SIDE-INFORMED WATERMARKING USING NTH-ORDER POLYNOMIAL DETECTORS

N.J. Hurley[†], G.C.M. Silvestre[†] and T. Furon[‡]
[†]University College Dublin, Ireland
[‡]Université Catholique de Louvain, Belgium

ABSTRACT

Most recent watermarking schemes differ from symmetric schemes in that the detection process does not require the use of the same private key in both the embedder and the detector. An advantage of such schemes is that estimation of the watermark by collusion attack is rendered impossible, so that the overall system is more secure. Almost all second generation schemes to date are also second-order; that is, they are based on the computation of a quadratic form in the detector. In this work, the authors propose a new class of watermarking schemes which employ an n^{th}-order detection process. The scheme is based on a generalised differential modulation scheme. We address the question of how to choose the watermark signal in order to optimise the output of the detection and examine the efficiency and security of this new class of schemes.

1 INTRODUCTION

Digital media contents, such as audio, images or video data, can now be distributed quickly and economically by means of the Internet. However the widespread adoption of electronic distribution by the software industry has been impeded by the fear of copyright infringements and illicit dissemination. In this context, digital watermarking has emerged as a promising technique to combat such piracy by embedding hidden information into digital media contents which can be used by copy-protection systems. The embedding process should not adversely affect the quality of the contents. In addition, it should be possible to detect robustly the watermark using an authorised detector, even in cases where contents have undergone transformation, such as compression or digital-to-analog conversion.

Watermarking can be understood as a communications problem in which the media contents constitutes the channel for transmission of the watermark data [1]. The watermarking embedder seeks to exploit capacity in the channel due to limitations in the human auditory or visual system. Watermarking algorithms are therefore in direct competition with lossy encoders such as MPEG [2] algorithms. In addition, large interference and deformation of the channel may result from coders, signal processing operations or malicious attacks, and seriously narrow the capacity.

1.1 Blind, Symmetric and Asymmetric Watermarking

First generation state-of-the-art watermarking schemes are *blind* and *symmetric*. In blind schemes, decoding is achieved without recourse to the original signal. In symmetric schemes, the embedding of watermark information depends on a private key which is also available at the detector. Spread-spectrum watermarking [3, 4] is the most common form of blind, symmetric watermarking. A pseudo-random signal, $\mathbf{z}$, is modulated on the original contents and detection relies on an hypothesis test on the result of a correlation of the received signal with $\mathbf{z}$. Hence, the signal $\mathbf{z}$ can be considered as a private key, which must be available to both the embedder and detector. The symmetry of such schemes presents a weakness from the security point-of-view. In typical copy-protection framework, the same detector must be able to detect watermarks in lots of different contents. It is then possible for an attacker to estimate the private key by averaging a set of contents marked using the same key in a so-called collusion attack. Hence, much recent watermarking research has focused on *asymmetric* watermarking schemes [5, 6], where the detection key is different from the embedding key. For secure schemes, the sole knowledge of the detection key should now be insufficient to determine the embedding key.

In a unified analysis of asymmetric watermarking schemes, Furon [7] showed that the asymmetric schemes proposed to date are second-order schemes, in that the detector determines the presence of the watermark by calculating a quadratic form on the received signal. Furon also showed that no scheme proposed to date is fully secure in a *public-key* sense. If an attacker has full knowledge of the detection process, then it is possible to remove the watermark while maintaining the quality of the original contents.

In this paper, we propose to use a higher-order detection scheme with an aim towards increased robustness and security. By chosing the watermark signal to maximise the detection power, we show that it is possible to achieve greater efficiency with our high-order scheme. Moreover, the technique is also robust to collusion attacks and and exhibits increased security for certain other types of attacks. Section 2 of the paper outlines the original differential scheme [8] on which our new class of schemes is based. The following section generalises the scheme to an n^{th}-order. The efficiency of n^{th}-order schemes is examined in Sections 5 and some experimental results are described in Section 7.

