# Performance Analysis of Correlation-based Watermarking Schemes employing Markov Chaotic Sequences

Anastasios Tefas, Athanasios Nikolaidis, Nikos Nikolaidis,
Vassilios Solachidis, Sofia Tsekeridou and Ioannis Pitas

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

**EDICS:** 7-DENC

## Abstract

In this paper, theoretical performance analysis of watermarking schemes based on correlation detection is undertaken, leading to a number of important observations on the watermarking system detection performance. Statistical properties of watermark sequences generated by piecewise-linear Markov maps are investigated. Correlation/spectral properties of such sequences are easily controllable, a fact that reflects on the watermarking system performance. A family of chaotic maps, namely the skew tent map family, is used for verifying the theoretical analysis. Skew tent chaotic sequences are compared against the widely used pseudorandom sequences, indicating the superiority of the former in watermarking applications. The minimum number of samples required for reliable watermark detection is also investigated. Experiments using audio data are conducted to verify the theoretical analysis results.

## Keywords

Watermarking, copyright protection, chaotic signals

## I. Introduction

During the last decades, the world has witnessed the massive digitization of photographs, paintings, speech, music, video, documents etc, an evolution boosted by the invention of new techniques for the representation, storage and distribution of digital multimedia information. At the same time, the amount of digital data distributed through communication networks has increased rapidly. In such an environment, copying, tampering and retransmission of original digital products can be achieved easily and without leaving any traces. Consequently, the design of robust techniques for copyright protection and content verification of multimedia data became an urgent necessity. 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 a watermarking scheme, one can distinguish three fundamental functional blocks: watermark generation, embedding and detection. Watermark generation aims at constructing the information-carrying watermark pattern, using an owner and/or host data dependent key. Watermark embedding can be considered as a superposition of the watermark signal on the original signal in a way that ensures watermark imperceptibility. Finally, watermark detection is usually performed using hypothesis testing, the test statistic being the correlation between the watermarked data and the watermark signal.

A number of watermarking techniques require that the original signal is available during the detection phase. Such schemes are sometimes referred to as private or non-oblivious schemes [1, 2]. Watermarking methods that do not require the original signal for watermark detection are called oblivious or blind methods [3, 4, 5, 6]. Another classification scheme for watermarking techniques can be devised by considering the domain where the watermark signal is embedded. Some methods perform data embedding in the spatial domain [6, 7], by modulating the intensity of preselected samples, while other techniques modify the magnitude of coefficients in an appropriate transform domain, i.e., the DCT [1, 8] DFT [9, 10, 4] or DWT [5, 11] domain. Watermark embedding on the DFT phase has also been proposed [12]. Watermarking techniques can also be classified on the basis of the watermark signal dependence on the host signal. Signal dependence is necessary if signal characteristics are to be exploited in order to obtain imperceptible watermarks using masking properties of the Human Auditory System (HAS) or the Human Visual System (HVS).

For a review of existing schemes and a detailed discussion on the main requirements of a watermarking scheme, the interested reader may consult [13, 14, 15, 16, 17]. A general watermarking framework is presented in [18].

So far, performance evaluation of the existing watermarking methods has been mostly experimental, without any theoretical justification of their efficiency. Only few approaches have attempted to statistically analyze the performance of image watermarking schemes in terms of detection reliability, by addressing the problem in a communication framework [19, 20, 21, 22]. In these papers, the statistical properties of watermarking schemes based on pseudorandom watermark signals and correlation detectors, among others, are derived. In [20, 21], the authors investigate the performance of white and lowpass-filtered pseudorandom watermarks, concluding that the former are ideal when no distortions are inflicted on the image, whereas the latter provide additional robustness against lowpass distortions. They also propose using a whitening filter prior to correlation, in order to achieve optimal detection when the channel (image) cannot be modelled as additive white Gaussian noise (AWGN).

Chaotic watermarks have been recently introduced [23, 24, 25], as a promising alternative to pseudorandom signals. An overview of chaotic watermarking techniques can be found in [26]. However, up to now, their performance has been evaluated solely within an experimental framework. The analysis presented in this paper involves theoretical evaluation of the detection performance. Furthermore, theoretical analysis provides the means for evaluating the minimum number of samples required in order to achieve a pre-specified probability of false watermark rejection/acceptance. The watermarking system is modeled in a communication framework, by considering the host signal as interference while trying to detect the underlying watermark signal. The aim of the paper is to theoretically investigate the properties of piecewise-linear Markov chaotic watermarks and establish their superiority against the widely used pseudorandom watermarks. Chaotic watermarks of this class have controllable spectral/correlation properties, a fact that renders them ideal for a variety of applications. Special attention will be paid to the family of skew tent sequences, which can be generated with lowpass, white, or highpass spectral characteristics. In applications where no severe distortions are expected, e.g. in captioning/indexing applications, highpass spectrum skew tent watermarks can be used since they guarantee superior performance. In cases where robustness to lowpass attacks is important, e.g. in copyright protection and tracing applications, either lowpass skew tent watermarks can be generated, or highpass skew tent watermarks can be embedded in the low frequencies of a transform domain (e.g. DFT). To summarize, the aims of the paper are the following:

- Theoretical performance analysis of correlation-based watermarking schemes using pseudorandom or chaotic sequences.
- Investigation of effects of watermark sequence characteristics on the system performance.
- Justification of the superior correlation properties of certain chaotic sequences compared to pseudorandom sequences.
- Evaluation of the minimum signal length required for reliable watermark detection.

Therefore, the aim of the paper is neither to propose a new watermarking scheme nor to study the influence of the other watermarking system modules and aspects i.e., embedding domain, perceptual masking, attack countermeasures etc. on the system performance.

The paper is organized as follows. In Section II, the mathematical formulation of the watermark embedding and detection procedures are presented and assumptions about the signal model are adopted. In Section III, the performance of watermarking systems based on pseudorandom white watermarks is being theoretically analyzed. Section IV describes the statistical and spectral properties of piecewise-linear Markov chaotic watermarks. The Frobenius-Perron operator is used to provide closed form expressions for the corresponding statistics. Section V is devoted to Markov chaotic watermarks and their influence on watermarking schemes based on correlation detection. In Section VI, theoretical analysis results are exemplified using watermarks generated by skew tent maps. Experimental verification of the theoretical analysis, using audio data, is reported in Section VII. Conclusions are drawn in Section VIII.

## II. Watermarking System Model

So far, the influence of the watermark sequence on the overall system performance received limited attention within the watermarking literature. In this paper, we investigate the influence of watermark generation functions in the performance of a correlation based watermarking scheme and compare the widely used pseudorandom sequences with sequences generated by chaotic systems. The watermark generation aims at constructing a sequence $\boldsymbol{w}$, $w[i] \in \mathcal{R}$, of $N$ samples using an appropriate function $g$:

$$\boldsymbol{w} = g(K, N) \tag{1}$$

where $K$ denotes the watermark key that corresponds to the host signal owner or copyright holder. Watermark embedding aims at inserting the watermark signal $\boldsymbol{w}$ in the host signal $\boldsymbol{f}_o$ in a way that ensures imperceptibility and robustness under intentional or unintentional attacks. For the model under study, additive watermark embedding is assumed:

$$\boldsymbol{f}_w = \boldsymbol{f}_o + p\boldsymbol{w} \tag{2}$$

where $\boldsymbol{f}_w$ is the watermarked signal and $p$ is a constant that controls the watermark embedding power, which will be called hereafter *watermark embedding factor*. Obviously, $p$ is closely related to the watermark perceptibility. Watermark embedding can be performed in any transform domain. In the following, we will assume, without loss of generality, spatial domain embedding. However, readers should bear in mind that a similar analysis can be conducted for other embedding domains as well.

Watermark detection aims at verifying whether a given watermark $\boldsymbol{w}_d$ is embedded in the test signal $\boldsymbol{f}_t$ or not. Thus, watermark detection can be formulated as a binary hypothesis test, the two hypotheses being the following:

- $H_0$: The test signal $\boldsymbol{f}_t$ contains the watermark $\boldsymbol{w}_d$, i.e., $\boldsymbol{f}_t = \boldsymbol{f}_o + p\boldsymbol{w}_d$, $\boldsymbol{f}_o$ being the host signal.
- $H_1$: The test signal $\boldsymbol{f}_t$ does not contain the watermark $\boldsymbol{w}_d$, i.e., $\boldsymbol{f}_t = \boldsymbol{f}_o$, or it contains a different watermark $\boldsymbol{w}_e \neq \boldsymbol{w}_d$ than the one under investigation.

