tag{45}$$

where σ_c^2 denotes the correlator variance under no distortions, given by (34) and (40) when Bernoulli chaotic watermarks or random watermarks are respectively used. By observing these equations, one may conclude that noise corruption is not a serious threat against a watermarking system's detection reliability, since it does not affect the mean value of the correlation and only slightly influences its

variance, provided that its power is insignificant compared to the power of the original signal (ϵ_r is rather small). Furthermore, it is noted that noise addition affects the system's performance similarly for either random or chaotic watermarks. Conclusions about their comparative performance after noise addition will be drawn in Section VI, where both theoretical and experimental results are shown.

B. Linear Lowpass Filtering

Lowpass filtering is a common attack usually inflicted intentionally to destroy watermark information known to exist in high frequencies (e.g. a significant part of the white spectrum of random watermarks). However, there is a number of lowpass distortions that may be accidental. Compression, for example, can be thought of as a case of lowpass filtering. In this study, we consider an example case of a non-causal moving average FIR filter of length $2F+1$ the impulse response of which is given by:

$$h_i = \frac{1}{2F+1} \quad i = -F \dots F \tag{46}$$

The filtered possibly watermarked signal $\mathbf{S'}_f$ is derived by the linear convolution of $\mathbf{S'}$ with $\mathbf{h}$:

$$S'_{f,i} = S'_i * h_i = \sum_{l=-F}^{F} h_l S'_{i-l} \quad i = 1 \dots N \tag{47}$$

The correlator detector should now estimate the correlation c_f between $\mathbf{S'}_f$ and a watermark $\mathbf{W'}$, which may or may not be $\mathbf{W}$:

$$c_f = \frac{1}{N} \sum_{i=1}^{N} \sum_{l=-F}^{F} h_l (S_{i-l} + pW_{i-l}) W'_i \tag{48}$$

Similarly to the noise addition attack, filtering does not modify the correlator's Gaussian distribution, since the contributions in the sums may be considered sufficiently independent. The mean value μ_{c_f} and the variance $\sigma^2_{c_f}$ of c_f can be derived as follows:

$$\mu_{c_f} = E[c_f] = \frac{1}{N} \sum_{l=-F}^{F} h_l \sum_{i=1}^{N} (E[S_{i-l}]E[W'_i] + pE[W_{i-l}W'_i]) \tag{49}$$

For the case of Bernoulli chaotic watermarks, (49) becomes:

$$\mu_{c_f} = \begin{cases} \frac{p}{12(2F+1)} \frac{1}{n^k} \left[1 + \frac{1-(\frac{1}{n})^F - n + n^{F+1}}{n-1} \right], & k \geq F \\ \frac{p}{12(2F+1)} \frac{1}{n^k} \left[1 + \frac{1-(\frac{1}{n})^F - n + n^{k+1} + n^{2k}(1-(\frac{1}{n})^{F-k})}{n-1} \right], & 0 \leq k < F \end{cases} \tag{50}$$

When random watermarks are used, (49) leads to:

$$\mu_{c_f} = \begin{cases} \frac{p}{12(2F+1)}, & \text{if } \mathbf{W} = \mathbf{W}' \\ 0, & \text{if } p = 0 \text{ or } \mathbf{W} \neq \mathbf{W}' \end{cases} \tag{51}$$

Estimation of $\sigma_{c_f}^2$ of c_f is performed as follows:

$$\begin{aligned} \sigma_{c_f}^2 &= E[c_f^2] - \mu_{c_f}^2 = E\left[\left(\frac{1}{N}\sum_{l=-F}^{F} h_l \sum_{i=1}^{N}(S_{i-l} + pW_{i-l})W_i'\right)^2\right] - \mu_{c_f}^2 \\ &= \frac{1}{N^2}E\left[\sum_{l=-F}^{F}\left(h_l\sum_{i=1}^{N}(S_{i-l}+pW_{i-l})W_i'\right)^2 + \right. \\ &\quad \left. \sum_{m=-F}^{F}\sum_{n=-F,n\neq m}^{F}\left(h_m\sum_{i=1}^{N}(S_{i-m}+pW_{i-m})W_i'\right)\left(h_n\sum_{i=1}^{N}(S_{i-n}+pW_{i-n})W_i'\right)\right] - \mu_{c_f}^2 \\ &= \sum_{l=-F}^{F} h_l^2 E[c^2] + \frac{1}{N^2}\sum_{m=-F}^{F}\sum_{n=-F,n\neq m}^{F} h_m h_n \left[\sum_{i=1}^{N}(E[S_{i-m}S_{i-n}]E[W_i'^2] + p^2E[W_{i-m}W_{i-n}W_i'^2]) + \right. \\ &\quad \left. \sum_{i=1}^{N}\sum_{j=1,j\neq i}^{N}(E[S_{i-m}S_{j-n}]E[W_i'W_j'] + p^2E[W_i'W_j'W_{i-m}W_{j-n}])\right] - \mu_{c_f}^2 \end{aligned} \tag{52}$$