2 SECOND-ORDER DIFFERENTIAL MODULATION

A differential modulation watermarking scheme was presented in [8, 9]. A similar differential scheme was proposed also by Smith and Dodge [10]. These techniques can be summarised as follows:

Given the original content $\mathbf{s}$, a vector $\mathbf{r}$ of dimension N is extracted from $\mathbf{s}$. A permutation π is applied to the components of $\mathbf{r}$ producing $\tilde{\mathbf{r}} = \mathbf{r}^T\Pi$. A central, random watermark signal $\mathbf{w}$ is then modulated on $\tilde{\mathbf{r}}$ using a mixing function $F(\tilde{\mathbf{r}}, g\mathbf{w})$ and the resulting vector $\mathbf{r_w}$ is embedded back into the original content. For simplicity, the embedding strength is taken to be constant and given by the scalar g. The watermark signal $\mathbf{w}$ is constructed with a special property such that

$$w(i + N/2) = w(i) \quad \text{for} \quad 1 \leq i \leq N/2 \tag{1}$$

Assuming that $\tilde{\mathbf{r}}$ has zero expectation and that $\mathbf{w}$ and $\tilde{\mathbf{r}}$ are independent, the autocorrelation

$$R(\tau) = \sum_{i=1}^{N/2} \tilde{r}_w(i)\tilde{r}_w(i+\tau) \tag{2}$$

has a non-zero expectation proportional to $E\{w^2\}$ for τ=$N/2$. Hence, the detector determines the presence of a watermark through an hypothesis test $R(N/2) \gtrless Th$ where Th is a threshold set with consideration of the probability of false detection. It has been shown [7] that this detection scheme can be written as the quadratic form $\mathbf{r}^T A\mathbf{r} \gtrless Th$ where

$$A = \Pi^T \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \Pi \tag{3}$$

and I is the $N/2 \times N/2$ dimensional identity matrix.

As a result, the differential scheme is a second-order detection scheme and is thus more secure to attack than first-order symmetric schemes [7]. It is possible to generalise such differential process to produce higher order schemes as proposed in the next Section. The security and robustness of the generalised scheme are also examined

3 GENERALISED NTH-ORDER DIFFERENTIAL MODULATION

A *differential correlation* of length S is a sum of the form

$$d(\mathbf{r}, i, S) = r_i r_{i+S/2} + r_{i+1} r_{i+1+S/2} + \cdots + r_{i+S/2-1} r_{i+S} \tag{4}$$

Given a vector $\mathbf{r^{(0)}}$ of length $N = TS$, it is possible to reduce it to a vector $\mathbf{r^{(1)}}$ of T components, where the i^{th} component is

$$r_i^{(1)} = d(\mathbf{r^{(0)}}, iS, S)\,. \tag{5}$$

For N=$S_1 S_2 \ldots S_k$, let $\mathbf{r^{(j)}}$ be the vector of length $S_{j+1} \ldots S_k$ whose i^{th} component is given by

$$r_i^{(j)} = d(\mathbf{r^{(j-1)}}, iS_j, S_j)\,. \tag{6}$$

Note that $\mathbf{r^{(k)}} \equiv r^{(k)}$ is a 1-dimensional (scalar) quantity. Setting the initial vector $\mathbf{r^{(0)}}$ to be extracted vector $\tilde{\mathbf{r}}$, a 2^k-order differential detector determines that a watermark is present if $c > Th$, where Th is a threshold and $c = r^{(k)}$.

For values of n which are not powers of 2, n^{th}-order detectors can be derived similarly by reducing the length of the initial vector using a series of differential correlations. For example, a third-order scheme can be derived for a vector of length $N = TS = T(S-1) + T$ by performing T differential correlations of length $S-1$ on the first $T(S-1)$ terms, resulting in a vector of total length $2T$, which is reduced to a single detection output value by a further differential correlation of length $2T$.

