MARKOV CHAOTIC SEQUENCES FOR CORRELATION BASED WATERMARKING SCHEMES

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

Department of Informatics, Aristotle University of Thessaloniki
Box 451, Thessaloniki 540 06, GREECE, `pitas@zeus.csd.auth.gr`

ABSTRACT

In this paper, statistical analysis of watermarking schemes based on correlation detection is presented. Statistical properties of watermark sequences generated by piecewise-linear Markov maps are exploited, resulting in superior watermark detection reliability. Correlation/spectral properties of such sequences are easily controllable, a fact that affects the watermarking system performance. A family of chaotic maps, namely the skew tent map family, is proposed for use in watermarking schemes.

1. INTRODUCTION

The design of robust techniques for copyright protection and content verification of multimedia data became an urgent necessity in the last years. 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. For a review of existing schemes and a detailed discussion on the main requirements of a watermarking scheme, the interested reader may consult [1].

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 [2, 3, 4]. In these papers, the statistical properties of watermarking schemes based on pseudorandom watermark signals and correlation detectors, among others, are derived. In [3], 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. An overview of chaotic watermarking techniques can be found in [5]. However, up to now, their performance has been evaluated solely within an experimental framework. The system is modeled in a communication framework considering the host signal as interference and converting the addressed problem to detection of the underlying watermark signal.

2. WATERMARKING SYSTEM MODEL

The watermark generation functional block aims at constructing a sequence $\boldsymbol{w}$, $w[i] \in \mathcal{R}$, of N samples using an appropriate function g, $\boldsymbol{w} = G(K, N)$, where K denotes the watermark key that corresponds to the host signal owner/copyright holder. Watermark embedding aims at inserting the watermark signal $\boldsymbol{w}$ in the host signal $\boldsymbol{f}$ in a way that ensures imperceptibility and robustness under intentional or unintentional attacks. For the model under study, additive watermark embedding is assumed: $\boldsymbol{f}_w = \boldsymbol{f} + p\boldsymbol{w}$, 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.

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., $\boldsymbol{f}_t = \boldsymbol{f}_o$

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

$$\boldsymbol{f}_t = \boldsymbol{f}_o + p\boldsymbol{w}_e \tag{1}$$

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}).

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:

$$c = \frac{1}{N}\sum_{n=0}^{N-1} f_t[n]w_d[n] = \frac{1}{N}\sum_{n=0}^{N-1}(f_o[n]w_d[n] + pw_e[n]w_d[n]) \tag{2}$$

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). The plot of P_{fa} versus P_{fr} is called the *receiver operating characteristics* (ROC) curve of the corresponding watermarking system. This curve conveys all the necessary system performance information.

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

For the watermark sequences that will be studied in this paper, i.e., the sequences generated by piecewise linear Markov maps,the correlation output is normally distributed (see Section 3). Thus, it can be fully determined in terms of its mean $\mu_{c|H_0}$, $\mu_{c|H_1}$, and variance $\sigma^2_{c|H_0}$, $\sigma^2_{c|H_1}$, which can be derived in a straightforward manner:

$$\mu_c = E[c] = \frac{1}{N}\sum_{n=0}^{N-1} E[f_o[n]]E[w_d[n]] + \frac{1}{N}\sum_{n=0}^{N-1} pE\left[w_e[n]w_d[n]\right] \tag{3}$$

$$\begin{aligned}\sigma_c^2 = \quad & E[c^2] - E[c]^2 = \frac{1}{N^2}\Bigg[\sum_{n=0}^{N-1}\big(E[f_o^2[n]]E[w_d^2[n]] + \\ & p^2E[w_d^2[n]w_e^2[n]] + 2pE[f_o[n]]E[w_e[n]w_d^2[n]]\big) + \\ & \sum_{n=0}^{N-1}\sum_{m=0,m\neq n}^{N-1}\big(E[f_o[n]f_o[m]]E[w_d[n]w_d[m]] + \\ & pE[f_o[n]]E[w_d[n]w_e[m]w_d[m]] + \\ & pE[f_o[m]]E[w_e[n]w_d[m]w_d[n]] + \\ & p^2E[w_e[n]w_e[m]w_d[n]w_d[m]]\big)\Bigg] - \mu_c^2\end{aligned} \tag{4}$$

Note that these expressions can be used to represent μ_c, σ_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 (3), (4), one can easily conclude that several moments 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. Let us denote by $R_g[\boldsymbol{k}]$ the statistic of the form:

$$R_g[k_1, k_2, \ldots, k_r] = E\left[g[n]g[n+k_1]g[n+k_2]\ldots g[n+k_r]\right] \tag{5}$$

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. Furthermore, a first order exponential autocorrelation function model will be assumed [4]:

$$R_{f_o}[k] = \mu_{f_o}^2 + \sigma_{f_o}^2\beta^k, \quad k \geq 0, \ |\beta| \leq 1 \tag{6}$$

where β is the parameter of the autocorrelation function and $\sigma^2_{f_o}$ is the host signal variance.