In (52), $E[c^2] = \sigma_c^2 + \mu_c^2$ denotes the 2nd moment of correlation c under no distortions for any kind of watermarks and is evaluated by (33),(34), (39) and (40). For the case of Bernoulli chaotic watermarks, $\sigma_{c_f}^2$ has been numerically estimated for predefined values of N, n and F. Such numerical estimation is prone to errors dependent on the computational accuracy. In the case of random watermarks, (52) leads to:

$$\sigma_{c_f}^2 = \begin{cases} \frac{\mu_S^2}{12N} + \frac{1}{12N(2F+1)}\left[\sigma_S^2\left(1 + \frac{2a(1-a^{2F})}{1-a} - \frac{2}{2F+1}\frac{a(1-(2F+1)a^{2F}+2Fa^{2F+1})}{(1-a)^2}\right)\right. & \\ \left. + \frac{p^2}{2F+1}\left(\frac{3}{20} - \frac{(2F+1)^2}{12} + \frac{2F}{12}\right)\right], & \text{if } \mathbf{W} = \mathbf{W}' \\ \frac{\mu_S^2}{12N} + \frac{1}{12N(2F+1)}\left[\frac{p^2}{12} + \sigma_S^2\left(1 + \frac{2a(1-a^{2F})}{1-a} - \frac{2}{2F+1}\frac{a(1-(2F+1)a^{2F}+2Fa^{2F+1})}{(1-a)^2}\right)\right], & \text{if } \mathbf{W} \neq \mathbf{W}' \\ \frac{\mu_S^2}{12N} + \frac{1}{12N(2F+1)}\left[\sigma_S^2\left(1 + \frac{2a(1-a^{2F})}{1-a} - \frac{2}{2F+1}\frac{a(1-(2F+1)a^{2F}+2Fa^{2F+1})}{(1-a)^2}\right)\right], & \text{if } p = 0 \end{cases} \tag{53}$$

Again, conclusions about the comparative performance of Bernoulli chaotic watermarks and random ones, after moving average filtering, will be drawn in Section VI.

VI. Experimental Results

Experimental verification of the theoretical analysis results is reported in this Section. During theoretical analysis, discrete-time continuous-valued signals have been considered. Experimental ver-

ification involves loss of accuracy, since all simulated signals must be discrete-valued (quantized). However, 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 2a and 2b illustrate the autocorrelation function $R_{WW}(k)$ with respect to shift k and the power spectral density (psd) $S_W(\omega)$ of the n-way Bernoulli shift generated chaotic watermarks for different values of n (3,5,7,9,11). 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 $S_W(\omega)$. The psd of random white watermarks (both analytical and empirical) is also shown in Figure 2b for comparison purposes. It is easily observed that the Bernoulli chaotic watermark spectrum is lowpass for small values of n and it converges to that of random white watermarks as n increases 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.

In order to empirically verify the watermarking system detection reliability in terms of ROC curves, the system is fed with 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, the audio signal is assumed to comply with the signal model of (16) for $\alpha = 0.97$, a fact that has also been verified experimentally. To better comply with the model of (16) 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 $H(z) = \frac{1-\beta}{1-\beta z^{-1}}$. 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 (16) 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 ones with similar accuracy. Slightly better performance in terms of probability errors is obtained in 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 SNR=30dB. 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_{fa} 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 one 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 (7), (8) and (11) to estimate P_{fa} and P_{fr} values for varying T within $[\mu_{H_{1b}}, \mu_{H_0}]$.

