MAC AWARE CODING STRATEGY FOR MULTIPLE USER INFORMATION EMBEDDING

Abdellatif Zaidi, Pablo Piantanida and Pierre Duhamel

{zaidi,piantanida,pierre.duhamel}@lss.supelec.fr
LSS/CNRS, Gif sur Yvette - FRANCE

ABSTRACT
Multiple user information embedding is concerned with embedding several messages into the same host signal. While emphasizing the tight relationship with conventional multiple user information theory, this paper presents several implementable “Dirty Paper Coding” (DPC) based schemes for multiple user information embedding. These are obtained by exploring strong connections with the well-known Gaussian Multiple Access Channel (MAC) with state information at the encoders. Two practical schemes are compared. The first -intuitive- one consists in a straightforward superimposition of DPC schemes. The second consists in a joint design of these Dirty Paper Coding schemes, based on the ideal DPC-based coding for the equivalent MAC channel. These results extend to the multiple user case the practical implementations (QIM and SCS) that have been originally conceived for one user. Then, we extend the results to a more general coding based on lattice (vector) codebooks, showing that the gap to full performances can be bridged up by using finite dimensional lattice codebooks, at the cost of an increased computational complexity. The improvements brought by a joint design are illustrated by both Bit Error Rates curves and Achievable rates regions.

1. INTRODUCTION
Consider the problem of communicating over a Gaussian channel corrupted by an additive Gaussian interfering signal that is non-causally known to the transmitter. This variation of the conventional additive white Gaussian noise (AWGN) channel is commonly known as channels with state information (SI) to the encoder. The state \( S \) is a random Gaussian variable with power \( Q \), independent of the gaussian noise \( Z \). The channel input is the index \( W \in \mathcal{M} \) with \( \mathcal{M} = \{1, \ldots, M\} \) and its output is \( Y^n = X^n + S^n + Z^n \), where \( M \) is the greatest integer smaller than or equal to \( 2^nR \) and \( R \) is the rate in bit per transmission. In his “Writing on Dirty Paper” [1], Costa showed that by choosing an adequate codebook, this channel capacity is the same as if the interfering signal \( S \) was not present. This is commonly known as the ideal Dirty Paper Coding (DPC). The term “Ideal” refers to an optimal random method for codebook generation and random binning coding.

However, in order to attain the full capacity, both the encoder and the decoder must share common knowledge of a huge codebook. This makes the ideal DPC unfeasible in practical situations. Therefore, several suboptimal, low-complexity practical schemes have been proposed, on a variety of application areas. Typical applications range from information embedding where the host signal is the state (non-causally) known at the encoder to more conventional communication over channels where a part of channel interference is (causally or non-causally) known to the transmitter. In all these practical schemes, randomized codebooks are replaced by quantization-based, or more generally, modulo-reduction-based algebraic codebooks. These single-user information embedding schemes are recalled in section 2. They have been extended, e.g. to non-Gaussian channel noise [2] and lattice codebooks [3–5].

In this paper, we rely on our recent work [6] to extend these schemes to multiple watermarking. This refers to the situation of embedding several messages into the same host signal, with or without different robustness and transparency requirements. The basic problem is to find the set of rates at which the different watermarks can be simultaneously embedded. Consider for example watermark applications such as copy control, transaction tracking, broadcast monitoring and tamper detection. Obviously, each application has its own robustness requirement and its own targeted data hiding rate. Embedding different watermarks intended to different usages into the same host signal naturally has strong links with transmitting different messages to different users in a conventional multi-user transmission context. More precisely, it is explained in [6] that multiple user information embedding parallels one of the two multi-user channels with state information available at the transmitter: the Gaussian Broadcast Channel (GBC) and the Gaussian Multiple Access Channel (GMAC). For the first case a practical SCS was addressed in [6]. In this paper we complete the study by addressing MAC-like multiple user information embedding scenarios (section 3).