The two events mentioned above can be summarized in the following formula:

$$\boldsymbol{f}_t = \boldsymbol{f}_o + p\boldsymbol{w}_e \tag{3}$$

where the watermark $\boldsymbol{w}_d$ is indeed embedded in the signal if $p \neq 0$ and $\boldsymbol{w}_e = \boldsymbol{w}_d$ (event $H_0$), and it is not embedded in the signal if $p = 0$ (no watermark is present, denoted hereafter as event $H_{1a}$) or $\boldsymbol{w}_e \neq \boldsymbol{w}_d$ (wrong watermark presence, denoted hereafter as event $H_{1b}$). The presence of multiple watermarks in the host signal will not be treated in this paper since multiple watermarking is usually considered in the watermarking literature as an attack and not as a typical situation for a watermarking system. Furthermore, system performance analysis in multiple watermarking situations is very complex. The reader should however bear in mind that, in general, multiple watermarking will result in a deterioration of the system performance.

A test statistic that is often employed in examining whether the signal $\boldsymbol{f}_t$ contains a watermark $\boldsymbol{w}_d$ or not, is the correlation between the signal under investigation and the watermark:

$$c = \frac{1}{N}\sum_{n=0}^{N-1} f_t[n]w_d[n] = \frac{1}{N}\sum_{n=0}^{N-1}\left(f_o[n]w_d[n] + pw_e[n]w_d[n]\right) \quad (4)$$

Such a detection scheme is usually called a correlation detector. In order to decide on the valid hypothesis, $c$ is compared against a suitably selected threshold $T$. For a given threshold, the system performance can be measured in terms of the probability of false alarm $P_{fa}(T)$, (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):

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

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

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

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

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

where $f_{c|H_0}, f_{c|H_1}$ are the conditional probability density functions of $c$ under the hypotheses $H_0$, $H_1$ respectively (Figure **??**).

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 detection performance information. Depending on which of the two error probabilities are more critical for a certain application, one can select the desired probability of false alarm and use the ROC curve to examine whether the corresponding probability of false rejection is satisfactory or select the desired probability of false rejection and judge whether the corresponding probability of false alarm is satisfactory. Using the ROC curve one can also evaluate the *equal error rate* (EER) point i.e., the point on the ROC curve where $P_{fa}$ is equal to $P_{fr}$. EER can be used as a single-valued metric of a watermarking scheme's performance or for comparing in an easy, although not always appropriate, way the performance of two algorithms.

For the watermark sequences that will be studied in this paper, i.e., the pseudorandom sequences and the sequences generated by piecewise linear Markov maps, $f_{c|H_0}$, $f_{c|H_1}$ are normal distributions (see Sections III,IV). Thus, they can be fully determined in terms of their means $\mu_{c|H_0}$, $\mu_{c|H_1}$, and variances $\sigma^2_{c|H_0}$, $\sigma^2_{c|H_1}$. As a consequence, the performance of a correlation-based watermarking system for this type of watermark signals depends only on those four parameters. By observing Figure **??**, one can conclude that the system performance improves (i.e. the probabilities of false alarm and false rejection for a certain threshold decrease) as the two distributions come further apart, i.e., as the difference $\mu_{c|H_0} - \mu_{c|H_1}$ increases. Furthermore the performance improves as the variances of the two distributions $\sigma^2_{c|H_0}$, $\sigma^2_{c|H_1}$ decrease.

The following expression can be derived for the ROC curve:

$$P_{fa} = \frac{1}{2}\left[1 - \mathrm{erf}\left[\frac{\sqrt{2}\sigma_{c|H_0}\mathrm{erf}^{-1}(2P_{fr}-1) + \mu_{c|H_0} - \mu_{c|H_1}}{\sqrt{2}\sigma_{c|H_1}}\right]\right] \tag{9}$$

The following expressions for the mean and variance of the correlation $c$ can be derived in a straightforward manner:

$$\mu_c = E[c] = E\left[\frac{1}{N}\sum_{n=0}^{N-1}\left(f_o[n]w_d[n] + pw_e[n]w_d[n]\right)\right] = \frac{1}{N}\sum_{n=0}^{N-1}E[f_o[n]]E[w_d[n]] + \frac{1}{N}\sum_{n=0}^{N-1}pE\left[w_e[n]w_d[n]\right] \tag{10}$$

$$\begin{aligned}\sigma_c^2 &= E[c^2] - E[c]^2 = E\left[\left(\frac{1}{N}\sum_{n=0}^{N-1}\left(f_o[n]w_d[n] + pw_e[n]w_d[n]\right)\right)^2\right] - \mu_c^2 \\ &= \frac{1}{N^2}E\left[\sum_{n=0}^{N-1}\left(f_o[n]w_d[n] + pw_e[n]w_d[n]\right)^2\right.\end{aligned}$$

$$
\begin{aligned}
&+ \sum_{n=0}^{N-1} \sum_{m=0,m\neq n}^{N-1} (f_o[n]w_d[n] + pw_e[n]w_d[n])(f_o[m]w_d[m] + pw_e[m]w_d[m]) \Bigg] - \mu_c^2 \\
= \; & \frac{1}{N^2}\Bigg[ \sum_{n=0}^{N-1} \Big( E[f_o^2[n]]E[w_d^2[n]] + p^2E[w_d^2[n]w_e^2[n]] + 2pE[f_o[n]]E[w_e[n]w_d^2[n]] \Big) \\
&+ \sum_{n=0}^{N-1} \sum_{m=0,m\neq n}^{N-1} (E[f_o[n]f_o[m]]E[w_d[n]w_d[m]] + pE[f_o[n]]E[w_d[n]w_e[m]w_d[m]] \\
&+ pE[f_o[m]]E[w_e[n]w_d[m]w_d[n]] + p^2E[w_e[n]w_e[m]w_d[n]w_d[m]]\Big)\Bigg] - \mu_c^2
\end{aligned}
\tag{11}
$$

Note, that these expressions can be used to represent $\mu_c$, $\sigma_c^2$ for both events $H_0$ ($\boldsymbol{w}_d = \boldsymbol{w}_e$) and $H_1$ ($\boldsymbol{w}_d \neq \boldsymbol{w}_e$ or $p = 0$). The obvious statistical independence between the host signal $\boldsymbol{f}_o$ and both watermarks $\boldsymbol{w}_e$, $\boldsymbol{w}_d$ has been exploited in order to derive the previous formulas.

By examining (10), (11), one can easily conclude that several moments need to be evaluated if $\mu_c, \sigma_c^2$ are to be computed. To proceed in such an evaluation, an assumption about the statistical properties of the host signal has to be adopted. Let us denote by $R_g[\boldsymbol{k}]$ the statistic of the form:

$$R_g[k_1, k_2, \ldots, k_r] = E\left[g[n]g[n+k_1]g[n+k_2]\ldots g[n+k_r]\right] \tag{12}$$

which will be called hereafter $r$-th order correlation statistic of a wide-sense stationary signal $g$. In our case, the host signal will be assumed to be wide-sense stationary, thus:

$$E[f_o[n]] = \mu_{f_o} \quad \forall n, \quad n = 0\ldots N-1 \tag{13}$$

$$E[f_o[n]f_o[n+k]] = R_{f_o}[k] \quad \forall n, \quad n = 0\ldots N-1 \tag{14}$$

Furthermore, a first order exponential autocorrelation function model will be assumed:

$$R_{f_o}[k] = \mu_{f_o}^2 + \sigma_{f_o}^2\beta^k, \quad k \geq 0, \; |\beta| \; \leq 1 \tag{15}$$

where $\beta$ is the parameter of the autocorrelation function, and $\sigma_{f_o}^2$ is the host signal variance:

$$\sigma_{f_o}^2 = E[f_o^2[n]] - E[f_o[n]]^2 \tag{16}$$

This model has been chosen because it is simple and tractable and can model fairly well the autocorrelation function of image scanlines and speech signals [21, 22, 27]. 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 VII.