As shown theoretically, the dependency of the correlation mean and variance on shift k, defined in Section III, will also be experimentally investigated. Figures 3a and b show the theoretical and empirical curves for the mean and variance respectively for various 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 4a. 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 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. In Figure 4b, respective results are shown after noise addition. Similar conclusions to the previous case are drawn. Furthermore, uncorrelated noise of small power (small value of ϵ_r), compared to the watermarked signal, does not greatly affect the system performance: P_{fa} and P_{fr} values are only slightly increased for a SNR of 14dB for the noisy watermarked signal ($\epsilon_r = \sqrt{0.12\sigma_S^2}$).

Experiments further involved system performance evaluation after the attack of lowpass filtering with moving average filters of length 3 and 5. Figure 5a shows both the theoretically and experimentally derived ROC curves after moving average filtering (window size 3) of the watermarked audio signal for both Bernoulli chaotic and random white watermarks. Both types of results tend to be similar. The numerical estimation of the theoretical $\sigma_{c_f}^2$ for Bernoulli watermarks has its impact on the derivation of ROC curves. It is easily observed that the Bernoulli chaotic watermarks lead to better performance, especially for small values of n, compared to the random white watermarks. This is easily justified by the lowpass spectral properties of the former for small n, which renders them robust against lowpass distortions. On the contrary, random watermarks tend to be severely affected by lowpass attacks, since they lose a significant part of their spectral power. In order to establish our latest observations, further experiments have been carried out, involving lowpass filtering of random watermarks prior to embedding, so that they attain similar spectral/correlation properties with Bernoulli chaotic watermarks for various n. The same lowpass filter $H(z)$ is used with the one employed to filter the input random signal in order for the latter to comply with the assumed signal model. The desirable autocorrelation function is now that of Bernoulli chaotic watermarks, i.e. $R_{WW}(k) = \frac{1}{12n^k}$. Thus, $\beta = \frac{1}{n}$ and $\sigma_W^2 = \frac{n+1}{12(n-1)}$ (random white watermark variance prior to filtering). Figure 5b shows the experimentally estimated ROC curves for LP random watermarks and for varying n, after moving average filtering of length 3 and for the LP random signal as input, compared against the

ones obtained when using respective Bernoulli chaotic watermarks. They are nearly identical proving that the watermark spectrum plays a significant role in watermarking applications. The advantage of Bernoulli chaotic watermarks is that no prefiltering is required and their probability distribution is not affected by simply modifying n (it remains uniform). Prefiltering, however, modifies the initial uniform distribution of random watermarks possibly leading to the risk of increasing their perceptibility.

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

VII. 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 or under simple attacks in order to examine the presented watermarking system detection reliability. Similar investigation is performed for random white watermarks, for comparison purposes. Bernoulli chaotic watermarks prove to perform similarly or better than random white ones. This is attributed to their 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 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.

Appendix

I. 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 (22), and that their joint distribution $f_{W_iW_{i+k}}$ is given by (27), takes the form:

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

Since the n-way Bernoulli shift map is piecewise linear in intervals of the range $[-0.5, 0.5]$, as shown in (20) (see also Figure 1a), the integral of (A-1) is restated as follows:

$$R_{WW}(k) = E[W_iW_{i+k}] = \sum_{u=1}^{n^k}\int_{\frac{u-1}{n^k}-0.5}^{\frac{u}{n^k}-0.5}\left(n^k(x+0.5) - (u-1) - 0.5\right)xdx = \frac{1}{12n^k} \tag{A-2}$$

Although these intervals are not exactly continuous, since the map takes only irrational values in $[-0.5, 0.5]$ belonging to the same chaotic orbit (Case 1), they are approximated as continuous. Subsequent joint moments are evaluated by following a similar approach:

$$E[W_i^2W_i'] = E(W_i^2W_{i+k}) = \sum_{u=1}^{n^k}\int_{\frac{u-1}{n^k}-0.5}^{\frac{u}{n^k}-0.5}\left(n^k(x+0.5) - (u-1) - 0.5\right)x^2dx = 0 \tag{A-3}$$

$$E[W_iW_i'^2] = E[W_iW_{i+k}^2] = \sum_{u=1}^{n^k}\int_{\frac{u-1}{n^k}-0.5}^{\frac{u}{n^k}-0.5}\left(n^k(x+0.5) - (u-1) - 0.5\right)^2xdx = 0 \tag{A-4}$$

$$E[W_i^2W_i'^2] = E[W_i^2W_{i+k}^2] = \sum_{u=1}^{n^k}\int_{\frac{u-1}{n^k}-0.5}^{\frac{u}{n^k}-0.5}\left(n^k(x+0.5) - (u-1) - 0.5\right)^2x^2dx = \frac{1}{144} + \frac{1}{180n^{2k}} \tag{A-5}$$

