IEE Secure Images and
Image Authentication
London, UK
April 10, 2000

A Blind Watermarking Scheme Based on Structured Codebooks

Joachim J. Eggers, Jonathan K. Su
Telecommunications Laboratory
University of Erlangen-Nuremberg
Cauerstrasse 7/NT, 91058 Erlangen, Germany
{eggers,su}@LNT.de

Bernd Girod
Information Systems Laboratory
Stanford University
Stanford, CA 94305-9510, USA
girod@ee.stanford.edu

ABSTRACT

Blind digital watermarking is the communication of information via multimedia host data, where the unmodified host data is not available to the watermark detector. Many watermarking schemes suffer considerably from the remaining host-signal interference. For the additive white Gaussian case, Costa showed theoretically that interference from the host can be eliminated. However, the proof involves a huge, unstructured, random codebook, which is not feasible in practical systems. We present a suboptimal, practical scheme that employs a lattice-structured codebook to reduce complexity. The performance of the proposed scheme is compared to the information-theoretic limit and similar recent proposals.

1. INTRODUCTION

Digital watermarking is the communication of information by embedding it into multimedia data, called "host data," without introducing perceptual changes and receiving it later. The data with embedded watermark are denoted as "public data". The embedded information can be used for copyright protection or protection against deliberate or coincidental alteration of multimedia data.

For most applications, digital watermarking schemes must be designed such that the embedded information can be decoded reliably after common signal processing operations, and in some cases, even after deliberate attacks, e.g., in copy protection applications. In most applications, the unmodified host signal is not available to the watermark detector. Therefore, many watermarking schemes suffer considerably from the host-signal interference. Using results from Costa [5], Chen and Wornell [3] have shown that, for IID Gaussian signals and an additive white Gaussian noise (AWGN) attack, the theoretical capacity of a blind watermarking system is equal to that of a receiver with access to the host signal. The host-signal interference can be eliminated if the host signal is used as side information by the watermark encoder.

Costa gave a theoretical solution to the communication problem depicted in Fig. 1. The message $m \in \{1, 2, \ldots, M\}$ should be transmitted with a power constraint for the signal $\vec{w} = [w_1, w_2, \ldots, w_n, \ldots, w_N]$ of length N. The interfering Gaussian noise sources $\vec{x} \sim \mathcal{N}(0, \sigma_{\mathbf{x}}^2 I_N)$ and $\vec{v} \sim \mathcal{N}(0, \sigma_{\mathbf{v}}^2 I_N)$ are not known to the decoder. However, the encoder knows $\vec{x}$. This problem resembles the blind watermarking problem, where $\vec{x}$ is the host signal, and $\vec{v}$ is noise due to an AWGN attack. Using mean squared error (MSE) as distortion measurement, the constraint on the watermark embedding distortion $\sigma_{\mathbf{w}}^2$ corresponds to the power constraint. The decoder must be able to decode the transmitted watermark message m without having access to the host signal $\vec{x}$.

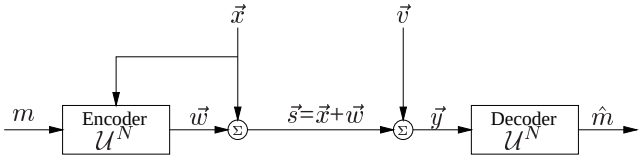

Figure 1. Watermark encoding followed by AWGN attack.

Costa's solution for the blind watermarking problem is not practical since a huge random codebook (CB) $\mathcal{U}^N$ is involved. In this paper, we discuss a watermarking scheme that is based on Costa's solution, however, the random CB is replaced by a lattice-structured CB to reduce complexity. Further, we restrict the discussion to schemes that are designed independently from a specific host signal distribution. These schemes can be easily implemented for many different host signals. We assume IID signals and consider only an AWGN attack. Thus, the communication scenario is completely described by the watermark-to-noise ratio WNR $= 10 \log_{10} \sigma_{\mathbf{w}}^2 / \sigma_{\mathbf{v}}^2$. Extensions to non-white signals and other attacks are not discussed here. In Section 2.1, Costa's approach is briefly reviewed using notation common for watermarking schemes. Then a watermark embedding process based on Costa's idea, but using a simplified CB, is derived. A performance analysis is given in Section 3 and some extensions and modifications are discussed in Section 4.

2. WATERMARKING EXPLOITING SIDE-INFORMATION AT THE ENCODER

2.1. Capacity-Achieving Blind Watermarking

The main ingredient of Costa's solution [5] to the transmission problem shown in Fig. 1 is the design of a specific CB $\mathcal{U}^N$ and appropriate encoding process. Here, we summarize the most important steps of Costa's approach. More details appear in [5, 6].