## III. Pseudorandom watermarks

Most watermarking schemes proposed so far, use a pseudorandom number generator in order to construct the watermark signal that will be embedded in the host data. Samples generated by such functions can be accurately modelled 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 $[-0.5, 0.5]$. Obviously, since $E[w[i]] = 0$, $\forall i$ and $E[w[i]w[i+k]] = \delta(k)E[w^2[i]]$ ($\delta(k)$ being the Dirac delta function), pseudorandom signals of this type are wide-sense stationary and ergodic [28]. 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 pseudorandom watermark signal moments that appear in expressions (10), (11):

$$E[w^m[i]] \;=\; \begin{cases} 0 & m \;\; \text{odd} \\ \frac{1}{(m+1)2^m} & m \;\; \text{even} \end{cases} \tag{17}$$

$$E[w^l[i]w^m[j]] = E[w^l[i]]E[w^m[j]] \tag{18}$$

Similar expressions can be derived for the joint moments involving more than two random variables. By substituting the above expressions in (10), (11), the mean value and the variance of the correlation $c$ for a watermarking system based on pseudorandom watermarks can be calculated:

$$\mu_c = \begin{cases} \frac{p}{12} & \text{if } \boldsymbol{w}_d = \boldsymbol{w}_e \ (H_0) \\ 0 & \text{if } \boldsymbol{w}_d \neq \boldsymbol{w}_e \ (H_{1b}) \\ 0 & \text{if } p = 0 \ (H_{1a}) \end{cases} \qquad \sigma_c^2 = \begin{cases} \frac{1}{12N}(\mu_{f_o}^2 + \sigma_{f_o}^2 + \frac{p^2}{15}) & \text{if } \boldsymbol{w}_d = \boldsymbol{w}_e \ (H_0) \\ \frac{1}{12N}(\mu_{f_o}^2 + \sigma_{f_o}^2 + \frac{p^2}{12}) & \text{if } \boldsymbol{w}_d \neq \boldsymbol{w}_e \ (H_{1b}) \\ \frac{1}{12N}(\mu_{f_o}^2 + \sigma_{f_o}^2) & \text{if } p = 0 \ (H_{1a}) \end{cases} \tag{19}$$

By observing (19), one concludes that $\mu_{c|H_{1a}} = \mu_{c|H_{1b}}$ while $\sigma^2_{c|H_{1a}} < \sigma^2_{c|H_{1b}}$, proving that event $H_{1b}$ is the worst case among events $H_{1a}$, $H_{1b}$. Thus, the experiments in Section VII will be conducted using the event $H_{1b}$.

Another very important observation is that $\mu_c$ depends only on the watermark embedding factor $p$, whereas $\sigma_c^2$ depends also on the mean value and the variance of the host signal. For certain classes of signals (i.e., images), the term $\mu_{f_o}$ is considerably large, especially in comparison to $\sigma^2_{f_o}$. Thus, the subtraction of the mean value $\mu_{f_o}$ from the test signal can result in lower variance for the correlation and, subsequently, to a considerable improvement of the system's performance. For a zero mean watermark, $\mu_{f_o}$ can be easily shown to be equal to the mean value of the test signal $\boldsymbol{f}_t$:

$$E[\boldsymbol{f}_t] = E[\boldsymbol{f}_o + p\boldsymbol{w}_e] = E[\boldsymbol{f}_o] + pE[\boldsymbol{w}_e] = E[\boldsymbol{f}_o] = \mu_{f_o} \tag{20}$$

By subtracting $E[\boldsymbol{f}_t]$ from the test signal, we obtain the signal $\boldsymbol{f}_t^{'}$:

$$\boldsymbol{f}_t^{'} = \boldsymbol{f}_t - E[\boldsymbol{f}_t] = (\boldsymbol{f}_o - \mu_{f_o}) + p\boldsymbol{w}_e = \boldsymbol{f}_o^{'} + p\boldsymbol{w}_e \tag{21}$$

where $\boldsymbol{f}_o^{'} = \boldsymbol{f}_o - \mu_{f_o}$ and $\mu_{f_o'} = 0$. Mean value subtraction has been proposed in the past as a heuristic for improving the system performance. However, no formal justification of the effect of the subtraction has been provided so far. Experimental verification of this result will be provided is Section VII.

## IV. Statistical Analysis of Chaotic Sequences generated by Markov Maps

Sequences generated by chaotic maps constitute an efficient alternative to pseudorandom watermarking sequences. A chaotic discrete-time signal $x[n]$ can be generated by a chaotic system with a single state variable by applying the recursion

$$x[n] = f(x[n-1]) = f^n(x[0]) = \underbrace{f(f(\ldots(f}_{n \text{ times}}(x[0]))\ldots)) \tag{22}$$

where $f(\cdot)$ is a nonlinear transformation that maps scalars to scalars and $x[0]$ is the system initial condition. Thus, a chaotic signal is generated through an iterative procedure, starting from $x[0]$. The notation $f^n(x[0])$ is used to denote the $n$-th application of the map. To proceed with the performance analysis of watermarking systems based on chaotic sequences, the correlation statistics of such sequences, that are involved in expressions (10) and (11), must be derived.

Let $p_n(\cdot)$ denote the probability density function of the $n$-th iterate $x[n]$. A linear operator can be defined such that:

$$p_n(\cdot) = P_f\{p_{n-1}(\cdot)\} = P_f^n\{p_0(\cdot)\} \tag{23}$$

This operator, which is referred to as the Frobenius-Perron (FP) operator [29], describes the time evolution of the density $p_n(\cdot)$ for a particular map. Although, in general, the densities at distinct iterates $n$ will differ, there can be certain choices of $p_0(\cdot)$ such that the densities of subsequent iterates do not change, i.e.,

$$p(\cdot) = P_f^n\{p(\cdot)\}, \quad \forall n \tag{24}$$

Such a density $p(\cdot)$, is referred to as the *invariant density* of the map $f(\cdot)$, and constitutes a fixed point of the FP operator. For a given map, more than one densities may satisfy (24). The invariant density plays an important role in the computation of time-averaged statistics of time series from nonlinear dynamics. When $p_0(\cdot)$ is chosen to be an invariant density, it is straightforward to verify that the resulting stochastic process is stationary and, subject to certain constraints on the map, ergodic [29].

A rich class of 1-D chaotic systems that are particularly amenable to analysis are the eventually expanding, piecewise-linear Markov maps. A map $\mathcal{M} : [0,1] \rightarrow [0,1]$ is an eventually expanding, piecewise-linear, Markov map if the following conditions hold:

1. The map is piecewise-linear, i.e., there is a set of points $\alpha_0, \alpha_1, \ldots, \alpha_M$ satisfying $0 = \alpha_0 < \alpha_1 < \cdots < \alpha_M = 1$ such that, when restricted to each of the intervals $(\alpha_{i-1}, \alpha_i)$, the map is affine. $\alpha_0, \alpha_1, \ldots, \alpha_M$ are called partition points and the corresponding intervals partition elements.

2. The map possesses the Markov property i.e., partition points are mapped to partition points:

$$\forall\, i\ \in [0, \ldots, M],\ \ \exists\, j\ \in [0, \ldots, M]\ \ :\ \ \mathcal{M}(\alpha_i) = \alpha_j \tag{25}$$

3. The map has the eventually expanding property, i.e., there exists an integer $r > 0$ such that

$$\inf_{x \in [0,1]} \left| \frac{d}{dx} \mathcal{M}^r(x) \right| > 1 \tag{26}$$

For simplicity, maps satisfying the above definition will be referred to as "Markov maps" when there is no risk of ambiguity. Markov maps possess a number of useful properties. All Markov maps have invariant densities and are ergodic under readily verifiable conditions [30]. In addition, suitably quantized outputs of Markov maps are equivalent to Markov chains. In particular, for almost all initial conditions, the sequence of partition element indices corresponding to successive iterates of the map is indistinguishable from a sample path of a Markov chain [31].

The statistics of Markov maps can be determined in closed form. A strategy for computing these statistics was developed in [32]. A unique property of the FP operator acting upon piecewise-linear Markov maps is that their invariant subspaces contain piecewise polynomials. Thus, the image of piecewise polynomials of degree $K$ is also piecewise polynomials of degree $K$. Moreover, by representing the density $p_0(\cdot)$ of the initial condition on a suitable system of basis functions (a polynomial space for the calculation of moments), the FP operator can be formulated as matrix operator. The densities can be uniquely represented by vectors, hereafter referred as coordinate vectors, comprised of the piecewise polynomial factors. As a result, all calculations required for the statistics of Markov maps involve finite dimensional linear algebra. The matrix $\boldsymbol{P}_K$, which we will refer to as the FP matrix, describes how the coefficients of expansion, in terms of the polynomial basis, map under the FP operator. The subscript $K$ denotes the sufficient dimension for the basis expansion. For a detailed definition of the matrices and vectors involved in statistics calculations that will be used in the sequel, one may consult [32].

Based on the representation of the FP operator on a finite set of basis functions, the invariant density $p(\cdot)$ of a Markov map, or equivalently the invariant density coordinate vector $\boldsymbol{p}$, can be calculated by solving the corresponding eigenvector problem:

$$\boldsymbol{P}_0\boldsymbol{p} = \boldsymbol{p} \tag{27}$$

where $\boldsymbol{P}_0$ is the FP matrix of zero expansion. Thus, this coordinate vector is the nonnegative eigenvector corresponding to the unit eigenvalue of the FP matrix. Moreover, Markov maps have the property that all invariant densities of interest are piecewise constant.