2. WATERMARKING AS COMMUNICATION WITH SI
Digital watermarking can be considered as a communication problem, where a message \( W \in \{1, \ldots, M\} \) has to be sent to a receiver. It is encoded into a code \( X \) called the watermark which is then embedded into the host signal \( S \) (also called cover signal), thus forming the watermarked data \( S + X \). The watermarked data is sent to the receiver through a channel (the watermark channel), which is assumed to be Gaussian. The watermark is usually embedded without introducing perceptible distortions to the host signal (transparency requirement). The robustness requirement, refers to the ability of the watermark to survive channel degradations. The resulting transmission scheme is equivalent to communication over a power-limited channel with state information at the encoder. The host signal, is entirely available at the encoder. Thus, the corresponding channel capacity is that of an AWGN channel with the same SNR and is attained with an ideal Dirty Paper Coding (DPC) scheme. Instead of the ideal coding, in [7] and [8] two suboptimal practical version of DPC have been proposed. The basic principles are reviewed below.

Review of well-known single-user techniques: Following the
ideal DPC, Chen et al. proposed the use of structured quantization-based codebooks in [7], denoted as Quantization Index Modulation (QIM). In [8], Eggers et al. designed a practical "Scalar Costa DPC". Chen et al. proposed the use of structured quantization consisting in superimposing two single-user DPCs (or SCSs for the corresponding practical implementation). Let $Y = X_1 + X_2 + S + Z$ denote the received signal. Upon reception, the receiver should reliably decode the messages $W_1$ and $W_2$. However, since decoding is performed jointly, the successful decoding of one message should help decoding the other message. Suppose for example that encoder 2 uses a DPC (DPC1) taking into account the known state $S$ and the unknown noise $Z$ in order to form the watermark $X_2$ of power $P_2$ and carrying $W_2$ as $X_2 = U_2 - \alpha_2 S$, where

$$U_2 \sim \mathcal{N}(\alpha_2 S, P_2),$$

and $\alpha_2 = \frac{P_2}{P_2 + N}$. (2)

At reception the decoder first decodes $W_2$ and then cleans up the channel by subtracting the interference penalty $U_2$ that the transmission of $W_2$ causes to that of $W_1$. Thus, the channel for transmitting $W_1$ is actually equivalent to $Y_1 = Y - U_2 = X_1 + (1 - \alpha_2) S + Z$. This "cleaning up" step is inherently associated with successive decoding and is sometimes referred to as peeling-off technique. Consequently, encoder 1 can reliably transmit $W_1$ over channel $Y_1$ by using a second DPC (DPC2). The watermark $X_1$ is formed as $X_1 = U_1 - \alpha_1 S$, where

$$U_1 \sim \mathcal{N}(\alpha_1 S, P_1),$$

and $\alpha_1 = (1 - \alpha_2) \frac{P_1}{P_1 + N}$. (3)

Achievable rates: The theoretically achievable rates of this strategy correspond to the corner point (B1) of the diagram depicted in Fig.3 and are given by

$$R_1(B1) = \frac{1}{2} \log_2 \left( 1 + \frac{P_1}{N} \right),$$

(4a)

$$R_2(B1) = \frac{1}{2} \log_2 \left( \frac{P_2(P_2 + Q + N + P_1)}{P_2Q(1 - \alpha_2)^2 + (N + P_1)(P_2 + \alpha_2^2Q)} \right).$$

(4b)

The corner point (A) corresponds to the watermark $X_1$ being sent at its maximum achievable rate while $X_2$ is not transmitted. The two corner points (C1) and (D) correspond to points (B1) and (A), respectively, by swapping the roles of watermarks $X_1$ and $X_2$. Any rate pair lying on the lines connecting these corner points is attained by time-sharing.

**Two super-imposed SCSs:** We concentrate on the corner point (B1) and consider a practical implementation of this theoretical scheme. This can be performed by using two SCSs, SCS1 and SCS2, consisting in scalar versions of DPC1 and DPC2. Their corresponding uniform scalar quantizers $Q_{\Delta_1}$ and $Q_{\Delta_2}$ have step sizes $\Delta_1 = \frac{\sqrt{P_1}}{\alpha_1}$ and $\Delta_2 = \frac{\sqrt{P_2}}{\alpha_2}$, with $\alpha_1 = (1 - \alpha_2) \sqrt{\frac{P_1}{P_1 + 2.71N}}$ and $\alpha_2 = \frac{P_2}{P_2 + N}$. (2)

4. **MAC-LIKE MULTIPLE WATERMARKING**

This section proposes implementable coding schemes for the situation shown in figure 1. We provide performance analysis for two MAC-aware and unaware coding strategies.