First of all, a random CB

$$\mathcal{U}^N = \{\vec{u}_l = \vec{w}_l + \alpha\vec{x}_l \mid l \in \{1,2,\ldots,L\}, \vec{\mathbf{w}} \sim \mathcal{N}(0,\sigma^2_{\mathbf{w}} I_N), \vec{\mathbf{x}} \sim \mathcal{N}(0,\sigma^2_{\mathbf{x}} I_N)\} \quad (1)$$

must be designed, where $\vec{\mathbf{w}}$ and $\vec{\mathbf{x}}$ are independent, $L = \lceil 2^{(N\cdot I(\mathbf{u};\mathbf{y})-\epsilon)} \rceil$ is the size of the CB, $I(\mathbf{u};\mathbf{y})$ is the mutual information between the CB entries and the received signals, and N is the codeword length. The CB is partitioned into M non-intersecting sub-CBs in such a way that each sub-CB $\mathcal{U}^N_m$ contains about the same number of sequences. Thus, the CB can be denoted by $\mathcal{U}^N = \mathcal{U}^N_1 \cup \mathcal{U}^N_2 \cup \cdots \cup \mathcal{U}^N_m \cup \cdots \cup \mathcal{U}^N_M$. This CB is available at the encoder and the decoder.

Assume a host signal $\vec{x}$ is given and a watermark message m should be transmitted. First, a jointly typical pair $(\vec{u}_0, \vec{x})$ in the sub-CB $\mathcal{U}^N_m$ must be found. This is equivalent to looking for a sequence $\vec{u}_0$ such that $\vec{w} = \vec{u}_0 - \alpha\vec{x}$ is nearly orthogonal to $\vec{x}$. The encoder declares an error if no such sequence is found. However, the probability of finding no suitable sequence $\vec{u}_0$ vanishes exponentially as $N \to \infty$. Second, the public signal is given by $\vec{s} = \vec{x} + \vec{w}$, or equivalently, the signal $\vec{w}$ is transmitted over the channel shown in Fig. 1. Third, the decoder searches the entire CB for a sequence $\vec{u}$ such that $(\vec{u}, \vec{y})$ is jointly typical. An error is declared if more than one or no such sequence is found. Again, with high probability the decoder will find only one such sequence, which will be equal to $\vec{u}_0$. The index $\hat{m}$ of the sub-CB $\mathcal{U}_{\hat{m}}$ containing $\vec{u}$ is the decoded watermark message. The probability of error averaged over the random choice of code goes to zero exponentially fast as $N \to \infty$.

Costa showed that for the CB (1) with

$$\alpha = \alpha^* = \frac{\sigma^2_{\mathbf{w}}}{\sigma^2_{\mathbf{w}} + \sigma^2_{\mathbf{v}}} = \frac{1}{1 + 10^{-\mathrm{WNR}/10}}, \quad (2)$$

the capacity is $C = \frac{1}{2}\log_2(1+\sigma^2_{\mathbf{w}}/\sigma^2_{\mathbf{v}})$, which is equal to the capacity of the transmission scenario where the host signal is known to the decoder. Thus, not knowing the host signal at the decoder does not decrease capacity. Note that the capacity is completely determined by the WNR, and independent from the host signal power $\sigma^2_{\mathbf{x}}$.

2.2. Watermarking using Lattice-Structured CBs

The CB size L of (1) can become very large, even for modest signal length N and size of the watermark alphabet. This can be easily seen for low channel noise power $\sigma^2_{\mathbf{v}}$, when α is close to 1. In this case, the CB (1) must provide a sufficiently accurate description of any possible host signal $\vec{x}$. Neither storing the CB (1) nor searching it is practical due to its random structure and huge size. Therefore, we propose using a suboptimal, lattice-structured CB while leaving the main concept of Costa's transmission scheme unchanged. Further, we develop a scheme that is independent from the host signal distribution, except for the assumption of a reasonably smooth PDF $p_{\mathbf{x}}(\mathbf{x})$ and $\sigma^2_{\mathbf{x}} \gg \sigma^2_{\mathbf{w}}, \sigma^2_{\mathbf{v}}$.

2.2.1. Embedding using Scalar Uniform Quantization

We assume that the watermark message m is encoded into a sequence $\vec{d} = [d_1, d_2, \ldots, d_n, \ldots, d_N]$ of N letters $d_n \in \mathcal{D} = \{0,1\}$, thus $m \equiv \vec{d}$.

First, the N-dimensional CB $\mathcal{U}^N$ is structured as product CB $\mathcal{U}^N = \mathcal{U}^1 \circ \mathcal{U}^1 \circ \cdots \circ \mathcal{U}^1$ of a one-dimensional component CB $\mathcal{U}^1$. All component CBs are identical.