Accordingly, using the FP matrix, the higher order correlation statistics of Markov maps can be derived. To do so, the FP matrix and the basis correlation matrix must be expanded in a sufficient dimension [32]. For example, for calculating the autocorrelation function of a chaotic sequence, the FP matrix $\boldsymbol{P}_1$ and the corresponding basis correlation matrix are needed. The Markov sequences that will be used in the sequel, attain exponential autocorrelation function given by (15), where $\beta$ is an eigenvalue of the corresponding FP matrix [33]. For higher order correlation statistics given by (12), the sufficient dimension for the basis expansion is linearly increased. According to (10) and (11), the highest order correlation statistic required for evaluating the mean value and the variance of the detector in the presented watermarking system is of third order and the corresponding FP matrix that need to be evaluated is $\boldsymbol{P}_3$.

## V. Employing Chaotic Sequences in Watermarking Schemes

From the preceding discussion, one can conclude that a chaotic sequence $\boldsymbol{x}$ is fully described by the map $f(\cdot)$ and the initial condition $x[0]$. By imposing certain constraints on the map or the initial condition, sequences of infinite period can be obtained. Thus, if we consider two finite sequences $\boldsymbol{x}, \boldsymbol{y}$ generated by the iterative application of the same map on two distinct initial conditions $x[0], y[0]$, respectively, that belong to the same chaotic orbit, there will always be an integer $k > 0$ such that:

$$x[0] = f^k(y[0]) \quad \text{or} \quad y[0] = f^k(x[0]) \tag{28}$$

The corresponding samples $x[n], y[n]$ are associated through the following expression for a suitably selected $k > 0$:

$$y[n] = f^n(y[0]) = f^n(f^k(x[0])) = x[n+k] \quad \text{or} \quad x[n] = y[n+k] \tag{29}$$

From now on, constant $k$ will be called sequence shift. Having described how a chaotic sequence $\boldsymbol{x}$ can be generated in the interval $[0, 1]$, the corresponding chaotic watermark sequence is given by:

$$\boldsymbol{w} = \boldsymbol{x} - d\boldsymbol{1} \tag{30}$$

where $d$ is a constant that controls the range of the watermark sequence and $\boldsymbol{1} = [1, 1, \ldots, 1]^T$. By substituting (30) in (10) and (11) and considering that $w_d[n] = w_e[n+k]$, according to (29), it is straightforward to show that the mean value and the variance of the correlation $c$ are given by:

$$\mu_c = \mu_{f_o}\mu_x - d\mu_{f_o} + pR_x[k] - 2pd\mu_x + pd^2 \tag{31}$$

$$\begin{aligned}
\sigma_c^2 &= B(d^2 + 2R_x[k]) - pd^3\mu_{f_o} + 2pd^2\mu_x(3\mu_{f_o} - 2pd) \\
&+ \frac{1}{N}\left[2B(R_x[0] + R_x[k]) - \frac{2B}{d}R_x[0,k] - 2p^2dR_x[k,k] + (d^2 - 2d\mu_x + R_x[0])R_{f_o}[0] + p^2R_x[0,k,k]\right] \\
&+ \frac{2}{N^2}\left[B\sum_{m=1}^{N-1}(N-m)(2R_x[m] + R_x[m+k] + R_x[k-m]) - \frac{B}{d}\sum_{m=1}^{N-1}(N-m)(R_x[k,m] + R_x[m,m+k])\right.
\end{aligned}$$

$$-p^2 d \sum_{m=1}^{N-1} (N-m)(R_x[k,k-m] + R_x[k,m+k]) + (d^2 - 2d\mu_x) \sum_{m=1}^{N-1} (N-m) R_{f_o}[m]$$
$$\left. + \sum_{m=1}^{N-1} (N-m) R_x[m] R_{f_o}[m] + p^2 \sum_{m=1}^{N-1} (N-m) R_x[m,k,m+k] \right] - \mu_c^2 \qquad (32)$$

where $B = p^2 d^2 - pd\mu_{f_o}$, $\mu_x$ is the mean value of the chaotic sequence, and $R[\boldsymbol{k}]$ is given by (12).

Expressions (31) and (32) are sufficiently broad to include all events that occur in the watermarking model described in Section II, provided that piecewise linear Markov maps are used to generate the watermark sequence. That is, the case of watermark absence (event $H_{1a}$) is represented by setting the watermark embedding factor $p$ equal to zero. The case of watermark presence is represented by a positive watermark embedding factor and $k = 0$ in the case of correct watermark presence (event $H_0$), or $k > 0$ in the case of wrong watermark presence (event $H_{1b}$). The correlation statistics needed for evaluating expressions (31) and (32) can be derived in closed form, or evaluated numerically [32, 34]. Furthermore, by using the appropriate expressions for correlation statistics, the above formulas can be used to describe correlation based, additive embedding watermarking schemes incorporating a wider class of watermark sequences. For example, expressions for a watermarking scheme based on zero-mean pseudorandom white watermarks can be obtained by substituting the expressions:

$$R_x[k] = \delta(k)E[x^2], \;\; R_x[k_1,k_2] = \delta(k_1)\delta(k_2)E[x^3], \;\; R_x[k_1,k_2,k_3] = \delta(k_1)\delta(k_2)\delta(k_3)E[x^4] \quad (33)$$

in equations (31), (32).

The constant value $d$ is usually chosen to be the mean value of the chaotic sequence $\boldsymbol{x}$ in order to have a DC free watermark which, according to [22], results in better system performance. Moreover, by subtracting the test signal mean value prior to detection (see Section III), we can decrease the variance of the correlation, thus obtaining better system performance as will be shown in Section VII. By using a DC free watermark and subtracting the test signal mean value prior to detection, the mean value and the variance of the correlation $c$ have a much simpler form:

$$\mu_c = p(R_x[k] - \mu_x^2) \qquad (34)$$

$$\begin{aligned}\sigma_c^2 &= \frac{p^2}{N^2}\sum_{m=0}^{N-1}(N-m)(2-\delta(m))\{\mu_x^2(2R_x[m]+R_x[m+k]+R_x[k-m]) \\ &-\mu_x(R_x[k,m]+R_x[m,m+k]+R_x[k,k-m]+R_x[k,m+k])+R_x[m,k,m+k]\} \\ &+\frac{1}{N^2}\sum_{m=0}^{N-1}(N-m)(2-\delta(m))(R_x[m]-\mu_x^2)R_{f_o}[m]-p^2(R_x[k]-2\mu_x^2)^2 \qquad (35)\end{aligned}$$

where $\delta(m)$ is the Dirac delta function.

Although samples of Markov chaotic watermarks are correlated for small $k > 0$, since they possess exponential autocorrelation function and $\boldsymbol{w}_d$ is a shifted version of $\boldsymbol{w}_e$, the Central Limit Theorem for random variables with small dependency [35] may be used in order to establish that the correlation $c$ in (4) attains a Gaussian distribution, even in the case of wrong watermark presence (assuming that $N$ is sufficiently large). Furthermore, under the worst case assumption (event $H_{1b}$), both $\mu_c$ and $\sigma_c^2$, given by (31) and (32) respectively, converge to constant values for large $k$. In such a case, $P_{fa|H_{1b}}$ substitutes $P_{fa|H_1}$ since this is the worst case. $P_{fa|H_{1b}}$ can be estimated using the limit values ($k \rightarrow \infty$) of $\mu_c$ and $\sigma_c^2$. $P_{fr}$ values are estimated using the values of $\mu_c$ and $\sigma_c^2$ for $k = 0$ (event $H_0$) and ROC curves are evaluated from (9).

Moreover, if we examine in detail the mean value of the correlation given by (34), we can notice that the mean value converges to zero for event $H_1$. Additionally, for event $H_0$ the mean value of the detector is equal to the variance of the watermark multiplied by the embedding power. This addresses the fact that the mean value of the correlation depends only on the power and the variance of the watermark and not on the watermark generator (chaotic or pseudorandom), or the spectral properties of the watermark signal.