$$\begin{aligned} E[W_iW_i'W_j] &= E[W_iW_{i+k}W_{i+l}] \\ &= \sum_{v=1}^{n^{\min(k,l)}}\sum_{u=1}^{n^{|l-k|}}\int_{\frac{v-1}{n^{\min(k,l)}}+\frac{u}{n^{\max(k,l)}}-0.5}^{\frac{v-1}{n^{\min(k,l)}}+\frac{u-1}{n^{\max(k,l)}}-0.5}\left[n^{\min(k,l)}(x+0.5) - (v-1) - 0.5\right] \\ &\quad \left[n^{\max(k,l)}(x+0.5) - [(v-1)n^{|l-k|} + (u-1)] - 0.5\right]xdx = 0 \end{aligned} \tag{A-6}$$

$$E[W_iW_jW_j'] = E[W_iW_{i+l}W_{i+k+l}] = 0 \tag{A-7}$$

$$\begin{aligned} E[W_iW_i'W_jW_j'] &= E[W_iW_{i+k}W_{i+l}W_{i+k+l}] \\ &= \sum_{v=1}^{n^{\min(k,l)}}\sum_{u=1}^{n^{|l-k|}}\sum_{q=1}^{n^{\min(k,l)}}\int_{\frac{v-1}{n^{\min(k,l)}}+\frac{u-1}{n^{\max(k,l)}}+\frac{q}{n^{k+l}}-0.5}^{\frac{v-1}{n^{\min(k,l)}}+\frac{u-1}{n^{\max(k,l)}}+\frac{q-1}{n^{k+l}}-0.5} \\ &\quad \left[n^{k+l}(x+0.5) - [(u-1)n^{\min(k,l)} + (v-1)n^{\max(k,l)} + (q-1)] - 0.5\right] \end{aligned}$$

$$\left[n^{\max(k,l)}(x+0.5)-[(v-1)n^{|l-k|}+(u-1)]-0.5\right]$$
$$\left[n^{\min(k,l)}(x+0.5)-(v-1)-0.5\right]xdx$$
$$= \frac{-1}{120n^{2k+2l}}+\frac{1}{144n^{2\min(k,l)}}+\frac{1}{72n^{2\max(k,l)}} \quad \text{(A-8)}$$

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

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

References

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

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

[3] G. Voyatzis, I. Pitas, The use of watermark in the protection of digital multimedia products, Proceedings of the IEEE, Special Issue on Identification and Protection of Multimedia Information 87 (7) (1999) 1197–1207.

[4] M. Swanson, M. Kobayashi, A. Tewfik, Multimedia data-embedding and watermarking technologies, Proceedings of the IEEE 86 (6) (1998) 1064–1087.

[5] S. Craver, N. Memon, B.-L. Yeo, M. Yeung, Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks and implications, IEEE Journal of Selected Areas in Communications 16 (4).

[6] M. Swanson, B.Zhu, A. Tewfik, L. Boney, Robust audio watermarking using perceptual masking, Elsevier Signal Processing, Sp. Issue on Copyright Protection and Access control 66 (3) (1998) 337–355.

[7] I. Pitas, A method for watermark casting in digital images,, IEEE Trans. on Circuits and Systems for Video Technology 8 (6).

[8] G. Voyatzis, I. Pitas, Digital image watermarking using mixing systems, Computer & Graphics 22 (3).

[9] M. Barni, F. Bartolini, V. Cappelini, A. Piva, A DCT-domain system for robust image watermarking, Elsevier Signal Processing 66 (3) (1998) 357–372.

[10] C.-T. Hsu, J.-L. Wu, Hidden digital watermarks in images, IEEE Trans. on Image Processing 8 (1) (1999) 58–68.

[11] D. Kundur, D. Hatzinakos, Improved robust watermarking through attack characterization, Optics Express 3 (12) (1998) 485–490.

[12] R. Wolfgang, C. Podilchuk, E. Delp, Perceptual watermarks for digital images and video, Proceedings of the IEEE 87 (7) (1999) 1108–1126.

[13] W. Zhu, Z. Xiong, Y. Zhang, Multiresolution watermarking for images and video, IEEE Trans. on Cirsuits and Systems for Video Technology 9 (4) (1999) 545–550.