### 4.1. Double DPCs

A simple approach for designing a watermark system for this situation consists in superimposing two single-user DPCs (or SCSs for the corresponding practical implementation). Let $Y = X_1 + X_2 + S + Z$ denote the received signal. Upon reception, the receiver should reliably decode the messages $W_1$ and $W_2$. However, since decoding is performed jointly, the successful decoding of one message should help decoding the other message. Suppose for example that encoder 2 uses a DPC (DPC1) taking into account the known state $S$ and the unknown noise $Z$ in order to form the watermark $X_2$ of power $P_2$ and carrying $W_2$ as $X_2 = U_2 - \alpha_2 S$, where

$$U_2 \sim \mathcal{N}(\alpha_2 S, P_2),$$

and $\alpha_2 = \frac{P_2}{P_2 + N}$. (2)

At reception the decoder first decodes $W_2$ and then cleans up the channel by subtracting the interference penalty $U_2$ that the transmission of $W_2$ causes to that of $W_1$. Thus, the channel for transmitting $W_1$ is actually equivalent to $Y_1 = Y - U_2 = X_1 + (1 - \alpha_2) S + Z$. This "cleaning up" step is inherently associated with successive decoding and is sometimes referred to as peeling-off technique. Consequently, encoder 1 can reliably transmit $W_1$ over channel $Y_1$ by using a second DPC (DPC2). The watermark $X_1$ is formed as $X_1 = U_1 - \alpha_1 S$, where

$$U_1 \sim \mathcal{N}(\alpha_1 S, P_1),$$

and $\alpha_1 = (1 - \alpha_2) \frac{P_1}{P_1 + N}$. (3)

Achievable rates: The theoretically achievable rates of this strategy correspond to the corner point (B1) of the diagram depicted in Fig.3 and are given by

$$R_1(B1) = \frac{1}{2} \log_2 \left( 1 + \frac{P_1}{N} \right),$$

(4a)

$$R_2(B1) = \frac{1}{2} \log_2 \left( \frac{P_2(P_2 + Q + N + P_1)}{P_2Q(1 - \alpha_2)^2 + (N + P_1)(P_2 + \alpha_2^2Q)} \right).$$

(4b)

The corner point (A) corresponds to the watermark $X_1$ being sent at its maximum achievable rate while $X_2$ is not transmitted. The two corner points (C1) and (D) correspond to points (B1) and (A), respectively, by swapping the roles of watermarks $X_1$ and $X_2$. Any rate pair lying on the lines connecting these corner points is attained by time-sharing.

**Two super-imposed SCSs:** We concentrate on the corner point (B1) and consider a practical implementation of this theoretical scheme. This can be performed by using two SCSs, SCS1 and SCS2, consisting in scalar versions of DPC1 and DPC2. Their corresponding uniform scalar quantizers $Q_{\Delta_1}$ and $Q_{\Delta_2}$ have step sizes $\Delta_1 = \frac{\sqrt{P_1}}{\alpha_1}$ and $\Delta_2 = \frac{\sqrt{P_2}}{\alpha_2}$, with $\alpha_1 = (1 - \alpha_2) \sqrt{\frac{P_1}{P_1 + 2.71N}}$ and $\alpha_2 = \frac{P_2}{P_2 + N}$. (2)

<table>
<thead>
<tr>
<th>Ideal DPC</th>
<th>Chen et al.</th>
<th>Proposed in [7]</th>
<th>Quantization Index Modulation (QIM)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[8] Eggers et al.</td>
<td>Designed a practical &quot;Scalar Costa DPC&quot;.</td>
<td>Chen et al. proposed the use of structured quantization-based codebooks</td>
</tr>
<tr>
<td></td>
<td>[8] Eggers et al.</td>
<td>Designed a practical &quot;Scalar Costa DPC&quot;.</td>
<td>Chen et al. proposed the use of structured quantization-based codebooks</td>
</tr>
</tbody>
</table>

**MAC-LIKE MULTIPLE WATERMARKING**

This section proposes implementable coding schemes for the situation shown in figure 1. We provide performance analysis for two MAC-aware and unaware coding strategies.

