MAC AWARE CODING STRATEGY FOR MULTIPLE USER INFORMATION EMBEDDING

Abdellatif Zaidi and Pablo Piantanida

Abdellatif.Zaidi@ensta.org,Piantanida@lss.supelec.fr
Signals and Systems Lab. 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 -rather intuitive- 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 Bit Error Rates curves and achievable rates region.

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 X^n is the output of the encoder, 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 capacity channel is the same as if the interfering signal S were not present. This is commonly known as Dirty Paper Coding (DPC). DPC involves 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, in 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 at 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 into different directions, 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 information embedding. 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. Thus, 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 former a practical SCS was addressed in [6]. In this paper, we complete the study by addressing MAC-like multiple user information embedding scenarios. We show that joint design is required so as to closely approach the theoretical performance limits. The improvement brought by this joint design is pointed out by comparison to the straightforward scheme obtained by super-imposing (i.e with no joint design) these SCSs. This improvement is shown through both achievable rates region and Bit Error Rates (BER) analysis. Finally, we show that these performances can be made closer to the theoretical limits by considering lattice-based codebooks. Some finite-dimensional lattices with good packing and quantization properties are considered.

2. WATERMARKING AS COMMUNICATION WITH SI

Digital watermarking can be considered as a communication problem, where a message $W \in \{1, \ldots, \mathcal{M}\}$ 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 a DPC scheme. Instead of the ideal coding, two sub-optimal practical versions of DPC have been proposed in [7] and [8]. The basic principles are reviewed below.

The authors would like to sincerely thank Prof. Pierre Duhamel for great help during this work and the project SDMO for funding.

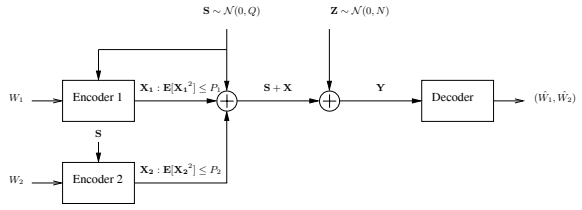

Fig. 1. Two users multiple watermarking system.

Review of well-known single-user techniques: Following the ideal DPC, Chen et al. proposed the use of a structured quantization-based codebook in [7], referred to as Quantization Index Modulation (QIM). In [8], Eggers et al. designed a practical "Scalar Costa Scheme" (SCS) where the random codebook $\mathbf{U}$ is chosen to be a concatenation of dithered uniform scalar quantizers. The watermark signal is a scaled version of the quantization error, i.e,

$$x_k = \widetilde{\alpha}\{\mathcal{Q}_\Delta\left(s_k - \frac{W}{M}\Delta\right) - (s_k - \frac{W}{M}\Delta)\}, \qquad (1)$$

with $\Delta = \frac{\sqrt{12P}}{\widetilde{\alpha}}$, $\widetilde{\alpha} = \sqrt{\frac{P}{P+2.71N}}$ and $\mathcal{Q}_\Delta$ is the uniform scalar quantizer with constant step size Δ. Decoding is also based on the scalar quantizer value of the received signal $\mathbf{y} = \mathbf{x} + \mathbf{s} + \mathbf{z}$ followed by a thresholding procedure. That is, the estimate $\widehat{W}$ of the transmitted message W is the closest integer to $\frac{r_k}{\Delta/M}$, with $r_k = \mathcal{Q}_\Delta(y_k) - y_k$. The optimum parameter $\widetilde{\alpha}$ is obtained by numerically maximizing Shannon's mutual information $I(r; W)$. With this set-up, SCS performs close to DPC. This constitutes the main motivation behind focusing on adapting it to the multi-user case.

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 $\mathbf{S}$. Embedding is performed by two different authorities, each 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 $\mathbf{X}_1$ of power P_1 (carrying W_1) and $\mathbf{X}_2$ of power P_2 (carrying W_2) should be designed independently of each other. The composite watermark signal $\mathbf{X} = \mathbf{X}_1 + \mathbf{X}_2$ 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 $\mathbf{S}$, 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 $\mathbf{Z} \sim \mathcal{N}(0, N)$ corrupting the watermarked signal $\mathbf{S} + \mathbf{X}$, a simplified diagram is shown in Fig.1. The encoder i, $i = 1, 2$, encodes W_i into $\mathbf{X}_i$ at rate R_i. The decoder outputs the pair $(\widehat{W}_1, \widehat{W}_2)$, and declares an error if $(\widehat{W}_1, \widehat{W}_2) \neq (W_1, W_2)$. 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, also sometimes referred to as "Double DPC".