[14] F. Hartung, B. Girod, Watermarking of uncompressed and compressed video, Elsevier Signal Processing, Sp. Issue on Copyright Protection and Access control 66 (3) (1998) 283–301.

[15] I. Cox, J. Kilian, F. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Trans. on Image Processing 6 (12) (1997) 1673–1687.

[16] M. Swanson, B. Zhu, A. Tewfik, Multiresolution scene-based video watermarking using perceptual models, IEEE Journal of Selected Areas of Communications 16 (4) (1998) 540–550.

[17] A. Bors, I. Pitas, Image watermarking using block site selection and D.C.T. domain constraints, Optics Express 3 (12) (1998) 512–523.

[18] M. Kutter, F. Jordan, F. Bossen, Digital watermarking of color images using amplitude modulation, SPIE Journal of Electronic Imaging 7 (2) (1998) 326–332.

[19] V. Solachidis, I. Pitas, Circularly symmetric watermark embedding in 2-d dft domain, in: Proc. of ICASPP'99, Phoenix, Arizona, USA, 1999.

[20] J. Ruanaidh, T. Pun, Rotation, scale and translation invariant spread spectrum digital image watermarking, Elsevier Signal Processing, Sp. Issue on Copyright Protection and Access control 66 (3) (1998) 303–317.

[21] S. Pereira, J. Ruanaidh, F. Deguillaume, G. Csurka, T. Pun, Template based recovery of fourier-based watermarks using log-polar and log-log maps, in: Proc. of ICMCS'99, Vol. I, Florence, Italy, 1999, pp. 870–874.

[22] C. Podilchuk, W. Zeng, Image-adaptive watermarking using visual models, IEEE Journal on Selected Areas in Communications 16 (4) (1998) 525–539.

[23] M. Barni, F. Bartolini, V. Cappellini, A. Lippi, A. Piva, A DWT-based technique for spatio-frequency masking of digital signatures, in: Proc. of SPIE Electronic Imaging'99, Security and Watermarking of Multimedia Contents, Vol. 3657, 1999.

[24] D. Kundur, D. Hatzinakos, Digital watermarking for telltale tamper proofing and authentication, Proceedings of the IEEE 87 (7) (1999) 1167–1180.

[25] S. Tsekeridou, I. Pitas, Embedding self-similar watermarks in the wavelet domain, in: Proc. of ICASSP'00, Vol. IV, Istanbul, Turkey, 2000, pp. 1967–1970.

[26] J. Puate, F. Jordan, Using fractal compression scheme to embed a digital signature into an image, in: Proc. of SPIE Photonics East Symposium, Boston, USA, 1996.

[27] P. Bas, J.-M. Chassery, F. Davoine, Using the fractal code to watermark images, in: Proc. of ICIP'98, Vol. I, Chicago, Illinois, USA, 1998, pp. 469–473.

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

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

[30] F. Hartung, J. Su, B. Girod, Spread spectrum watermarking: Malicious attacks and counter-attacks, in: Proc. of SPIE: Security and Watermarking of Multimedia Contents, Vol. 3657, California, USA, 1999.

[31] J. Delaigle, C. D. Vleeschouwer, B. Macq, Watermarking algorithm based on a human visual model, Elsevier Signal Processing, Sp. Issue on Copyright Protection and Access control 66 (3) (1998) 319–335.

[32] G. 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 44 (10) (1997) 937–947.

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

[34] J. Su, F. Hartung, B. Girod, A channel model for a watermark attack, in: Proc. of SPIE: Security and Watermarking of Multimedia Contents, Vol. 3657, California, USA, 1999.

[35] I. Cox, J. Linnartz, Some general methods for tampering with watermarks, IEEE Journal of Selected Areas of Communications 16 (4).

[36] G. Depovere, T. Kalker, J.-P. Linnartz, Improved watermark detection reliability using filtering before correlation, in: Proc. of ICIP'98, Vol. I, 1998, pp. 430–434.

[37] G. Voyatzis, I. Pitas, Chaotic watermarks for embedding in the spatial digital image domain, in: Proc. of ICIP'98, Vol. II, Chicago, USA, 1998, pp. 432–436.

[38] A. Nikolaidis, I. Pitas, Comparison of different chaotic maps with application to image watermarking, in: Proc. of ISCAS'00, Vol. V, Geneva, Switzerland, 2000, pp. 509–512.