### 3. MULTIPLE WATERMARKING AND MULTIPLE ACCESS

Consider the 2-user watermarking situation, where the transmitters aims at embedding two messages $W_1$ and $W_2$ into the same cover signal $S$. Embedding is performed by two different authorities, each one embedding its own message. At the receiver, a single trusted authority checks for the two watermarks. We assume no particular cooperation between the two embedding authorities, meaning that the watermarks $X_1$ of power $P_1$ (carrying $W_1$) and $X_2$ of power $P_2$ (carrying $W_2$) should be designed independently of each other. The composite watermark signal $X = X_1 + X_2$ must however satisfy the input-power constraint $P$, meaning that $P_1 + P_2 \leq P$.

In practice, this multiple watermarking scenario can be used to serve multiple purposes. An example stemming from proof-of-ownership applications is as follows. Consider two different creators independently watermarking the same original content $S$, as it is common for large artistic works such as feature films and music recordings. Each of the two watermarks may contain private information. A common trusted authority may have to check for the two watermarks. This is the case when an authenticator agent needs to track down the initial owner of an illegally distributed image, for example. A second example is the so-called hybrid in-band on-channel digital audio broadcasting [7]. In this application, we would like to simultaneously transmit two digital signals within the same existing analog (AM and/or FM) commercial broadcast radio without interfering with conventional analog reception. Thus the analog signal is the cover signal and the two digital signals are the two watermarks. These digital signals may be designed independently. One signal may be used as an enhancement to refine the analog signal and the other as supplemental information such as station identification.

**MAC-like Set-up and Mathematical Model:** Assuming a Gaussian noise $Z \sim \mathcal{N}(0, N)$ corrupting the watermarked signal $S + X$, a simplified diagram is shown in Fig.1. The encoder $i, i = 1, 2$, encodes $W_i$ into $X_i$ at rate $R_i$. The decoder outputs the pair $(\tilde{W}_1, \tilde{W}_2)$, and declares an error if $(\tilde{W}_1, \tilde{W}_2) \neq (W_1, W_2)$. Functionally, this is the transmission over a two users Gaussian Multiple Access Channel (GMAC) with state information available to the transmitters. Therefore in section 4, we heavily rely on [9] to devise an efficient implementable multiple watermarking scheme. The resulting "joint design" is called "MAC-aware" and is evaluated in comparison with the corresponding "MAC-unaware" strategy, obtained by superimposing two DPC "Double DPC".

![Fig. 1. Two users multiple watermarking system.](image-url)
\[ \tilde{\omega}_2 = \frac{\sqrt{p_2}}{p_2 + p_1 N}. \] The feasible transmission rate pair achieved by this practical coding corresponds to the corner point (B') shown in Fig.3. The point (C') corresponds to the point (B') with the roles of the watermarks \( X_1 \) and \( X_2 \) being swapped.

**Discussion:** Performance of the first approach, including its theoretical and practical settings, are summarized as follows:

(i) From (4a), we see that DPC2- as given by (3)- is optimal, since the interference due to the cover signal \( S \) and the second watermark \( X_2 \) is completely cancelled. Hence, the watermark \( X_1 \) can be sent at its maximal rate \( R_1 \), if it were alone over the watermark channel. However, DPC1- as given by (2)- is non optimal, because the achievable rate \( R_2 \) given by (4b), is inferior to \( \frac{1}{2} \log_2 \left( 1 + \frac{p_2}{p_1 + N} \right) \), which is that of a watermark subject to the full interference penalty from both the cover signal \( S \) and watermark \( X_1 \).

(ii) SCS2 performs close to optimality. The scalar channel is equivalent to that from \( W_1 \) to \( r_1 = Q_{\Delta_1}(y) - y \). The practical transmission rate over this channel is given by \( I(r_1, W_1) \), the maximum of which (i.e \( R_1 \)) is obtained with the above choice of \( \tilde{\omega}_1 \). However, SCS1 is not optimal, simply because DPC1 is not. The encoding of \( W_2 \) can be improved so as to bring the practical rate \( \tilde{R}_2(\text{B}';) \) close to \( R_2^{(\text{max})} = \frac{1}{2} \log_2 \left( 1 + \frac{p_2}{p_1 + N} \right) \). The corresponding scheme, called "joint scalar DPC", enhances the performances by making multiple watermarking coding MAC-aware.