The aforementioned remark leads us to the conclusion that, for watermark signals of the same power and the same variance, the watermarking system performance is affected only by the variance of the correlation detector. That is, the lower the variance of the correlation for events $H_0$ and $H_1$, the better the watermarking system performance. Therefore, the objective is to construct watermarks that result in small correlation variance. According to (35), this can be achieved by utilizing watermark signals with suitable first, second and third order correlation statistics. In order to elaborate on eqs. (34) and (35), we rewrite them for the two events $H_0$ and $H_{1a}$.

$$\mu_c = \begin{cases} 0 & p = 0\ (H_{1a}) \\ p\sigma_x^2 & k = 0, p \neq 0\ (H_0) \end{cases} \qquad (36)$$

$$\sigma_c^2 = \begin{cases} \frac{1}{N}\sigma_x^2\sigma_{f_o}^2 + \frac{2}{N^2}\sum_{m=1}^{N-1}(N-m)(R_x[m]-\mu_x^2)R_{f_o}[m] & p=0\ (H_{1a}) \\ \frac{1}{N}\sigma_x^2\sigma_{f_o}^2 + \frac{p^2}{N}(4\mu_x^2R_x[0]-4\mu_xR_x[0,0]+R_x[0,0,0]) - p^2(R_x[0]-2\mu_x^2)^2 & \\ +\frac{2p^2}{N^2}\sum_{m=1}^{N-1}(N-m)\{4\mu_x^2R_x[m]-2\mu_x(R_x[0,m]+R_x[m,m])+R_x[0,m,m]\} & \\ +\frac{2}{N^2}\sum_{m=1}^{N-1}(N-m)(R_x[m]-\mu_x^2)R_{f_o}[m] & k=0, p\neq 0\ (H_0) \end{cases} \tag{37}$$

When event $H_{1a}$ holds, it can be easily observed that the correlation variance depends only on the watermark autocorrelation function $R_x[m]$. The autocorrelation function of a signal is directly associated with its *power spectral density* (psd):

$$S_x(\omega) = \sum_{k=-\infty}^{\infty} R_x[k]e^{-j\omega k} = R_x[0] + \sum_{k=1}^{\infty} R_x[k]\left(e^{-j\omega k}+e^{j\omega k}\right) \tag{38}$$

Therefore, the spectral properties of the watermark signal determine the variance of the correlation for the event $H_{1a}$. Moreover, if we consider the exponential autocorrelation function of Markov chaotic sequences given by (15), it can be easily derived that the correlation variance given by (37) depends on the sum over the samples of the autocorrelation function in the interval $[0, N-1]$, which is minimized for $\beta \to -1$, and maximized for $\beta \to 1$. Using (38), one can observe that the two cases correspond to the most highpass and most lowpass signals that can be generated having exponential autocorrelation function. Considering the above discussion, one can conclude that highpass watermarks perform better than lowpass ones, when no attacks on the watermarked signal are considered, since the correlation variance is reduced. When event $H_{1b}$ holds, the correlation variance $\sigma^2_{c|H_{1b}}$ still depends only on the spectrum of the watermark signal, as will be presented in Section VII.

A final interesting conclusion that we can draw on the basis of the previous analysis is that, even when two sequences holds have the same power, variance and spectral properties, their performance in a watermarking scheme might be different. For such sequences, the correlation mean and variance for event $H_1$, would have the same value. However, the correlation variance for event $H_0$ could differ, since it also depends on the second and third order correlation statistics $R_x[0,m], R_x[m,m], R_x[0,m,m]$ of the watermark sequence. As a consequence, it is possible to generate white chaotic watermark sequences that perform better than pseudorandom white sequences, as will be presented in the following Sections.

## VI. The Skew Tent Map

In this section, analysis techniques presented so far are being exemplified using the *skew tent* map, which is a piecewise linear Markov map. The skew tent map [36] is illustrated in Figure **??** and can be expressed as:

$$\mathcal{T} : [0,1] \rightarrow [0,1]$$

$$\text{where} \quad \mathcal{T}(x) = \begin{cases} \frac{1}{\alpha}\, x & 0 \leq x \leq \alpha \\ \frac{1}{\alpha-1}\, x + \frac{1}{1-\alpha} & \alpha < x \leq 1 \end{cases} \quad , \ \alpha \in (0,1) \tag{39}$$

A trajectory $t[k]$ of the dynamical system is obtained by iterating this map i.e.,

$$t[k] = \mathcal{T}(t[k-1]) = \mathcal{T}^k(t[0]) \tag{40}$$

The invariant density of the skew tent map is uniform, as can be derived using (27). Following the methodology described in Section IV, the statistical properties of sequences produced using the skew tent map can be derived. The analytical expressions for the first, second and third order correlation statistics, required for evaluating the performance of watermarking schemes based on the skew tent map, can be found in Appendix A. For example, the first order correlation statistic (autocorrelation function) is given by:

$$R_t[k] = \frac{1}{4} + \frac{1}{12} e_2^k = \frac{1}{4} + \frac{1}{12}(2\alpha - 1)^k \tag{41}$$

where $e_2 = 2\alpha - 1$ is an eigenvalue of the FP matrix $\boldsymbol{P}_3$. It can be observed that the autocorrelation function depends only on the parameter $\alpha$ of the skew tent map. Thus, by controlling the parameter $\alpha$, we can generate sequences having any desirable exponential autocorrelation function. Using (38), (41), the power spectral density of the skew tent map sequences are derived:

$$S_t(\omega) = \frac{1 - e_2^2}{12(1 + e_2^2 - 2e_2 \cos\omega)} \tag{42}$$

Thus, by varying the parameter $\alpha$, either highpass ($\alpha < 0.5$), or lowpass ($\alpha > 0.5$) sequences can be produced. For $\alpha = 0.5$, the symmetric tent map is obtained. Sequences generated by the symmetric tent map possess white spectrum, since the autocorrelation function becomes the Dirac delta function. The control over the spectral properties is very useful in watermarking applications, since the spectral characteristics of the watermark sequence are directly related to watermark robustness against common types of attack, such as filtering and compression.

Using the analytical expressions for the correlation statistics of skew tent sequences given in Appendix A, one can derive the mean value and the variance of the correlation detector for this map:

$$\mu_c = \begin{cases} 0 & p = 0 \ (H_{1a}) \\ \frac{p}{12} & k = 0, p \neq 0 \ (H_0) \end{cases} \tag{43}$$

$$\sigma_c^2 = \begin{cases} \frac{\sigma_{fo}^2}{12N^2}\frac{N-2\beta e_2-N\beta^2 e_2^2+2(\beta e_2)^{N+1}}{(1-\beta e_2)^2} & p = 0 \ (H_{1a}) \\ \frac{p^2}{180N^2}\frac{N-2e_1-Ne_1^2+2e_1^{N+1}}{(1-e_1)^2} + \frac{\sigma_{fo}^2}{12N^2}\frac{N-2\beta e_2-N\beta^2 e_2^2+2(\beta e_2)^{N+1}}{(1-\beta e_2)^2} & k = 0, p \neq 0 \ (H_0) \end{cases} \tag{44}$$

where $e_1, e_2$ are eigenvalues of the FP matrix $\boldsymbol{P}_3$ and $\beta$ is the parameter of the host signal autocorrelation function given by (15).

## VII. Experimental Results and Discussion

In this Section, the experimental verification of the results obtained through theoretical analysis is reported. Discrete-time, continuous-valued signals have been considered throughout the previous sections. Unfortunately, experimental verification 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.

In order to experimentally verify the theoretical performance analysis of a watermarking system based on correlation detection, the system is fed with a music audio signal of 1sec duration, sampled at 44.1kHz with 16 bits per sample ($N = 44100$). The audio signal is assumed to comply with the signal model of (15). The value of the audio signal autocorrelation parameter that is required for calculating the theoretical expressions derived above, was estimated using Mean Square Error minimization for the first 10 samples of the calculated test signal autocorrelation function. Using more than 10 samples for $\beta$ calculation does not alter the estimated value. Furthermore, it has been proven experimentally that incorrect estimates of $\beta$ ($\pm 15\%$ of the actual value) do not significantly affect the obtained theoretical results. For the audio signal used in the experiments, the parameter $\beta$ was found to be 0.97. The audio signal autocorrelation function complies with the assumed model as it will be verified by the accordance of the theoretical and experimental curves. System performance was measured for three classes of watermark signals, namely, chaotic watermarks generated by tent maps with different spectral properties, pseudorandom white watermarks and watermarks generated by Bernoulli sequences, exhibiting lowpass characteristics [26]. A watermark embedding factor $p$ that resulted in watermarked signals with SNR=30dB has been used in all cases. Experiments were conducted using a total of 10000 keys for each class of signals. In subsequent analysis, ROC curve evaluation is performed under the worst case assumption for $P_{fa}$ evaluation, corresponding to the signal being watermarked by a watermark different than the one used in detection (event $H_{1b}$).

At first, the statistical and spectral properties of the tent chaotic watermarks are experimentally evaluated and compared with the analytical expressions. Figure **??** illustrates the power spectral density (psd) $S_t(\omega)$ of the tent generated chaotic watermarks for different values of the map parameter $\alpha$ (0.1,0.3,0.5,0.7,0.9). The experimental curves are almost identical with the theoretical ones. It is easily observed that the spectrum of tent chaotic watermarks is highpass for small values of $\alpha$, becomes white for $\alpha = 0.5$ and tends to lowpass as $\alpha \rightarrow 1$. This observation justifies our earlier remark about the controllable spectral/correlation properties of the tent chaotic watermarks. Tent chaotic watermarks, generated for the above mentioned values of $\alpha$, were used in all subsequent experiments in order to illustrate the influence of $\alpha$ (spectral properties) on the system performance.