3. EMPLOYING CHAOTIC SEQUENCES IN WATERMARKING SCHEMES

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. The notation $f^n(x[0])$ is used to denote the n-th application of the map $f(\cdot)$.

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

$$p_n(\cdot) = P_f\{p_{n-1}(\cdot)\} = P_f^n\{p_0(\cdot)\} \tag{7}$$

This operator, which is referred to as the Frobenius-Perron (FP) operator [6], 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 does not change, i.e.,

$$p(\cdot) = P_f^n\{p(\cdot)\}, \quad \forall n \tag{8}$$

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. The invariant density plays an important role in the computation of time-averaged statistics of time series from nonlinear dynamics.

A rich class of 1-D chaotic systems that are particularly amenable to analysis are the eventually expanding, piecewise-linear Markov maps. The statistics of Markov maps can be determined in closed form. For a detailed definition of the matrices and vectors involved in statistics calculations that will be used in the sequel, one may consult [7], where, a strategy for computing these statistics, was developed. By using the FP matrix, the higher order correlation statistics of Markov maps can be derived.

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 be an integer $k > 0$ such that:

$$x[0] = f^k(y[0]) \quad \text{or} \quad y[0] = f^k(x[0]) \tag{9}$$

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

$$y[n] = f^n(y[0]) = f^n(f^k(x[0])) = x[n+k] \ \text{ or } \ x[n] = y[n+k] \tag{10}$$

Constant k will be called from now on 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:

$$\boldsymbol{w} = \boldsymbol{x} - d\mathbf{1} \tag{11}$$

where d is a constant that controls the range of the watermark sequence, and $\mathbf{1}$ is the unit vector. By substituting (11) in (3) and (4) and considering that $w_d[n] = w_e[n+k]$, according to (10), it is straightforward to derive the mean value and the variance of the correlation c. 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 [4], results in better system performance. Moreover, by subtracting the test signal mean value prior to detection, we can decrease the variance of the correlation, thus obtaining better system performance. 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 are given by:

$$\mu_c = p(R_x[k] - \mu_x^2) \tag{12}$$

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

$$+\frac{1}{N^2}\sum_{m=0}^{N-1}(N-m)(2-\delta(m))(R_x[m]-\mu_x^2)R_{f_o}[m]-$$
$$p^2(R_x[k]-2\mu_x^2)^2 \tag{13}$$

where $\delta(m)$ is the Dirac delta function, μ_x is the mean value of the chaotic sequence and $R[\boldsymbol{k}]$ is given by (5).

Expressions (12) and (13) are sufficiently broad to include all events that occur in the watermarking model described in Section 2, 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 positive watermark embedding factor and $k = 0$ in the case of right 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 (12) and (13) can be derived in closed form or evaluated numerically [7].

Although samples of Markov chaotic watermarks are correlated for small $k > 0$, since they posses 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 [8] may be used in order to establish that the correlation c in eq. (2) 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 μ_c and σ_c^2, given by eqs. (12) and (13) respectively, converge to constant values for large k. In such a case, $P_{fa|H_{1b}}$ substitutes $P_{fa|H_1}$ since it is the worst case and it can be estimated using the limit values ($k \to \infty$) of μ_c and σ_c^2. P_{fr} values are estimated using the values of μ_c and σ_c^2 for $k = 0$ (event H_0).

Moreover, if we examine in detail the mean value of the correlation given by (12) 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 (13), this can be achieved by utilizing watermark signals with suitable first, second and third order correlation statistics.

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) which is given by:

$$S_x(\omega) = \sum_{k=-\infty}^{\infty} R_x[k]e^{-j\omega k} = R_x[0]+\sum_{k=1}^{\infty} R_x[k]\left(e^{-j\omega k}+e^{j\omega k}\right) \tag{14}$$

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 (6), it can be easily derived that the correlation variance given by (13) 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 (14) 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.

4. 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 can be expressed as:

$$\mathcal{T}:[0,1]\to[0,1] \tag{15}$$
$$\mathcal{T}(x) = \begin{cases} \frac{1}{\alpha}\,x & ,\ 0 \le x \le \alpha \\ \frac{1}{\alpha-1}\,x + \frac{1}{1-\alpha} & ,\ \alpha < x \le 1 \end{cases} \quad ,\ \alpha \in (0,1)$$

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

$$t[k] = \mathcal{T}(t[k-1]) = \mathcal{T}^k(t[0]) \tag{16}$$

The invariant density of the skew tent map is uniform. Following the methodology described in [7], 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 easily evaluated [7]. The nonzero eigenvalues of the Frobenius-Perron matrix $\boldsymbol{P}_3$ are:

$$\boldsymbol{e} = \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \end{bmatrix} = \begin{bmatrix} 1-3\,\alpha+3\,\alpha^2 \\ -1+2\alpha \\ 4\,\alpha^3-6\,\alpha^2+4\,\alpha-1 \\ 1 \end{bmatrix} \tag{17}$$

and the first order correlation statistic (autocorrelation function) is given by:

$$R_t[k] = \frac{1}{4}+\frac{1}{12}e_2^k = \frac{1}{4}+\frac{1}{12}(2\alpha-1)^k \tag{18}$$