[39] S. Tsekeridou, N. Nikolaidis, N. Sidiropoulos, I. Pitas, Copyright protection of still images using self-similar chaotic watermarks, in: Proc. of ICIP'00, Vancouver, Canada, 2000, to appear.

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

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

[42] R. Rovatti, G. Setti, 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) (1998) 496–506.

[43] H. Schuster, Deterministic Chaos: An Introduction, Physik-Verlag, 1984.

[44] J. Froyland, Introduction to Chaos and Coherence, Institute of Physics, 1992.

[45] P. Billingsley, Probability and Measure, Wiley, 1995.

List of Figures

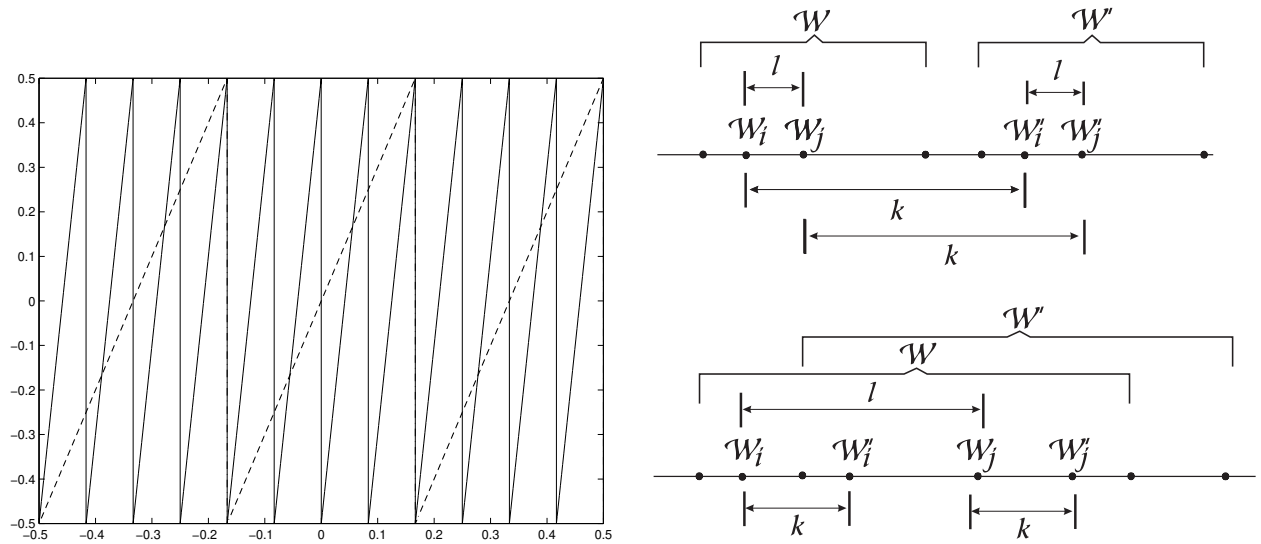
1 (a) Bernoulli shift generated chaotic signal for $n = 3$ (dashed line) and $n = 12$ (solid line). (b) Watermark $\mathbf{W}' = B_{n^k}(\mathbf{W})$, assumed to be shifted by k with respect to $\mathbf{W}$, may not overlap with $\mathbf{W}$ if $k \geq N$ (top figure), or may overlap with it if $k < N$ (bottom figure). The distance between two watermark samples, indexed by i and j, is l. 30

2 Theoretical and experimental evaluation of: (a) the autocorrelation function, (b) the power spectral density of Bernoulli chaotic watermarks for different values of n. 30

3 Theoretical (square) and empirical (* symbol) correlation (a) mean and (b) variance curves for Bernoulli chaotic watermarks with respect to shift k for various n. 31