Then, the component CB $\mathcal{U}^1$ must be separated into two distinct parts, $\mathcal{U}^1_0$ and $\mathcal{U}^1_1$, to allow for the transmission of $d_n \in \{0,1\}$ per signal sample n. Here, we set

$$\mathcal{U}^1_0 = \{u = k\alpha\Delta \mid k \in \mathbb{Z}\} \quad (3)$$

$$\mathcal{U}^1_1 = \left\{u = k\alpha\Delta + \frac{\alpha\Delta}{2} \,\middle|\, k \in \mathbb{Z}\right\}, \quad (4)$$

where $\alpha, \Delta \in \mathbb{R}^+$ are parameters yet to be derived. The entire composite CB $\mathcal{U}^1 = \mathcal{U}^1_0 \cup \mathcal{U}^1_1$ can be written as

$$\mathcal{U}^1 = \left\{u = k\alpha\Delta + d\frac{\alpha\Delta}{2} \,\middle|\, d \in \{0,1\}, k \in \mathbb{Z}\right\}. \quad (5)$$

Next, the random CB (1) in Costa's transmission scheme is replaced by the product CB $\mathcal{U}^N = \mathcal{U}^1 \circ \mathcal{U}^1 \circ \cdots \circ \mathcal{U}^1$, with $\mathcal{U}^1$ as defined in (5). For embedding the watermark bit sequence $\vec{d}$ we have to look for a jointly typical pair $(\vec{u}_0, \vec{x})$, or equivalently find a sequence $\vec{e} = \vec{w}/\alpha = (\vec{u}_0/\alpha) - \vec{x}$ which is nearly orthogonal to $\vec{x}$. For the given scheme, this process can be reduced to samplewise scalar uniform quantization

$$\frac{u_{n,0}}{\alpha} = \mathcal{Q}\left(x_n, \frac{\mathcal{U}^1_{d_n}}{\alpha}\right), \quad (6)$$

where $\mathcal{Q}(\cdot,\mathcal{U})$ denotes quantization to the CB $\mathcal{U}$, and $\mathcal{U}^1_{d_n}/\alpha$ means scaling all CB entries by $1/\alpha$. Here, the scaled CB corresponds to a uniform scalar quantizer with step size Δ. Finally, the transmitted watermark signal is given by

$$\vec{w} = \vec{u}_0 - \alpha\vec{x} = \alpha\vec{e}, \quad (7)$$

where $\vec{e} = \vec{u}_0/\alpha - \vec{x}$ is equal to the quantization error when quantizing the host signal $\vec{x}$ using the scaled product CB $\mathcal{U}^N_{\vec{d}}/\alpha$. Note that it is well-known that the quantization error $\vec{e}$ is almost orthogonal to the quantizer input $\vec{x}$ for an almost uniform host signal PDF in the range of one quantization bin and that the power of the quantization error is given by $\mathrm{E}\{\mathbf{e}^2\} = \Delta^2/12$.

In the described embedding scheme, two parameters, namely Δ and α, are involved. For a given watermark power $\sigma^2_{\mathbf{w}}$, these parameters are related by

$$\alpha = \sqrt{\frac{\sigma^2_{\mathbf{w}}}{\mathrm{E}\{\mathbf{e}^2\}}} = \sqrt{\frac{12\sigma^2_{\mathbf{w}}}{\Delta^2}}. \quad (8)$$

Costa determined α^*, given in (2), to be the optimal value for the random CB (1). The optimal value of α for the structured CB can be different. However, it appears that this optimal value is hard to find analytically, even for the simple AWGN channel. We will turn back to this problem in Section 3.2.

The presented watermark embedding scheme is depicted in Fig. 2. We denote it by SCS (scalar Costa scheme). Note that the embedding process works samplewise. The embedding of $d_n \in \{0,1\}$ can be expressed as subtractive dithered quantization, where $\Delta d_n/2$ is the dither signal and Δ is the step size of the uniform scalar quantizer.

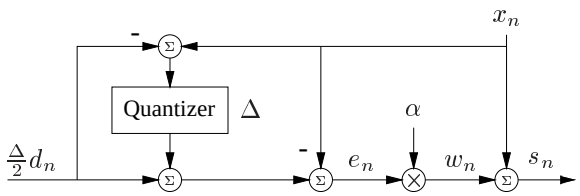

Figure 2. Watermark embedding for Costa's scheme with a scalar component CB.