4 Using Side Information to Maximise the Power of the Detector

It is necessary to choose a watermark embedding that can be successfully detected by the n^{th}-order detector. In determining the watermark, we seek a watermarking scheme which maximises the detection power. Consider an additive mixing function,

$$F(\mathbf{r}, g\mathbf{w}) = \mathbf{r} + g\mathbf{w}\,, \tag{7}$$

and let the detection function be written as $D(\mathbf{r})$. Given that the embedding strength is much smaller than the power of $\mathbf{r}$, to first order we can write,

$$D(\mathbf{r} + g\mathbf{w}) \simeq D(\mathbf{r}) + g\mathbf{w}.\nabla D(\mathbf{r})\,. \tag{8}$$

Hence, the watermark signal which maximises the power of the detector is,

$$\mathbf{w} = K\nabla D(\mathbf{r})\,, \tag{9}$$

where the constant K is chosen to normalise the power of $\mathbf{w}$ to one. Assuming that D is chosen such that the expected value $E\{D(\mathbf{r})\} = 0$, then, with the above choise of $\mathbf{w}$, under hypothesis H_1 that the watermark is present, the expected value of the output of the detector is $gK|\nabla D(\mathbf{r})|^2$ to the first order. In the following, we examine the efficiency of the side-informed detector, when D is the n^{th}-order detector described in Section 3.

5 A Maximum Power Detector

The efficiency of the scheme is defined as,

$$e = \frac{\mu_{D|H_1} - \mu_{D|H_0}}{\sigma_{D|H_1}}\,. \tag{10}$$

Given a particular detector $D(\mathbf{r})$, Eq. (8) shows how to choose the watermark $\mathbf{w}$ in order to maximise the power. We now address the question of which function $D(\mathbf{r})$ has maximum power, over all possible functions. Consider the class of n^{th}-order polynomials of the input vector.

In the following analyses, assume a constant embedding strength g and let $G = g^2/\sigma_r^2$ be the watermark to signal power ratio.

5.1 Second Order Polynomial Detectors

A second-order polynomial dectector, can be written as the quadratic form,

$$D(\mathbf{r}) = \sum_{i=1}^{N}\sum_{j=1}^{N} a_{ij} r_i r_j\,. \tag{11}$$

Assume that a_{ii}=0 $\forall i$ so that the mean of the detector is zero, without loss of generality, that $a_{ij} = a_{ji}$. Hence,

$$\frac{\partial D}{\partial r_i} = 2\mathbf{a}_i.\mathbf{r}\,, \tag{12}$$

where $\mathbf{a}_i$ is the vector $(a_{i1} \dots a_{iN})$. The expected value of the detector when the watermark is present is,

$$E\{d|H_1\} = 2g\sigma_r \sum_{i=1}^{N} ||\mathbf{a}_i|| \,. \tag{13}$$

The standard deviation of the detector under the null hypothesis is,

$$\sigma_{d|H_0} = \sqrt{2}\sigma_r^2 \sqrt{\sum_{i=1}^{N} ||\mathbf{a}_i||^2} \tag{14}$$

Using the fact that the maximum of $\sum_i^N x_i$ is $\sqrt{N}$ when $\mathbf{x}$ is a vector of unit length, the maximum efficiency that can be obtained from a second order polynomial correlator

$$e_{\max} = \sqrt{2NG} \,. \tag{15}$$

Note also, that the maximum efficiency of a first order detector is $\sqrt{NG}$.

5.2 N-th Order Polynomial Detectors

A general n^{th}-order polynomial detector can be written as

$$D_n(\mathbf{r}) = \sum a_{i_1,\dots,i_N} r_1^{i_1} r_2^{i_2} \dots r_N^{i_N} \tag{16}$$

where $n{=}\sum_{k=1}^{N} i_k$. In the case where $\max(i_1, \dots, i_N) = 1$, it can be shown that the maximum efficiency is $\sqrt{nNG}$ to first order. Using the subscript to denote the order of the detector, the n^{th} order detector can be written as

$$D_n(\mathbf{r}) = \sum_{i=1}^{N} r_i D_{n-1}(r_1 \dots r_N) \,. \tag{17}$$

Note that the expected value of the product of any pair of terms in this sum is zero, and we can write, as a first order approximation

$$V\{D_n|H_1\} = N\sigma_r^2 V\{D_{n-1}|H_1\} \,. \tag{18}$$

where $V\{X\}$ is the variance of X. When the watermark is present, the expected value of D_n can be written as