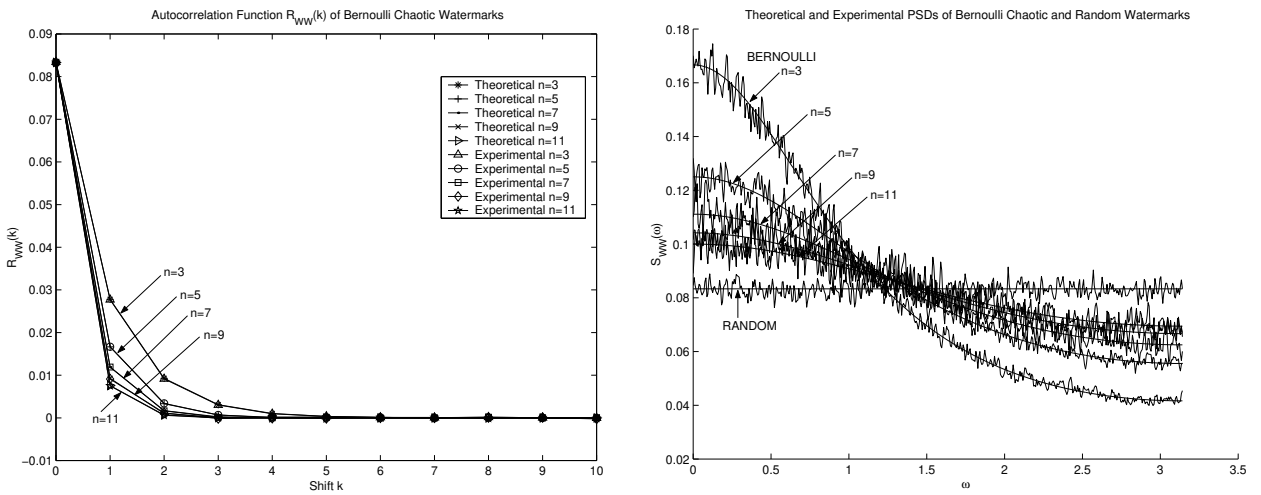
4 Theoretical and empirical ROC curves for Bernoulli chaotic watermarks after (a) no attack, and (b) noise addition. Respective curves for random white watermarks are also shown for comparison purposes. 31

5 (a) Theoretical and empirical ROC curves for Bernoulli chaotic and random white watermarks after moving average filtering ($F = 1$) (for the audio signal as input), and (b) empirical ROC curves for Bernoulli chaotic watermarks (solid lines) and random white watermarks (dashed lines), prefiltered to attain similar spectral/correlation properties with the chaotic ones. 32



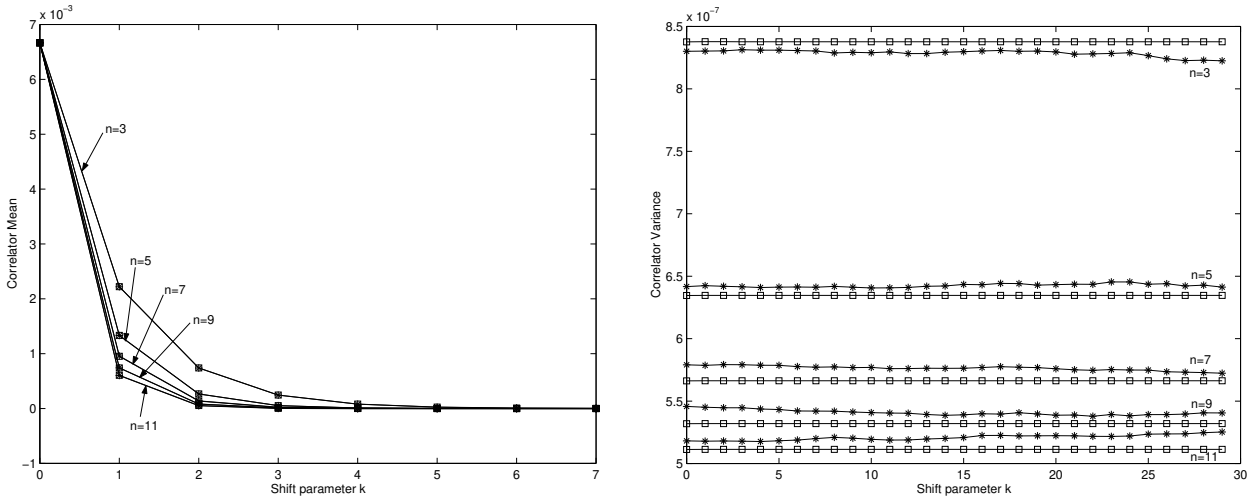
(a) (b)

Fig. 1. (a) Bernoulli shift generated chaotic signal for $n = 3$ (dashed line) and $n = 12$ (solid line). (b) 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.