2.2.2. Detection Based on Scalar Uniform Quantization

As in Costa's scheme, the watermark decoder has access to the same CB as the encoder. For SCS, the product CB $\mathcal{U}^N = \mathcal{U}^1 \circ \mathcal{U}^1 \circ \cdots \circ \mathcal{U}^1$, with $\mathcal{U}^1$ as in (5), is used. Treating this CB as a quantizer, the decoder acts as if it quantizes the received signal $\vec{y} = \vec{x} + \vec{w} + \vec{v}$, which can be done for each component CB $\mathcal{U}^1$ separately. From the index i of the selected quantizer bin, the decoded watermark letter is $\hat{d} = i \bmod |\mathcal{D}|$. From this view of the decoding process, a sound interpretation of the encoding process results: The encoder perturbs the host signal $\vec{x}$ by $\vec{w}$ to form the sent signal $\vec{s} = \vec{x} + \vec{w}$ so that, with high probability, $\vec{y}$ will fall into the correctly indexed quantization bin.

2.2.3. Comparison With Previously Proposed Schemes

Chen and Wornell [1, 2, 3] investigated a watermarking scheme called quantization index modulation (QIM). QIM is a special case of Costa's transmission scheme, where $\alpha = 1$ regardless of the noise variance $\sigma_{\mathbf{v}}^2$. As a result, QIM can achieve capacity as the WNR goes to infinity. However, for negative WNRs, which are very likely in watermarking applications, reliable transmission is difficult since the quantizer cells are too small. Chen and Wornell proposed a low-complexity QIM scheme based on dithered scalar uniform quantization, called dither modulation (DM), which is an analog to Costa's scheme using the scalar uniform CB. Since in Costa's scheme α is optimized for each WNR to achieve the best transmission performance, it is obvious that QIM can never perform better. Chen and Wornell used a spreading technique to improve the robustness of DM for low WNRs which leads to spread transform dither modulation (STDM). The same technique can be applied to Costa's scheme, which is discussed in Section 4.3. In [3], Chen and Wornell discuss the extension of QIM using Costa's ideas, and denote the derived scheme as QIM with distortion compensation.

Ramkumar [7] proposed a watermarking scheme based on the idea of continuous periodic functions for self noise suppression (CP-SNS). The periodicity is related to the cell size in Costa's scheme using lattice CBs. In general, both schemes cannot be translated directly into each other. However, their similar nature is recognizable for binary signaling. In this case, CP-SNS with thresholding* is almost equal to SCS, except that the weighted embedding of the quantization error $\vec{e}$ is replaced by thresholding each quantization error sample to a maximum absolute value of $\beta/2$. Thus,

$$w_n = \begin{cases} e_n & : \quad |e_n| \leq \beta/2 \\ \text{sign}(e_n)\beta/2 & : \quad \text{else} \end{cases} . \tag{9}$$

The embedding process for CP-SNS is depicted in Fig. 3. For $\beta \geq \Delta$, CP-SNS is equal to DM. However, the parameter β can be optimized for each WNR to improve robustness. Therefore, this scheme can also never perform worse than DM.

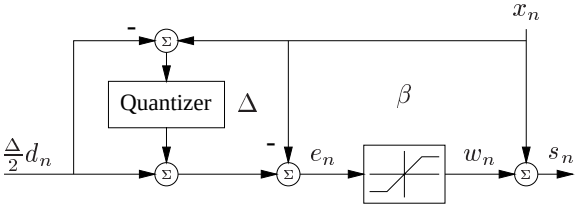

Figure 3. Watermark embedding using CP-SNS with binary signaling per sample.

For a constrained watermark embedding distortion $\sigma_{\mathbf{w}}^2$, the quantizer step size Δ and the threshold β are dependent on each other, as Δ and the weight α are for SCS. Assuming an almost-constant host signal PDF in the range of one quantization bin, Ramkumar [7] derived the relation

$$\sigma_{\mathbf{w}}^2 = \frac{\beta^2}{12\Delta}(3\Delta - 2\beta). \tag{10}$$

Note, that the weighting by α in SCS can be considered high dimensional thresholding of the watermark energy to the maximal value of $N\sigma_{\mathbf{w}}^2$.

3. PERFORMANCE ANALYSIS

We are interested in the performance loss of SCS compared with Costa's ideal scheme. Further, the performance should be compared to the suboptimal DM and CP-SNS. The comparison should be independent from specific realizations of channel coding, which in practice would be combined with all proposed methods. A fair comparison can be obtained by computing the mutual information $I(\mathbf{y}; \mathbf{d})$ between the received signal $\vec{y}$ and the sent watermark message $\vec{d}$, which is equivalent to the achievable rate of the specific scheme. First, we propose an efficient way to compute $I(\mathbf{y}; \mathbf{d})$ for the investigated schemes in case of an AWGN attack. Then, the proposed method is used to determine the optimal value of the CB parameter α for SCS, and the performance of the watermarking schemes is compared.