$$\begin{aligned} E\{D_n|H_1\} &= g\sum_{i=1}^{N} \sqrt{E\left\{\left(\tfrac{\partial D_n}{\partial r_i}\right)^2\right\}} \\ &= g\sum_{i=1}^{N} \sqrt{E\left\{D_{n-1}^2 + \sum_{j=1}^{N}\left(r_j \tfrac{\partial D_{n-1}}{\partial r_i}\right)^2\right\}} \\ &= gN\sqrt{V\{D_n|H_1\} + N\sigma_r^2 E\left\{\left(\tfrac{\partial D_{n-1}}{\partial r}\right)^2\right\}} \end{aligned} \tag{19}$$

Dividing by the standard deviation and simplifying, we get

$$e_{\max}^2(D_n) = NG\left[1 + \frac{e_{\max}^2(D_{n-1})}{GN}\right] , \tag{20}$$

and hence the result follows by induction.

Note that the differential detector of Section 3 has maximum efficiency $\sqrt{nNG}$.

5.3 Polynomial Detectors of Higher Degree

Consider an n^{th}-order detector of the following form:

$$D(\mathbf{r}) = \sum_{i=1}^{N/2} r_i^{n-1} r_j \tag{21}$$

where j is a randomly chosen index, which is matched with each index i. Assuming that $\mathbf{r}$ is drawn from a distribution which is symmetric about the origin, then $E\{D\}$ is zero for even values of n. Using the side-informed watermarking method, the efficiency of this detector is

$$e \approx \sqrt{\frac{GN}{2}} \left((n-1)\sqrt{\frac{M_{2n-4}}{M_{2n-2}}} + 1 \right) (1{-}G/2(1{+}(n{-}1)^2)) \tag{22}$$

where $M_i = E\{r^i\}$ is the i^{th} moment of the normalised distribution of r.

For some distributions, this leads to a higher efficiency than obtained for the first class of detectors. For example, if r is uniformly distributed, then $e \approx n\sqrt{GN/2}$. However, this approximation only holds while Gn^2 is small. We can expect the power of the detector to deteriorate for large values of n.

A similar scheme can be devised for odd values of n, for example

$$D(\mathbf{r}) = \sum_{i=1}^{N/3} r_i^{n-2} r_j r_k \,. \tag{23}$$

6 Security

All of the schemes presented above can be protected by permuting $\mathbf{r}$ before applying the embedder. The same permutation must be available at the detector in order to retrieve the watermark. In this sense the schemes are not asymmetric.

7 Experimental Results

The n^{th}-order watermarking schemes described above have been tested for vectors $\mathbf{r}$ drawn from a uniform random distribution. This is justified by the fact that we generally apply a filtering function, h, to the extracted vector prior detection. In watermarking applications, g is very small and can be estimated by the detector to first order. If h is designed such that $\sigma_{h(\mathbf{r})}^2 \simeq \sigma_g^2$, $h(\mathbf{r})$ is usually uniformly distributed and an additional gain of 14 dB can be achieved in the detection process [8]. This gain was not included in the simulation results presented in this paper. The experimental efficiency is calculated on a large set of trials, and the power of the test is plotted using

$$P_p = 1 - Q\left(\frac{\sigma_{d|H_0}}{\sigma_{d|H_1}} Q^{-1}(1 - P_{fa}) - e\right) \tag{24}$$

where Q is the cdf of the detector, which is approximated by assuming normality. Figures 1 and 2 show the ROC curves of n^{th}-order polynomial detectors when N=2400 and G=-26 dB. As expected from the analysis of Sections 5.2 and 5.3, detectors using polynomials of higher degree show much better detection performance than spread-sprectrum. A deterioration is however observed for larger values of n. Figures 3 and 4 give the power functions for both detectors as a function of G for $P_{fa}{=}10^{-4}$. At n=4, high-order polynomial detectors show a additional gain of about 1 dB compared to the same n^{th} order differential scheme, which is increased to 4 dB at n=7. This is in good agreement with the expected $\sqrt{n/2}$ efficiency ratio of the two classes of detectors.