### 4.2. Connection to the Gaussian MAC with SI

In section 3, we have argued that the communication scenario depicted in Fig.1 is basically that of a Gaussian Multiple Access Channel with SI non-causally known to the transmitters. In [9], it is reported that the capacity region of this channel is given by: \( (R_1, R_2) : R_1 \leq \frac{1}{2} \log_2 \left( 1 + \frac{p_2}{p_1 + p_3} \right) \), \( R_2 \leq \frac{1}{2} \log_2 \left( 1 + \frac{p_2}{p_1 + p_3} \right) \), \( R_1 + R_2 \leq \frac{1}{2} \log_2 \left( 1 + \frac{p_2}{p_1 + p_3} \right) \), which is that of a Gaussian MAC with no interfering signal \( S \). This region, with corner points (A), (B), (C) and (D), is shown in Fig.3. Any point of it can be attained by an appropriate successive encoding scheme using the above well-designed DPCs. Consider for example, the corner point (B). The encoding of \( W_1 \) is again given by (3), recognized above as being optimal. The encoding DPC of \( W_2 \) however should be changed so as to consider the watermark \( X_1 \) as additional noise. The resulting DPC (again denoted by DPC1) uses the cover signal \( S \) as channel state and the signal \( Z + X_1 \) as total channel noise, i.e

\[ U_2 \sim N(\alpha_2 S, P_2), \quad \text{with} \quad \alpha_2 = \frac{P_2}{P_2 + (P_1 + N)}. \] (5)

Note that the interference due to \( X_1 \) is not completely removed, but this scheme is now optimal in that it achieves the maximal rate \( R_2^{(\text{max})} \) at which the message \( W_2 \) can be sent as long as \( W_1 \) is sent at its maximum rate.

#### 4.3. MAC-aware Coding and Joint Design

We consider now, as practical implementation of this joint scheme, two jointly designed SCs with parameters \( (\tilde{\omega}_1, \Delta_1) \) and \( (\tilde{\omega}_2, \Delta_2) \), respectively. This results in a maximal feasible transmission rate \( \tilde{R}_2 \) given, as before, by \( \tilde{R}_2 = \max_{\alpha_2} I(r, W_2) \). However, the corresponding scale parameter \( \alpha_2 \) is set this time to its optimal choice, i.e \( \tilde{\omega}_2 = \sqrt{\frac{P_2}{p_2 + p_1 N + P_1}} \). The resulting transmission rate pair \( (\tilde{R}_1, \tilde{R}_2) \) is represented by the corner point (B') in Fig.3.

**Practical Achievable Rates Region:** Reversing the roles of \( X_1 \) and \( X_2 \), the joint design also pushes out the corner point (C') to (C'). More generally, any rate pair on the region frontier delimited by the corner points (A), (B'), (C') and (D') is made practically feasible by time-sharing. Therefore, it is easy to show that the practically feasible achievable rates region is given by the closure of all rate pairs \( (R_1, R_2) \) satisfying

\[ \tilde{R}_1 \leq \max_{0 \leq \alpha_1 \leq 1} I(r_1, W_1), \quad \text{with} \quad r_1 = Q_{\Delta_1}(y) - y, \] (6a)

\[ \tilde{R}_2 \leq \max_{0 \leq \alpha_2 \leq 1} I(r_2, W_2), \quad \text{with} \quad r_2 = Q_{\Delta_2}(y) - y, \] (6b)

\[ \tilde{R}_1 + \tilde{R}_2 \leq \max_{0 \leq \alpha_1 \leq 1} I(r_1, W_1) + \max_{0 \leq \alpha_2 \leq 1} I(r_2, W_2). \] (6c)

with \( r_2 = Q_{\Delta_2}(y) - y \). Fig.3 shows the capacity region gain provided by the joint design of the DPCs with respect to the first method addressed above. This improvement is especially visible in the situations where \( W_1 \) and \( W_2 \) are both transmitted with non-zero rates, i.e. for a given transmission rate \( \tilde{R}_2 \) of \( W_2 \), the maximal transmission rate at which \( W_1 \) can be sent is larger, which is also valid for \( W_2 \). Note also that the gap to the theoretical limit can be reduced by use of sufficiently large size alphabets \( M_1 \) and \( M_2 \) as shown in Fig.4. Of course, this is achieved at the cost of a slight increase in encoding and decoding complexities.