3.1. Mutual Information

For the investigation of SCS, DM and CP-SNS, it is sufficient to consider the transmission statistics for one signal sample since $\vec{x}$, $\vec{v}$ and $\vec{d}$ are modelled by IID random processes and the schemes operate samplewise†. We assume

*Throughout the paper, we consider only CP-SNS with thresholding due to its superior performance.

†Ramkumar did not propose a non-separable N-dimensional extension to his scheme. However, SCS and DM can be easily extended to higher dimensional schemes using appropriate lattice quantizers

that the watermark message is encoded such that for each signal sample an alphabet $\mathcal{D} = \{0, 1, \ldots, |\mathcal{D}| - 1\}$ of watermark letters is used, where each letter is equiprobable. Again, the host signal PDF can be approximated by a uniform distribution since $\sigma_{\mathbf{x}}^2 \gg \sigma_{\mathbf{w}}^2, \sigma_{\mathbf{v}}^2$. The size of the scalar CB is infinite, which is permissible due to the regular structure. Any boundary effects are neglected in our analysis.

For our assumptions, the mutual information is given by

$$\begin{aligned} I(\mathbf{y};\mathbf{d}) &= \mathcal{H}(\mathbf{y}) - \mathcal{H}(\mathbf{y}|\mathbf{d}) \\ &= -\int p_{\mathbf{y}}(y) \log_2 p_{\mathbf{y}}(y)\, \mathrm{d}y \\ &\quad + \frac{1}{|\mathcal{D}|} \sum_{d \in \mathcal{D}} \int p_{\mathbf{y}}(y|d) \log_2 p_{\mathbf{y}}(y|d)\, \mathrm{d}y. \end{aligned} \tag{11}$$

Thus, $I(\mathbf{y};\mathbf{d})$ is completely determined by the PDFs $p_{\mathbf{y}}(y)$ and $p_{\mathbf{y}}(y|d)$. These PDFs can be expressed in terms of the conditional PDF $p_{\mathbf{s}}(s|d)$ of the sent value s for a given watermark letter d and the PDF $p_{\mathbf{v}}(v)$ of the additive channel noise:

$$p_{\mathbf{y}}(y|d) = p_{\mathbf{s}}(y|d) * p_{\mathbf{v}}(y) \tag{12}$$

$$p_{\mathbf{y}}(y) = \frac{1}{|\mathcal{D}|} \sum_{d \in \mathcal{D}} p_{\mathbf{y}}(y|d), \tag{13}$$

where '$*$' denotes convolution.

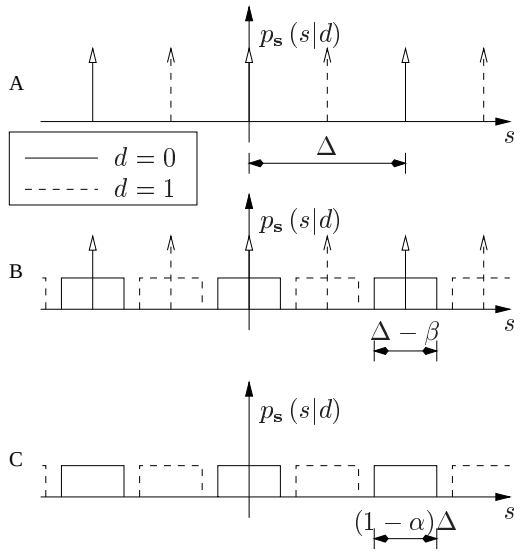

Figure 4. Qualitative diagram of the PDFs of the sent value s for a given watermark letter $d \in \mathcal{D} = \{0, 1\}$ in the case of (A) DM, (B) CP-SNS, and (C) SCS.

In most cases, a simple analytical expression for $p_{\mathbf{y}}(y|d)$ cannot be found. Thus, (11) must be computed numerically for a numerically derived $p_{\mathbf{y}}(y|d)$. The PDFs of the sent value s in case of binary signaling ($d \in \mathcal{D} = \{0, 1\}$) are depicted in Fig. 4 qualitatively for all three considered schemes. Note that for low WNR $p_{\mathbf{y}}(y|d=0)$ and $p_{\mathbf{y}}(y|d=1)$ may even overlap. Further, observe that even for DM and Gaussian $p_{\mathbf{v}}(v)$ the PDF of the received value will be not exactly Gaussian. We have to consider periodically overlapping Gaussian PDFs due to the multiple representation of the watermark letters. For the same reason, the expression for $p_{\mathbf{y}}(y|d)$ derived by Ramkumar [7] for CP-SNS is not exact. In [7], $p_{\mathbf{y}}(y|d)$ is expressed in terms of the error function, which is approximately correct only if Δ is significantly larger than the noise standard deviation $\sigma_{\mathbf{v}}$.