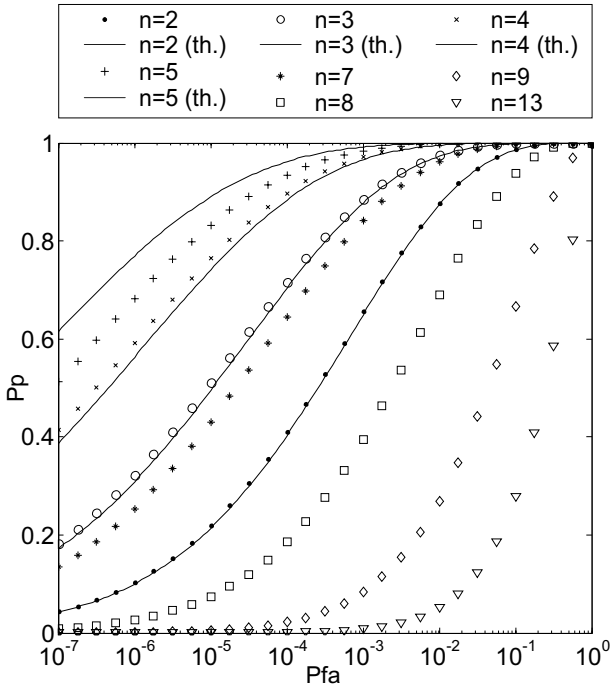

Figure 1: ROC curves of a first degree polynomial detector for G=-26 dB.

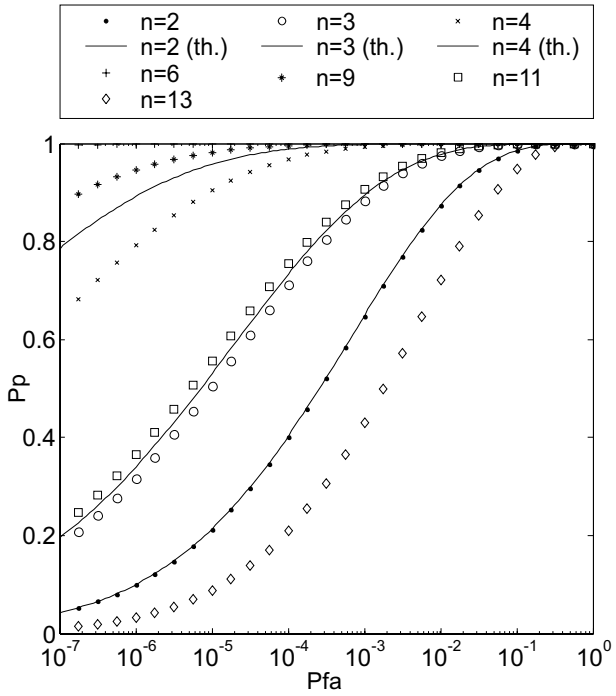

Figure 2: ROC curves of a higher degree polynomial detector for G=-26 dB.

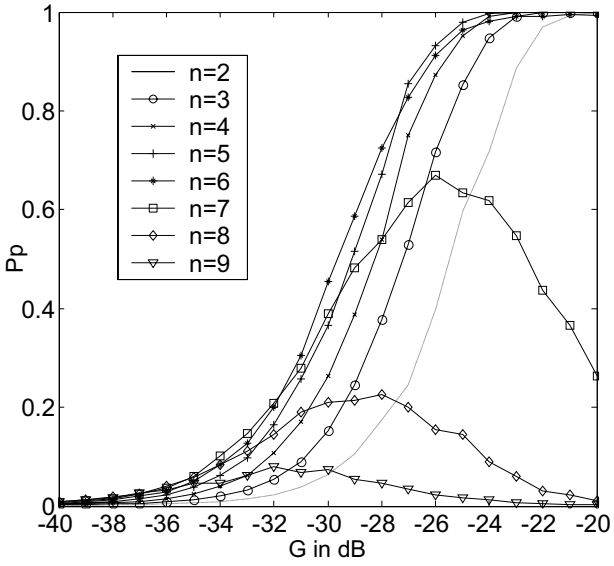

Figure 3: Power functions for a first degree polynomial detector with P_{fa}=10^{-4}.