Experimental verification of the dependency of $\mu_c$, $\sigma_c^2$ on the watermark shift $k$, for watermark signals generated by tent maps was also pursued. Figure **??** shows the theoretical and empirical curves for the mean and variance of the correlation, for various values of $\alpha$. When $k = 0$, the detected watermark is identical to the embedded one ($\boldsymbol{w}_d = \boldsymbol{w}_e$). The main observation here is that the correlation variance for the correct watermark ($k = 0$) is smaller than the correlation variance observed when the test watermark is different from the embedded one. Moreover, correlation mean and variance quickly converge to constant values. The convergence depends on the parameter $\alpha$ of the tent map. As the chaotic sequence becomes more lowpass or highpass, the correlation mean and variance converge slower to a constant value. This leads to the conclusion that the probability of detecting a shifted watermark as the correct one, reduces as the parameter $\alpha$ of the map tends to 0.5. Subsequent analysis will proceed under the assumption that $k$ is sufficiently large to guarantee convergence of $\mu_c$, $\sigma_c^2$ to their limit values. Under this assumption, the respective correlation detector attains a Gaussian distribution.

The influence of the map parameter $\alpha$ on the watermarking system performance was also considered. The ROC curves for lowpass ($\alpha = 0.7$), white ($\alpha = 0.5$) and highpass ($\alpha = 0.3$) tent chaotic watermarks were theoretically and experimentally evaluated. The superior performance of the highpass tent chaotic watermarks can be easily observed in Figure **??**a. The performance of the watermarking system is considerably inferior for white tent watermarks, whereas the worst performance is observed when lowpass watermarks are used.

It is obvious that in case of lowpass attacks, such as filtering or compression, the lowpass watermark will be more robust. In order to take advantage of the superior correlation properties of highpass watermarks even in the case of lowpass attacks, one can perform embedding in another domain and not in the spatial one. For example, if a highpass watermark is embedded in the low frequencies of the DFT domain, as it has been proposed in many watermarking algorithms [37, 38], the watermark becomes robust to lowpass attacks, while retaining its correlation properties.

Next, we proceed to illustrate the fact that schemes utilizing watermark signals of the same spectral properties may exhibit different behavior. In other words, we will experimentally verify the theoretical expressions that indicate the fact that two watermarking schemes using sequences of the same spectral properties attain the same correlation mean and variance for event $H_1$, but exhibit different correlation variance for event $H_0$, since in that case $\sigma_c^2$ depends also on the second and third order correlation statistics (35). In order to do so, we compare the white tent chaotic watermarks ($\alpha = 0.5$) with the pseudorandom white watermarks. Furthermore, we compare lowpass tent watermarks against watermarks generated by Bernoulli maps, possessing the same spectral characteristics. The autocorrelation function of Bernoulli watermarks can be derived using the methodology described in Section IV. For such sequences, the first order correlation statistic is:

$$R_b[k] = E[b[n]b[n+k]] = \frac{1}{4} + \frac{1}{12m^k} \tag{45}$$

where $m \in \mathcal{Z}+$ is the number of Bernoulli map partition elements. By comparing (41), (45) one can conclude that for $\alpha = \frac{m+1}{2m}$ the tent map generates sequences that have the same spectral properties with the corresponding Bernoulli sequences. It is worth noting here that Bernoulli chaotic maps can generate only lowpass sequences. Lowpass characteristics of Bernoulli sequences weaken as $m \to \infty$, where the sequences obtain a white spectrum. The most lowpass sequence that can be generated using Bernoulli maps is the one obtained for $m = 2$. This is a very crucial limitation in the flexibility of Bernoulli maps. On the contrary, tent chaotic watermarks can generate any sequence with exponential autocorrelation function and thus, any desirable spectral characteristics.

Experimental results show that sequences produced by tent maps have superior performance, in terms of the ROC curve, compared to white pseudorandom and Bernoulli sequences attaining the same spectral properties. The theoretical ROC curves for white tent ($\alpha = 0.5$), pseudorandom white, lowpass tent ($\alpha = 0.6$) and lowpass Bernoulli ($m = 5$) are plotted in Figure **??**b. The experimental ROCs are also plotted in the same Figure and illustrate the accordance between theoretical and experimental results.

Another issue that is worth commenting, is the influence of the watermark embedding factor $p$ on the watermarking system performance. It can be observed in (19),(34) that, in both tent and pseudorandom watermarks, $p$ multiplies the correlation mean value for the correct watermark (event $H_0$). Therefore, the system performance improves with the the watermark embedding factor in both cases. However, expressions (19), (35) highlight that the correlation variance is also affected by the watermark embedding factor. The correlation variance for tent chaotic watermarks using different embedding factors is illustrated in Figure **??**. It is obvious that, as the watermark becomes stronger, the correlation variance decreases for event $H_0$ ($k = 0$) while it increases, but to smaller extent, for event $H_{1b}$ ($k \to \infty$). This is not the case with pseudorandom watermarks, where the correlation variance increases with the watermark embedding factor for both events $H_0$,$H_{1b}$, according to (19). In other words, an increase of $p$

results in the same performance improvement for both pseudorandom and tent watermarks, in what concerns the effect of the mean values. However, in what concerns the contribution of variance in the system performance, an increase of $p$ results in a decrease of performance for pseudorandom watermarks whereas for tent watermarks the performance increases. Thus the gap in the performance between white pseudorandom and white tent watermarks increases as $p$ increases.

Another important aspect that can be treated by exploiting the theoretical analysis presented in the previous Sections, is the minimum number of watermarked data samples required for a watermarking scheme based on correlation detection in order to achieve a certain prespecified performance. This number can be estimated by setting the desired $P_{fa}$ and $P_{fr}$ values in (9) and using (34), (35). The EER (operating state where $P_{fr} = P_{fa}$) versus the number of watermarked data samples is plotted in Figure **??**a for a system based on tent chaotic watermarks. It can be observed that the number of samples required, for a reliable watermarking scheme (e.g. EER $\approx 10^{-12}$), is 80000 for a highpass spectrum watermark and this number increases to 190000 samples for a white watermark. For a lowpass tent watermark, the minimum number is much larger. The influence of the test signal mean value in the watermark performance is also illustrated in this example (Figure **??**b). By subtracting the test signal mean value, the number of watermarked samples required reduces significantly. That is, 10000 samples are enough to ensure reliable watermark detection (EER $\approx 10^{-12}$) for a highpass tent watermark ($\alpha = 0.3$), whereas for white tent watermarks more than 15000 samples are required. The worst case occurs for lowpass tent watermarks where more than 35000 samples should be contained in the host signal. The issue of the minimum watermark sequence length that achieves a certain performance is very critical in multi-bit watermarking, where this number corresponds to the minimum number of samples needed for encrypting just one bit. The reader should bear in mind that, in order to encrypt a message consisting of L bits, one needs at least L times the number of samples derived above.

Experiments were conducted to investigate robustness of the pseudorandom and the chaotic sequences against mean filtering of window size 3. The ROC curves after mean filtering are plotted in Figure **??**. It can be observed that watermarks having lowpass characteristics (Bernoulli with $m = 5$, tent with $\alpha = 0.6$) attain better performance than white or highpass ones. The best performance is achieved using lowpass tent watermarks having $\alpha = 0.7$.

Finally, the argument that controllable spectral characteristics can be also obtained using prefiltered pseudorandom white sequences can be easily confronted. The advantage of Markov chaotic watermarks is that no prefiltering is required and the probability distribution of the generated samples is not affected (when it is chosen to be the invariant density of the map) by the modification of the sequence spectral characteristics. In the case of tent chaotic watermarks, this distribution is uniform regardless of the sequence spectral characteristics. On the contrary, prefiltering of pseudorandom watermarks modifies their initial uniform distribution. Thus, filtered watermarks with long tailed probability density function can result, increasing the risk of obtaining perceptible watermarks. Moreover, generating uniformly distributed sequences with predefined first, second and third order correlation statistics by filtering pseudorandom sequences is a very complicated task.

## VIII. Conclusions

In this paper, chaotic watermarks generated by Markov maps are introduced and their statistical properties related to watermarking are investigated. Furthermore, statistical analysis of the employed correlation detector is undertaken, leading to a number of important observations on the watermarking system detection performance. Highpass chaotic watermarks prove to perform better than white ones, whereas lowpass watermarks have the worst performance when no distortion is inflicted on the watermarked signal. The controllable spectral/correlation properties of Markov chaotic watermarks prove to be very important for the overall system performance. Moreover, Markov maps that have appropriate second and third order correlation statistics, like the skew tent map, perform better than sequences with the same spectral properties generated by either Bernoulli or pseudorandom number generators.