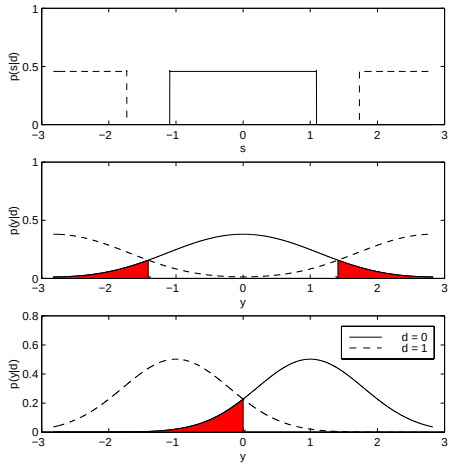

Figure 5. The upper two plots show one period of the PDFs of the sent and the received signal for SCS with binary signaling ($\sigma_{\mathbf{w}}^2$=1; WNR = 2dB; $\Delta = 5.65$; $\alpha = 0.613$). The lowest plot shows the PDF of the pre-processed received signal for binary watermark transmission with host signal at the receiver. The filled areas represent the probability of detection errors assuming $d = 0$ was sent.

We compute $p_{\mathbf{y}}(y|d)$ using characteristic functions and the discrete Fourier transform (DFT) which gives very accurate results for $\sigma_{\mathbf{x}}^2 \gg \sigma_{\mathbf{w}}^2, \sigma_{\mathbf{v}}^2$. Analytic expressions for the characteristic function of a Gaussian PDF, a Dirac and a rectangular PDF are easy to obtain, and the convolution in (12) can be translated into a multiplication in the domain of characteristic functions. Using the DFT for the inverse transformation from the characteristic function of the received signal into its PDF $p_{\mathbf{y}}(y|d)$, the periodic overlapping is computed implicitly for a proper DFT window width and sufficient DFT length. Fig. 5 depicts one period of the resulting $p_{\mathbf{y}}(y|d)$ for SCS and the PDF $p_{\mathbf{y}}(y|d)$ for a binary transmission scheme with host signal at the receiver. These plots clearly demonstrate the differences of both detection cases.

3.2. Optimal Quantizer Cell Size

Costa showed that (2) is the optimal value of the random CB parameter α for a given WNR. For the suboptimal SCS scheme, the optimal value of α has still to be determined. As shown in Section 2.2.1, α can be expressed in terms of the quantizer cell size Δ (8). Thus, optimizing α is equivalent to finding the optimal quantizer cell size Δ. We maximized the mutual information for a given WNR over all $\Delta \in \mathbb{R}^+$. Numerical optimization is necessary since no analytical expression for the mutual information is known. The resulting

optimal quantizer cell sizes can be approximated by

$$\Delta_{\mathrm{opt,SCS}} = \sqrt{12\left(\sigma_{\mathbf{w}}^2 + 2.71\sigma_{\mathbf{v}}^2\right)}, \tag{14}$$

which corresponds to

$$\alpha_{\mathrm{opt,SCS}} = \sqrt{\frac{\sigma_{\mathbf{w}}^2}{\sigma_{\mathbf{w}}^2 + 2.71\sigma_{\mathbf{v}}^2}}. \tag{15}$$

3.3. Comparison of Detection Performance

Fig. 6 shows the achievable rates obtained for SCS, DM and CP-SNS with binary signaling. DM performs poorly for negative WNRs. SCS and CP-SNS are much more robust since α and β are optimized to achieve better noise resistance. SCS performs slightly better than CP-SNS. Note that the depicted capacity curve is valid for a Gaussian host signal, whereas the achievable rate is derived for schemes that are designed independent from specific assumptions about the host signal (except for the assumption that $p_{\mathbf{x}}(\mathbf{x})$ is reasonable smooth and $\sigma_{\mathbf{x}}^2 \gg \sigma_{\mathbf{w}}^2, \sigma_{\mathbf{v}}^2$). Further, the optimal random CB is substituted by a suboptimal lattice CB. Therefore, we cannot expect to achieve capacity. However, the result indicates that the very simple SCS scheme performs quite well in comparison to the other schemes.

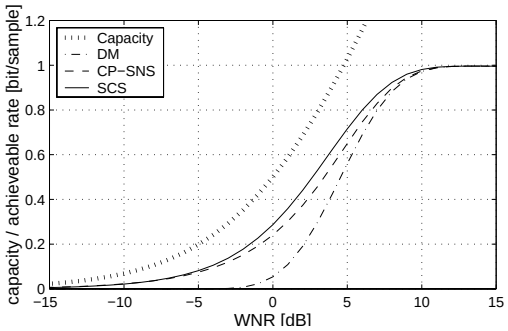

Figure 6. Capacity compared with the achievable rate of different suboptimal blind watermarking schemes.