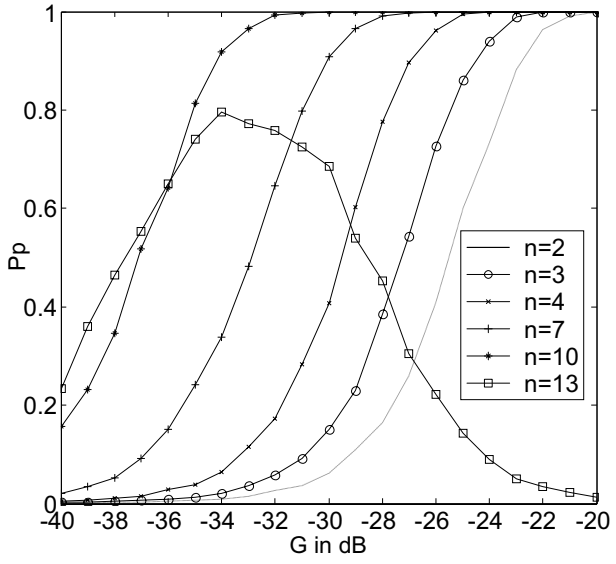

Figure 4: Power functions for a higher degree polynomial detector with P_{fa}=10^{-4}.

8 Conclusions

A new watermarking scheme has been presented which employs an n^{th}-order detection process. It has been shown that this scheme exhibits greater efficiency than has been achieved in the past. It also has some advantages in terms of security. The scheme depends on a private permutation key which is used in both the embedder and detector and hence is not truly asymmetric.

ACKNOWLEDGEMENTS

This project is supported by Enterprise Ireland Strategic Research Grant ST/2000/107/Y.

References

[1] J. Eggers, J. Su, and B.Girod, "Asymmetric watermarking schemes," in *Tagungsband des GI Workshops Sicherheit in Mediendaten*, *Springer Reihe: Informatik Aktuell*, (Berlin, Germany), Sept. 2000.

[2] *Coding of moving pictures and associated audio for digital storage media at up to about 1.5Mbit/s*, Tech. Rep., ISO/CEI 11172-3, 1993.

[3] I. Cox, J. Kilian, T. Leighton, and T. Shannon, "Secure spread sprectrum watermarking for multimedia," *IEEE Transactions on Image Processing* **6**(12), pp. 1673–1687, 1997.

[4] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," *Signal Processing* **66**(3), pp. 283–301, May 1998.

[5] J. Eggers, J. Su, and B.Girod, "A blind watermarking scheme based on structured codebooks," in *IEE Colloquium on Secure Images and Image Authentication*, pp. 41–46, (Savoy Place London), April 10 2000.

[6] T. Furon and P. Duhamel, "An asymmetric public detection watermarking technique," in *Workshop on information hiding*, (Dresden, Genmany), Oct. 2000.

[7] T. Furon, I. Venturini, and P. Duhamel, "Unified approach of asymmetric watermarking schemes," in *Security and Watermarking of Multimedia Contents III*, *Proc. SPIE* **4313**, 22-25 January 2001.

[8] G. C. M. Silvestre, N. Hurley, G. Hanau, and W. Dowling, "Informed audio watermarking scheme using digital chaotic signals," in *Proc. IEEE ICASSP*, 2001.

[9] G. Hanau, N. Hurley, G. Silvestre, and W. Dowling, "Informed perceptual audio watermarking," in *Proc. ISSC*, *Irish Signals and Systems Conference*, June 2001.

[10] J. Smith and C. Dodge, "Developments in steganography," in *Third International Workshop on Information Hiding*, A. Pfitzmann, ed., pp. 77–87, Springer Verlag, Sept. 1999.

[11] B. Chen and G. Wornell, "Dither modulation: a new approach to digital watermarking and information embedding," in *Security and Watermarking of Multimedia Contents*, *Proc. SPIE* **3657**, January 1999.