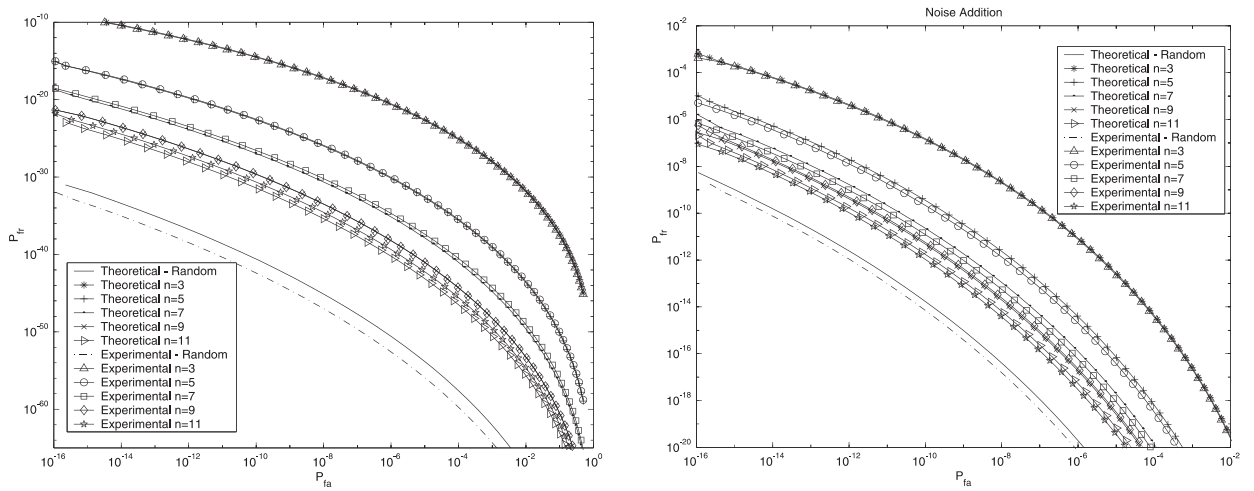
(a) (b)

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



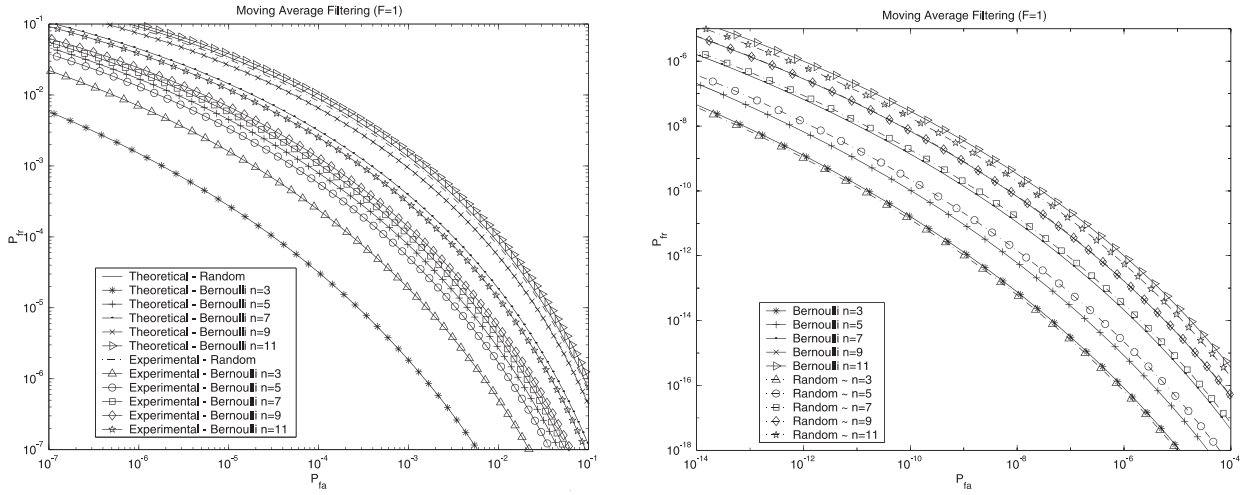
(a) (b)

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



(a) (b)

Fig. 4. Theoretical and empirical ROC curves for Bernoulli chaotic watermarks after (a) no attack, and (b) noise addition. Respective curves for random white watermarks are also shown for comparison purposes.



(a) (b)

Fig. 5. (a) Theoretical and empirical ROC curves for Bernoulli chaotic and random white watermarks after moving average filtering ($F = 1$) (for the audio signal as input), and (b) empirical ROC curves for Bernoulli chaotic watermarks (solid lines) and random white watermarks (dashed lines), prefiltered to attain similar spectral/correlation properties with the chaotic ones.