Fig. 7 depicts the probability of bit error for uncoded transmission. An additive bipolar random watermark sequence is used in the reference scheme with host signal at the decoder. High error probabilities occur, particularly for negative WNRs, where transmitting one letter per sample means operating above capacity. In practice, low-rate error correction codes need to be implemented. Here, we are only interested in the relative performance of different schemes, so it is sufficient to consider the uncoded case. SCS and CP-SNS perform comparably, and are significantly better than DM. We also observe that the error probability predicted using the numerically derived PDF $p_{\mathbf{y}}(y|d)$ agrees with the simulation results. Thus, it is possible to use $p_{\mathbf{y}}(y|d)$ as a soft input to channel coding algorithms.

4. EXTENSIONS AND MODIFICATIONS

To roundoff the investigations, we examine some obvious extensions and minor modifications of SCS. This shows how well the simple SCS already performs.

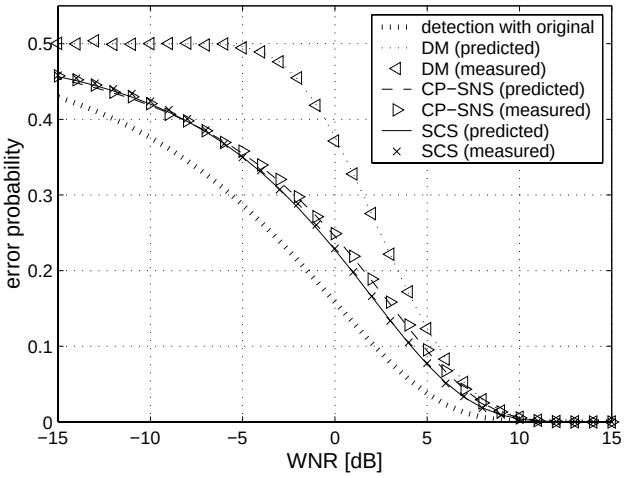

Figure 7. Error probability for uncoded binary transmission.

4.1. n-ary Signaling

In the previous sections, only binary transmission, that is $\mathcal{D} = \{0, 1\}$, was discussed. This is reasonable since in most cases watermarking schemes will operate at negative WNRs, where the capacity is lower than 0.5 bit/sample. However, in some cases positive WNRs might be of interest, e.g., when applying the spreading technique discussed in Section 4.3. SCS with n-ary signaling, meaning $\mathcal{D} = \{0, 1, \ldots, n-1\}$, can be implemented easily by distributing n different signaling points equidistantly over the range of one quantizer cell size Δ. The corresponding achievable rate is depicted in Fig. 8. We observe that the size of the alphabet $\mathcal{D}$ is important only for higher WNRs.

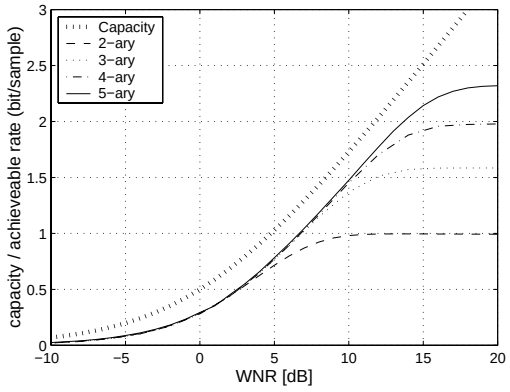

Figure 8. Achievable rate for SCS with n-ary signaling.

4.2. 2D Lattice Quantization With Hexagonal Cells

It is known from rate-distortion theory that higher dimensional quantizers give an improved quantization performance due to better sphere-packing abilities. Thus, there is hope to improve the simplified Costa scheme by using a product CB of hexagonal lattices instead of scalar uniform quantizers. We implemented this idea and denoted the approach by hexagonal Costa scheme (HCS). Fig. 9 shows

the achieveable rate for HCS, which was computed using a Monte Carlo approach. It appears that SCS and HCS perform almost identically, as long the finite alphabet size has no limiting effect. From our investigation it is not clear if the small differences are due to the precision of the Monte Carlo method. However, we can conclude at least that HCS does not give the expected gain. Note that this result is most probably due to the host signal independent design of the transmission scheme. Thus, these results do not contradict to the gains reported for higher dimensional signal constellations in [4].