**Bit Error Rate and discussion:** Consider the coding scheme given by (3) and (5). The peeling off technique aims at cleaning up the channel before decoding \( W_1 \), by subtracting the codeword \( U_2 \). Thus, the transmission of \( W_2 \) suffers from the additional noise \( X_1 \). The corresponding Signal-to-Noise Ratios (per-bit) SNR1 and SNR2 are given by \( \text{SNR}_1 = \frac{1}{2} \log_2 \left( 1 + \frac{p_2}{p_1 + p_3} \right) \) and \( \text{SNR}_2 = \frac{1}{2} \log_2 \left( 1 + \frac{p_2}{p_1 + p_3} \right) \). Thus, the BER curve corresponding to the transmission of \( W_2 \) can be obtained by translating to the right that of \( W_1 \), by \( \beta(R_1, R_2) = \frac{R_1}{R_2} \left( \frac{p_2}{p_1 + p_3} \right) \). The upper curve in Fig.2 depicts the error probability relative to the transmission of \( W_1 \) using binary alphabets. In practice the estimation \( U_2 \) does not provide the exact \( U_2 \). This can be seen as an additional noise source. However, at high SNR the estimation \( U_2 \) of codeword \( U_2 \) is accurate and the peeling off technique is efficient.

5. **STRUCTURED LATTICE-BASED CODEBOOKS**

The gap to the ideal capacity region of the practical achievable rates region (6) shown in Fig.3 and corresponding to the sample-wise joint scalar DPC can be partially bridged up using finite-dimensional lattice-based codebooks. Each index \( W_1 \in M_1 \) is assigned to a certain set of vectors \( c_{w_1} = \{ c_{w_1} : w_1 \in M_1 \} \), and so does each \( W_2 \in M_2 \). We focus on the improvement of the feasible rate pair \( (R_1(\Lambda), R_2(\Lambda)) \) brought by the use of lattice codebooks \( C_{w_i}, \) \( i = 1, 2 \), with comparison to the baseline scalar codebooks considered in section 4.

Relying on the optimal coding in [10], this achievable rates region using the modulo reduction with respect to the lattice \( \Lambda \) straightforwardly generalizes (6) and is given by the closure of all rates \( (R_1(\Lambda), R_2(\Lambda)) \) simultaneously satisfying

\[ R_1(\Lambda) \leq \max_{0 \leq \alpha_1 \leq 1} \frac{1}{n} \log_2 \left( \frac{\text{SNR}_1(V(\Lambda))}{1 - h(V_1)} \right), \] (7a)

\[ R_2(\Lambda) \leq \max_{0 \leq \alpha_2 \leq 1} \frac{1}{n} \log_2 \left( \frac{\text{SNR}_2(V(\Lambda))}{1 - h(V_2)} \right), \] (7b)

\[ R_1(\Lambda) + R_2(\Lambda) \leq \max_{0 \leq \alpha_2 \leq 1} \frac{1}{n} \log_2 \left( \frac{\text{SNR}_2(V(\Lambda))}{1 - h(V)} \right) + \max_{0 \leq \alpha_2 \leq 1} \frac{1}{n} \log_2 \left( \frac{\text{SNR}_1(V(\Lambda))}{1 - h(V)} \right). \] (7c)

where \( V = (\alpha_2 Z - (1 - \alpha_2) X_1) \mod \Lambda, \) \( i = 1, 2 \) and \( V = (\alpha_2 Z - (1 - \alpha_2) X_2) \mod \Lambda. \)