# Appendix A

In order to estimate the correlation statistics for sequences generated by skew tent maps, we must first derive the FP matrix for this map. According to (10) and (11), the highest order correlation required for evaluating the mean value and the variance of the detector in a watermarking system is of third order and thus, the corresponding FP matrix needed is $\boldsymbol{P}_3$. This matrix can be derived in a straightforward manner using the definitions in [32].

$$\boldsymbol{P}_3 = \begin{bmatrix} \alpha & 1-\alpha & 0 & 1-\alpha & 0 & 1-\alpha & 0 & 1-\alpha \\ \alpha & 1-\alpha & 0 & 1-\alpha & 0 & 1-\alpha & 0 & 1-\alpha \\ 0 & 0 & \alpha^2 & -(\alpha-1)^2 & 0 & -2\,(\alpha-1)^2 & 0 & -3\,(\alpha-1)^2 \\ 0 & 0 & \alpha^2 & -(\alpha-1)^2 & 0 & -2\,(\alpha-1)^2 & 0 & -3\,(\alpha-1)^2 \\ 0 & 0 & 0 & 0 & \alpha^3 & -(\alpha-1)^3 & 0 & -3\,(\alpha-1)^3 \\ 0 & 0 & 0 & 0 & \alpha^3 & -(\alpha-1)^3 & 0 & -3\,(\alpha-1)^3 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^4 & -(\alpha-1)^4 \\ 0 & 0 & 0 & 0 & 0 & 0 & \alpha^4 & -(\alpha-1)^4 \end{bmatrix} \tag{A-1}$$

where $\alpha$ is the parameter of the map. The corresponding correlation basis matrix is:

$$\boldsymbol{M}_3 = \begin{bmatrix} \alpha & 0 & \frac{\alpha^2}{2} & 0 & \frac{\alpha^3}{3} & 0 & \frac{\alpha^4}{4} & 0 \\ 0 & 1-\alpha & 0 & \frac{1-\alpha^2}{2} & 0 & \frac{1-\alpha^3}{3} & 0 & \frac{1-\alpha^4}{4} \\ \frac{\alpha^2}{2} & 0 & \frac{\alpha^3}{3} & 0 & \frac{\alpha^4}{4} & 0 & \frac{\alpha^5}{5} & 0 \\ 0 & \frac{1-\alpha^2}{2} & 0 & \frac{1-\alpha^3}{3} & 0 & \frac{1-\alpha^4}{4} & 0 & \frac{1-\alpha^5}{5} \\ \frac{\alpha^3}{3} & 0 & \frac{\alpha^4}{4} & 0 & \frac{\alpha^5}{5} & 0 & \frac{\alpha^6}{6} & 0 \\ 0 & \frac{1-\alpha^3}{3} & 0 & \frac{1-\alpha^4}{4} & 0 & \frac{1-\alpha^5}{5} & 0 & \frac{1-\alpha^6}{6} \\ \frac{\alpha^4}{4} & 0 & \frac{\alpha^5}{5} & 0 & \frac{\alpha^6}{6} & 0 & \frac{\alpha^7}{7} & 0 \\ 0 & \frac{1-\alpha^4}{4} & 0 & \frac{1-\alpha^5}{5} & 0 & \frac{1-\alpha^6}{6} & 0 & \frac{1-\alpha^7}{7} \end{bmatrix} \tag{A-2}$$

In order to facilitate the calculations and derive closed form expressions for the correlation statistics, the FP matrix must be expressed in the form

$$\boldsymbol{P}_3 = \boldsymbol{V}\boldsymbol{E}\boldsymbol{V}^{-1} \tag{A-3}$$

where $\boldsymbol{V}$ is the generalized eigenvectors matrix and $\boldsymbol{E} = \mathrm{diag}(\boldsymbol{e})$ is the diagonal matrix of the corresponding eigenvalues. The eigenvalues of $\boldsymbol{P}_3$ are:

$$\boldsymbol{e} = \begin{bmatrix} e_1 & e_2 & \dots & e_8 \end{bmatrix} = \begin{bmatrix} 1 - 3\,\alpha + 3\,\alpha^2 & -1 + 2\alpha & 4\,\alpha^3 - 6\,\alpha^2 + 4\,\alpha - 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{A-4}$$

and the corresponding eigenvectors are the columns of

$$\boldsymbol{V} = \begin{bmatrix} 1 & 1 & 1 & 1 & \frac{a-1}{a} & \frac{a-1}{a} & \frac{a-1}{a} & \frac{a-1}{a} \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 6\,a - 6 & -2 & 6\,a - 6 & 0 & 0 & 2\,\frac{(a-1)^2}{a^2} & 3\,\frac{(a-1)^2}{a^2} & \frac{(a-1)^2}{a^2} \\ 6\,a - 6 & -2 & 6\,a - 6 & 0 & 0 & 0 & 0 & 1 \\ -9\,a + 6 & 0 & 12\,(a-1)^2 & 0 & 0 & \frac{(a-1)^3}{a^3} & 3\,\frac{(a-1)^3}{a^3} & 0 \\ -9\,a + 6 & 0 & 12\,(a-1)^2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -16\,a^2 + 20\,a - 8 & 0 & 0 & 0 & \frac{(a-1)^4}{a^4} & 0 \\ 0 & 0 & -16\,a^2 + 20\,a - 8 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{A-5}$$

The objective is to calculate correlation statistics of the form:

$$R_t[y_1, y_2, \cdots, y_r] = E\left[t[n]t[n+y_1]t[n+y_2]\dots t[n+y_r]\right] = \int g_1(x)g_2(x)\,dx \tag{A-6}$$

where

$$g_1(x) = x \tag{A-7}$$

$$g_2(x) = P_t^{y_r - y_{r-1}}\{x \cdots P_t^{y_2 - y_1}\{xP_t^{y_1}\{xp(x)\}\}\cdots\} \tag{A-8}$$

where $p(\cdot)$ is the invariant density of the Markov map, which in the case of tent maps is uniform. In matrix notation, the correlation is given by:

$$R_t[y_1, y_2, \cdots, y_r] = \boldsymbol{g}_1^T \boldsymbol{M} \boldsymbol{g}_2 \tag{A-9}$$

where

$$\boldsymbol{g}_1 = \boldsymbol{g} = [0 \;\; 0 \;\; 1 \;\; 1 \;\; 0 \;\; 0 \;\; 0 \;\; 0\;] \tag{A-10}$$

is the coordinate vector of $g(x) = x$ and

$$\boldsymbol{g}_2 = \boldsymbol{P}^{y_r - y_{r-1}}(\boldsymbol{g} \odot \cdots \odot \boldsymbol{P}^{y_2 - y_1}(\boldsymbol{g} \odot \boldsymbol{P}^{y_1}\boldsymbol{g})\cdots) \tag{A-11}$$

In the previous formula $\boldsymbol{P}$, $\boldsymbol{M}$ are the FP and the correlation basis matrices of sufficient dimension, respectively, and $\odot$ denotes the polynomial product operator. For two coordinate vectors $\boldsymbol{u}_1, \boldsymbol{u}_2$, the notation $\boldsymbol{u}_1 \odot \boldsymbol{u}_2$ denotes the coordinate vector of the corresponding product of piecewise polynomials $u_1(x), u_2(x)$ in a basis of suitably high dimension. Let $y_{(k)}$ be the $k$-th order statistic of the samples $y_1, y_2, \ldots, y_N$, where $y_{(0)} = \min\{\boldsymbol{y}\}$, $y_{(N-1)} = \max\{\boldsymbol{y}\}$. The correlation statistics of first, second and third order for tent sequences can be derived in closed form using A-9:

$$\begin{aligned}
R_t[y_1] &= \frac{1}{4} + \frac{1}{12} e_2^{y_{(0)}} && \text{(A-12)} \\
R_t[y_1, y_2] &= \frac{1}{8} + \frac{1}{24}\left(e_2^{y_{(0)}} + e_2^{y_{(1)}} + e_2^{(y_{(1)}-y_{(0)})}\right) + \frac{a}{12h} e_2^{y_{(0)}}\left(e_1^{(y_{(1)}-y_{(0)})} - e_2^{(y_{(1)}-y_{(0)})}\right) && \text{(A-13)} \\
R_t[y_1, y_2, y_3] &= \frac{1}{16} + \frac{1}{48}\left(e_2^{y_{(0)}} + e_2^{(y_{(1)}-y_{(0)})} + e_2^{(y_{(2)}-y_{(1)})}\right) + \frac{1}{144}(e_2^{y_{(1)}} + e_2^{(y_{(2)}-y_{(1)}+y_{(0)})} + e_2^{(y_{(2)}-y_{(0)})}) + \\
&\quad \frac{1}{72}(e_1^{(y_{(2)}-y_{(1)})} e_2^{(y_{(1)}-y_{(0)})} + e_2^{y_{(0)}} e_1^{(y_{(1)}-y_{(0)})}) + \frac{1}{216}(e_2^{(y_{(2)}-y_{(1)}+y_{(0)})} e_1^{(y_{(1)}-y_{(0)})} + e_2^{y_{(1)}} e_1^{(y_{(2)}-y_{(1)})}) + \\
&\quad \frac{1}{432} e_2^{y_{(2)}} - \frac{1}{54} e_2^{y_{(0)}} e_1^{(y_{(2)}-y_{(0)})} + \\
&\quad \frac{1}{36h}(e_1^{(y_{(2)}-y_{(1)})} e_2^{(y_{(1)}-y_{(0)})} - e_2^{(y_{(2)}-y_{(0)})} + e_2^{y_{(0)}} e_1^{(y_{(1)}-y_{(0)})} - e_2^{y_{(1)}}) - && \text{(A-14)} \\
&\quad \frac{1}{54h}(e_2^{y_{(0)}} e_1^{(y_{(2)}-y_{(0)})} + e_2^{y_{(2)}}) - \frac{1}{108h} e_2^{y_{(1)}} e_1^{(y_{(2)}-y_{(1)})} + \frac{1}{216h} e_2^{(y_{(2)}-y_{(1)}+y_{(0)})} e_1^{(y_{(1)}-y_{(0)})} + \\
&\quad \frac{1}{27h^2}(e_2^{y_{(2)}} + e_2^{y_{(0)}} e_1^{(y_{(2)}-y_{(0)})} - e_2^{y_{(1)}} e_1^{(y_{(2)}-y_{(1)})} - e_2^{(y_{(2)}-y_{(1)}+y_{(0)})} e_1^{(y_{(1)}-y_{(0)})}) + \\
&\quad \frac{1+2a^2}{40v_1} e_2^{y_{(0)}} e_1^{(y_{(1)}-y_{(0)})} e_3^{(y_{(2)}-y_{(1)})} + \frac{a(a-1)^2}{4hv_1} e_1^{(y_{(2)}-y_{(0)})} e_2^{y_{(0)}}
\end{aligned}$$

where $h = 3\alpha - 2$ and $v_1 = 4\alpha^2 - 5\alpha + 2$. Moreover, correlation statistics for the special case (37) are:

$$\begin{aligned}
R_t[m] &= \frac{1}{4} + \frac{1}{12} e_2^m && \text{(A-15)} \\
R_t[m, m] &= \frac{1}{6} + \frac{1}{12} e_2^m && \text{(A-16)} \\
R_t[0, m] &= \frac{1}{6} + \frac{\alpha - 1}{6(3\alpha - 2)} e_2^m + \frac{\alpha}{12(3\alpha - 2)} e_1^m && \text{(A-17)} \\
R_t[0, m, m] &= \frac{1}{9} + \frac{\alpha - 1}{6(3\alpha - 2)} e_2^m + \frac{9\alpha - 1}{90(3\alpha - 2)} e_1^m && \text{(A-18)}
\end{aligned}$$

# References

[1] I.J. Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, December 1997.

[2] J.K. Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Elsevier Signal Processing, Sp. Issue on Copyright Protection and Access control*, vol. 66, no. 3, pp. 303–317, 1998.

[3] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Elsevier Signal Processing, Sp. Issue on Copyright Protection and Access control*, vol. 66, no. 3, pp. 385–403, May 1998.

[4] C.-Y. Lin M. Wu J. Bloom I. Cox M. Miller Y. Lui, "Rotation, scale, and translation resilient watermarking for images," *IEEE Transactions on Image Processing*, vol. 10, no. 5, pp. 767–782, May 2001.

[5] Y. Wang J. Doherty and R. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Transactions on Image Processing*, vol. 11, no. 2, pp. 77–88, February 2002.

[6] A.Nikolaidis and I.Pitas, "Robust watermarking of facial images based on salient geometric pattern matching," *IEEE Trans. on Image Processing*, vol. 2, no. 3, pp. 172–184, September 2000.

[7] A. Tefas and I. Pitas, "Robust spatial image watermarking using progressive detection," in *Proc. of 2001 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2001)*.

[8] M. Barni, F. Bartolini, V. Cappelini, and A. Piva, "A DCT-domain system for robust image watermarking," *Elsevier Signal Processing*, vol. 66, no. 3, pp. 357–372, 1998.

[9] V.Solachidis and I.Pitas, "Circularly symmetric watermark embeddong in 2-d dft domain," *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1741–1753, 2001.

[10] S. Pereira, J. Ruanaidh, F. Deguillaume, G. Csurka, and T. Pun, "Template based recovery of fourier-based watermarks using log-polar and log-log maps," in *Proc. of ICMCS'99*, Florence, Italy, 7-11 June 1999, vol. I, pp. 870–874.

[11] S. Tsekeridou and I. Pitas, "Embedding self-similar watermarks in the wavelet domain," in *Proc. of ICASSP'00*, Istanbul, Turkey, 5-9 June 2000.

[12] J. Ó Ruanaidh, W.J. Dowling, and F.M. Boland, "Phase watermarking of digital images," in *Proc. of ICIP'96*, Lausanne, Switzerland, September 1996, vol. III, pp. 239–242.

[13] N. Nikolaidis and I. Pitas, "Digital image watermarking: an overview," in *Int. Conf. on Multimedia Computing and Systems (ICMCS'99)*, Florence, Italy, 7-11 June 1999, vol. I, pp. 1–6.

[14] M.D. Swanson, M. Kobayashi, and A.H. Tewfik, "Multimedia data embedding and watermarking technologies," *Proceedings of the IEEE*, vol. 86, no. 6, pp. 1064–1087, June 1998.

[15] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1079–1107, July 1999.

[16] F.A.P. Petitcolas, R.J Anderson, and M.G. Kuhn, "Information hiding - a survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, July 1999.

[17] I. Cox M. Miller J. Bloom, *Digital Watermarking*, Morgan Kaufmann, San Francisco, CA, 2002.

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

[19] J.R. Hernandez and F. Perez-Gonzalez, "Statistical analysis of watermarking schemes for copyright protection of images," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1142–1166, July 1999.

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

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

[22] 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*, Oregon, USA, April 1998, pp. 329–343.

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

[24] 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, vol. V, pp. 509–512.

[25] 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.

[26] N. Nikolaidis, S. Tsekeridou, A. Nikolaidis, A. Tefas, V. Solachidis, and I. Pitas, "Applications of chaotic signal processing techniques to multimedia watermarking," in *Proceedings of the IEEE workshop on Nonlinear Dynamics in Electronic Systems*, Catania Italy, May 18-20 2000, pp. 1–7.

[27] N. Jayant P. Noll, *Digital Coding of Waveforms*, Prentice Hall, Englewood Cliffs, NJ, 1984.

[28] Athanasios Papoulis, *Probability, random variables, and stochastic proccesses*, McGraw-hill, New York, 1991.

[29] A. Lasota and M.C. Mackey, *Probabilistic Properties of Deterministic Systems*, Cambridge Univ. Press, 1985.

[30] A. Boyarsky and M. Scarowsky, "On a class of transformations which have unique absolutely continues invariant measures," *Trans. Amer. Math. Soc.*, vol. 255, pp. 243–262, 1979.

[31] R. Kalman, "Nonlinear aspects of sampled-data control systems," in *Proc. Symp. Nonlinear Circuit Analysis*, April 1956, pp. 273–313.

[32] S.H. Isabelle and G.W. Wornell, "Statistical analysis and spectral estimation techniques for one-dimensional chaotic signals," *IEEE Trans. on Signal Processing*, vol. 45, no. 6, pp. 1495–1506, June 1997.

[33] T. Kohda, H Fujisaki, and S. Ideue, "On distributions of correlation values of spreading sequences based on markov information sources," in *Proc. of ISCAS'00*, Geneva, Switzerland, 28-31 May 2000, vol. V, pp. 225–228.

[34] T. Schimming, M Gotz, and W. Schwarz, "Signal modeling using piecewise linear chaotic generators," in

*Proc. of EUSIPCO'98*, Rodos, Greece, 8-11 September 1998, pp. 1377–1380.

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

[36] S. N. Rasband, *Chaotic Dynamics of Nonlinear Systems*, John Wiley & Sons, New York, 1990.

[37] M. Kutter, F. Jordan, and F. Bossen, "Digital watermarking of color images using amplitude modulation," *SPIE Journal of Electronic Imaging*, vol. 7, no. 2, pp. 326–332, 1998.

[38] V. Solachidis and I. Pitas, "Circularly symmetric watermark embedding in 2-d dft domain," in *Proc. of ICASPP'99*, Phoenix, Arizona, USA, 15-19 March 1999.