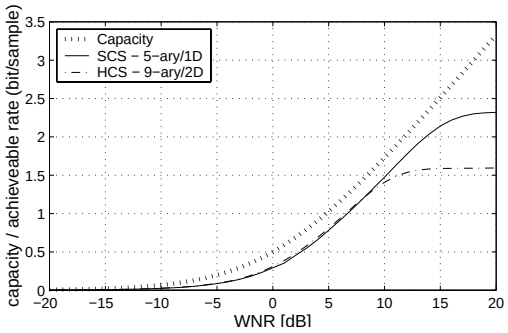

Figure 9. Achievable rate for 5-ary signaling per dimension using a scalar uniform CB and for 9-ary signaling per two dimensions using an hexagonal lattice CB.

4.3. Spreading of the Watermark Information

It is possible to combine DM, CP-SNS and SCS with a spreading technique as proposed already by Chen and Wornell for DM [1]. The corresponding mutual information can be computed by a mapping of the already derived mutual information curves via

$$I_\eta(\mathbf{y};\mathbf{d})|_{\mathrm{WNR}} = \frac{I_1(\mathbf{y};\mathbf{d})|_{\mathrm{WNR}_\eta}}{\eta}, \qquad (16)$$

where η is the spreading factor, $I_\eta(\mathbf{y};\mathbf{d})|_{\mathrm{WNR}}$ is the mutual information between $\mathbf{y}$ and $\mathbf{d}$ for given WNR and fixed η, and $\mathrm{WNR}_\eta = \mathrm{WNR}_1 + 10\log_{10}\eta$.

Maximizing $I_\eta(\mathbf{y};\mathbf{d})|_{\mathrm{WNR}}$ over all $\eta \in \mathbb{N}$ for each WNR gives the achieveable rates for STDM and STSCS (spread transform SCS) shown in Fig. 10. We observe that spreading can improve DM significantly in the range of negative WNRs, where for SCS only a minor gain can be achieved. However, STDM does not perform as well as STSCS, and for most WNRs even not as well as SCS. Thus, in practice it is recommendable to use SCS instead of improving DM using the spreading technique. Further, STSCS can have an increased gain over SCS at low WNRs, because good practical channel codes for such low WNRs are not known.

5. CONCLUSIONS AND FUTURE WORK

A practical blind watermarking scheme was derived from Costa's solution to the communication problem with side information at the encoder. A numerical method for analyzing the statistics of the received watermark information after an AWGN attack was developed, which enables us to compute the achievable rates and predict error probabilites for different noise powers of the attack. We found that the proposed suboptimal scheme performs better than previously proposed schemes and not much worse than the theoretical limit suggests. Closing the remaining gap to the theoretical limit is subject for future research. For this, the transmission scheme must be made dependent on the host signal distribution. Chou et al [4] have shown that duality between blind watermarking and distributed source coding exists, which can be exploited to design better structured codebooks.

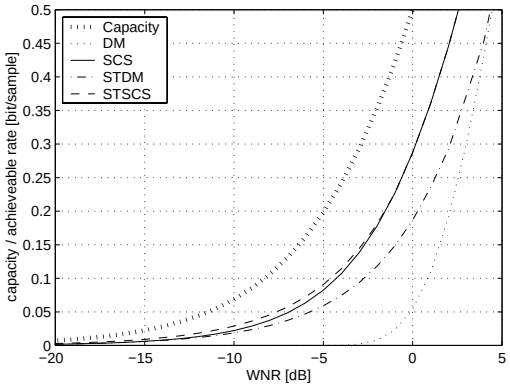

Figure 10. Achievable rate for DM and SCS with spreading.

REFERENCES

1. B. Chen and G. W. Wornell. Achievable performance of digital watermarking systems. In *Proceedings of the IEEE Intl. Conference on Multimedia Computing and Systems*, volume 1, Florence, Italy, June 1999.
2. B. Chen and G. W. Wornell. Dither modulation: a new approach to digital watermarking and information embedding. In *Proceedings of SPIE Vol. 3657: Security and Watermarking of Multimedia Contents*, San Jose, January 1999.
3. Brian Chen and Greg Wornell. Preprocessed and postprocessed quantization index modulation methods for digital watermarking. In *Proceedings of SPIE Vol. 3971: Security and Watermarking of Multimedia Contents II*, San Jose, Ca, USA, January 2000.
4. J. Chou, S. Pradhan, L. El Ghaoui, and Kannan Ramchandran. A robust optimization solution to the data hiding problem using distributed source coding principles. In *Proceedings of SPIE Vol. 3974: Image and Video Communications and Processing 2000*, San Jose, Ca, USA, January 2000.
5. M. H. M. Costa. Writing on Dirty Paper. *IEEE Transactions on Information Theory*, 29(3):439–441, May 1983.
6. T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons, New York, 1991.
7. M. Ramkumar. *Data Hiding in Multimedia: Theory and Applications*. PhD thesis, New Jersey Institute of Technology, Kearny, NJ, USA, November 1999.