It can be observed that the autocorrelation function depends only on the parameter α of the skew tent map. Thus, by controlling the parameter α we can generate sequences having any desirable exponential autocorrelation function. Using (14), (18), the power spectral density of the skew tent map sequences can be shown to be:

$$S_t(\omega) = \frac{1-e_2^2}{12(1+e_2^2-2e_2\cos\omega)} \tag{19}$$

Thus, by varying the parameter α 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 posses 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, one can derive the mean value and the variance of the correlation detector for this map:

$$\mu_c = \begin{cases} 0 & , \quad p = 0 \ (H_{1a}) \\ \frac{p}{12} & , \quad k = 0, p \neq 0 \ (H_0) \end{cases} \tag{20}$$

$$\sigma_c^2 = \begin{cases} \frac{\sigma_{f_o}^2}{12N^2} \frac{N - 2\beta e_2 - N\beta^2 e_2^2 + 2(\beta e_2)^{N+1}}{(1-\beta e_2)^2} & , p = 0 \ (H_{1a}) \\ \frac{p^2}{180N^2} \frac{N - 2e_1 - Ne_1^2 + 2e_1^{N+1}}{(1-e_1)^2} + \\ \frac{\sigma_{f_o}^2}{12N^2} \frac{N - 2\beta e_2 - N\beta^2 e_2^2 + 2(\beta e_2)^{N+1}}{(1-\beta e_2)^2} & , k = 0, p \neq 0 \ (H_0) \end{cases} \tag{21}$$

where β is the parameter of the host signal autocorrelation function given by (6).

5. EXPERIMENTAL RESULTS

In order to experimentally verify the theoretical performance analysis of a watermarking system based on correlation detection, the system is fed with a host signal that is compliant with the autocorrelation model in (6). More specifically, the system is fed with a uniformly-distributed zero mean random white signal of 45000 samples that has been pre-filtered with an IIR filter having system function $H(z) = \frac{1-\beta}{1-\beta z^{-1}}$. Such prefiltering generates a signal exhibiting an autocorrelation function of the form $R_f[k] = \frac{1-\beta}{1+\beta}\sigma_f^2 \beta^k$ which is equivalent to the model in (6) for $\mu_{f_o} = 0$ and filtered signal variance $\frac{1-\beta}{1+\beta}\sigma_f^2$. In the filtered signal a constant value is added that serves as the mean value of the final host signal. The host signal was generated having standard deviation 30, mean value 100 and autocorrelation parameter (see (6)) equal to 0.95.

The spectrum of tent chaotic watermarks is highpass for small values of the map parameter α, becomes white for $\alpha = 0.5$ and tends to lowpass as $\alpha \rightarrow 1$. 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}).

The influence of the map parameter α on the watermarking system performance was also considered. The ROC curves for lowpass ($\alpha = 0.7$), white ($\alpha = 0.5$) and highpass ($\alpha = 0.3$) skew tent chaotic watermarks were theoretically and experimentally evaluated. The superior performance of the highpass tent chaotic watermarks can be easily observed in Figure 1. The performance of the watermarking system is considerably inferior for white tent watermarks whereas the worst performance is observed when lowpass watermarks are used. However, 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, the watermark becomes robust to lowpass attacks while retaining its correlation properties.

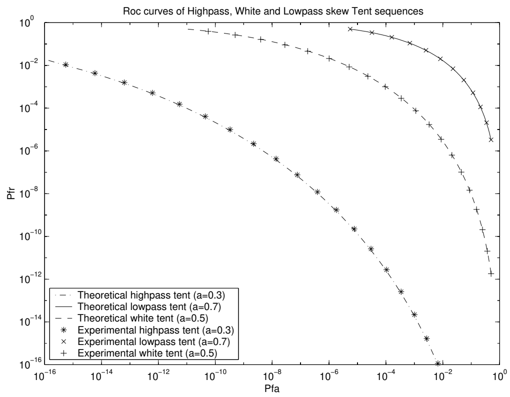

Fig. 1. Receiver Operating Characteristics for watermarking schemes based on highpass, lowpass and white skew tent chaotic watermarks.

6. CONCLUSIONS

In this paper, chaotic watermarks generated by Markov maps are introduced and their watermarking related statistical properties are investigated. Furthermore, statistical analysis of the employed correlation detector is undertaken leading to a number of important observations concerning the watermarking system detection reliability. 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.

7. REFERENCES

[1] "Identification & protection of multimedia information," *Special issue on Proceedings of the IEEE*, vol. 87, no. 7, July 1999.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

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

[7] 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.

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