**Bit Error Rate Analysis and Discussion:** The improvement brought by lattice coding is illustrated in Fig.2 through the use of some finite dimensional lattices with good coding and quantizing properties. Lattice codebooks provide gains over scalar codebooks.
by improving the coding (coding gain \( \gamma_0(\Lambda) \)) and introducing the
shaping (shaping gain \( \gamma_1(\Lambda) = 1/12G(\Lambda) \)). \( G(\Lambda) \) is the second
moment of the lattice. A full focus on lattices can be found in [11].
In Fig. 2, we use the lattices (i) Cubic: \( G(Z^n) = 1/12, \gamma_0(Z^n) =
0\,[\text{dB}], (ii) Hexagonal \( (A_2) \), \( G(\Lambda) = \frac{\pi}{\sqrt{3}}, \gamma_0(\Lambda)[db] = 0.17,
\gamma_1(\Lambda)[\text{bit per dimension}] = 0.028, (ii) 4D Checkerboard lattice,
\( G(\Lambda) = 0.0766, \gamma_0(\Lambda)[db] = 0.37 \) and \( \gamma_1(\Lambda)[\text{bit per dimension}] =
0.061. \) Fig. 2 depicts the bit error probability relative to \( W_1 \). Note
that for a fair comparison of the error correction capability of these
lattices, we assumed the same energy \( E_0(\Lambda) \) to transmit one bit of
information per-dimension. Denoting by \( SNR_1 \) and \( SNR_2 \) the
resulting SNRs (per-bit per-dimension), the BER curve corresponding
to the transmission of message \( W_2 \) can be obtained by shifting to the
right that of \( W_1 \) by the factor \( \beta (R_1, R_2) \).

6. CONCLUSION

This paper investigates the tight relationship between multiple user
information embedding situations and conventional communication
over a Multiple Access Channel (MAC) with SI non-causally known
at the transmitters. Several examples of multiple watermarking rele-
vant of the MAC situation were outlined. Based on this equivalence,
a practically feasible scalar scheme for simultaneously embedding
two messages into the same host signal is proposed (referenced to
as MAC-aware). This scheme extends the initial QIM and SCS
schemes to the two-watermarks case. The careful design concerns
the joint encoding as well as the appropriate order needed so as to
reliably decode the different watermarks. The improvement brought
by this joint design is shown through comparison with the corre-
sponding intuitive scheme, obtained through superimposition of the
single user schemes QIM and SCS (referenced to as MAC-unaware).
Performance is analyzed in terms of both achievable rates region and
Bit Error Rates. Finally, the proposed schemes are straightforwardly
extended to the vector case through lattice-based codebooks.

7. REFERENCES


“Additive non-gaussian noise attacks on the scalar costa
scheme (scs),” in Proc. of SPIE & IST, San Joze, CA, USA,


Fig. 2. Bit Error Probability v.s. (per-dimension per-bit) SNR
\( SNR_1 = E_0(\Lambda)/N \) for QIM-embedding message \( W_1 \). From bottom
to top: lattices Checkerboard \( D_4 \), Hexagonal \( A_2 \) and Cubic \( Z \).

Fig. 3. Comparison joint scalar DPC with two Double DPCs for
binary alphabets. Solid line delineates the capacity region of both
ideal (upper) and practical coding (lower). Dashed line delineates
the achievable rates with the Double DPC for both ideal (upper) and
practical coding.

Fig. 4. Achievable rates with the joint scalar DPCs for \( M_1 \)-ary
and \( M_2 \)-ary alphabets.

watermarking,” in proc. of European Signal Processing Conf.
EUSIPCO, Antalya, Turkey, september 2005.

nel for QIM watermarking,” in proc of Int. Conf. Image Proces-
sing ICIP, Genova, Italy, september 2005.

multiple user information embedding,” in Proc. of Interna-
tional Conference on Acoustics, Speech, and Signal Processing

class of provably good methods for digital watermarking and
information embedding,” IEEE Transactions on Information

[8] Joachim J. Eggers, Robert Bäuml, Roman Tzschoppe, and
Bernd Girod, “Scalar costa scheme for information embed-
ing,” IEEE Transactions on Signal Processing, pp. 1–39,
2002.

[9] Young-Han Kim, Arak Sutivong, and Styrmir Sigurjonsson,
“Multiple user writing on dirty paper,” in Proc. ISIT 2004,
Chicago-USA, June 2004, p. 534.

for structured multiterminal binning,” IEEE Transactions on