4. MAC-LIKE MULTIPLE WATERMARKING

This section proposes implementable coding schemes for the model shown in Fig.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 $\mathbf{Y} = \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{S} + \mathbf{Z}$ denote the received signal. Upon reception, the receiver should reliably decode 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 $\mathbf{S}$ and the unknown noise $\mathbf{Z}$ in order to form the watermark $\mathbf{X}_2$ (of power P_2 and carrying W_2) as $\mathbf{X}_2 = \mathbf{U}_2 - \alpha_2\mathbf{S}$, where

$$\mathbf{U}_2 \sim \mathcal{N}\left(\alpha_2\mathbf{S}, P_2\right), \text{ and } \alpha_2 = \frac{P_2}{P_2 + N}. \qquad (2)$$

At reception the decoder first decodes W_2 and then cleans up the channel by subtracting-off the interference penalty $\mathbf{U}_2$ that the transmission of W_2 causes to that of W_1. Thus, the channel for transmitting W_1 is actually equivalent to $\mathbf{Y}_1 = \mathbf{Y} - \mathbf{U}_2 = \mathbf{X}_1 + (1 - \alpha_2)\mathbf{S} + \mathbf{Z}$ and then it decodes W_1. 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 $\mathbf{Y}_1$ by using a second DPC (DPC2). In order to do so, the watermark $\mathbf{X}_1$ is formed as $\mathbf{X}_1 = \mathbf{U}_1 - \alpha_1\mathbf{S}$, where

$$\mathbf{U}_1 \sim \mathcal{N}\left(\alpha_1\mathbf{S}, P_1\right), \text{ and } \alpha_1 = (1 - \alpha_2)\frac{P_1}{P_1 + N}. \qquad (3)$$

Achievable rates: The theoretically achievable rates of this strategy correspond to the corner point (B1) of the diagram shown in Fig.2 and are given by

$$R_1(B1) = \frac{1}{2}\log_2\left(1 + \frac{P_1}{N}\right), \qquad (4a)$$

$$R_2(B1) = \frac{1}{2}\log_2\left(\frac{P_2(P_2 + Q + N + P_1)}{P_2Q(1 - \alpha_2)^2 + (N + P_1)(P_2 + \alpha^2Q)}\right). \qquad (4b)$$

Corner point (A) corresponds to $\mathbf{X}_1$ being sent at its maximum achievable rate while the watermark $\mathbf{X}_2$ is not transmitted at all. The two corner points (C1) and (D) correspond to points (B1) and (A), respectively, by swapping the roles of the watermarks $\mathbf{X}_1$ and $\mathbf{X}_2$. Any rate pair lying on the lines connecting these corner points is attained by time-sharing.

Two super-imposed SCSs: We concentrate on 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 $\mathcal{Q}_{\Delta_1}$ and $\mathcal{Q}_{\Delta_2}$ have step sizes $\Delta_1 =$

$\frac{\sqrt{12P_1}}{\widetilde{\alpha_1}}$ and $\Delta_2 = \frac{\sqrt{12P_2}}{\widetilde{\alpha_2}}$, with $\widetilde{\alpha_1} = (1-\alpha_2)\sqrt{\frac{P_1}{P_1+2.71N}}$ and $\widetilde{\alpha_2} = \sqrt{\frac{P_2}{P_2+2.71N}}$. The feasible transmission rate pair achieved by this practical coding corresponds to the corner point (B1') shown in Fig.2. The point (C1') corresponds to the point (B1') with the roles of the watermarks $\mathbf{X}_1$ and $\mathbf{X}_2$ being reversed.

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 $\mathbf{S}$ and the second watermark $\mathbf{X}_2$ is completely canceled. Hence, the watermark $\mathbf{X}_1$ can be sent at its maximal rate R_1, as 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 $\mathbf{S}$ and watermark $\mathbf{X}_1$.

(ii) SCS2 performs close to optimality. The scalar channel is equivalent to that from W_1 to $\mathbf{r}_1 = \mathcal{Q}_{\Delta_1}(\mathbf{y}_1) - \mathbf{y}_1$. The practical transmission rate over this channel is given by $I(r_1, W_1)$, the maximum of which (i.e $\widetilde{R_1}$) is obtained with the above choice of $\widetilde{\alpha_1}$. However, SCS1 is non optimal, simply because DPC1 is not. The encoding of W_2 can be improved so as to bring the practical rate $\widetilde{R_2}(B1')$ close to $R_2^{(max)} = \frac{1}{2}\log_2\left(1+\frac{P_2}{P_1+N}\right)$. 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: $\Big\{(R_1,R_2): R_1 \le \frac{1}{2}\log_2\left(1+\frac{P_1}{N}\right),\ R_2 \le \frac{1}{2}\log_2\left(1+\frac{P_2}{N}\right)\ R_1+R_2 \le \frac{1}{2}\log_2\left(1+\frac{P_1+P_2}{N}\right)\Big\}$, which is that of a Gaussian MAC with no interfering signal $\mathbf{S}$. This region, with corner points (A), (B), (C) and (D), is shown in Fig.2. 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 to be optimal. The encoding DPC1 of W_2 however should be changed so as to consider the watermark $\mathbf{X}_1$ as additional noise. The resulting DPC (again denoted by DPC1) uses the cover signal $\mathbf{S}$ as channel state and the signal $\mathbf{Z}+\mathbf{X}_1$ as total channel noise, i.e

$$\mathbf{U}_2 \sim \mathcal{N}\left(\alpha_2\mathbf{S}, P_2\right), \text{ with } \alpha_2 = \frac{P_2}{P_2+(P_1+N)}. \quad (5)$$

Note that the interference due to $\mathbf{X}1$ is not completely removed, but this scheme is now optimal, in that it achieves the maximum rate $R_2^{(max)}$ 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 SCSs with parameters $(\widetilde{\alpha_1}, \Delta_1)$ and $(\widetilde{\alpha_2}, \Delta_2)$, respectively. This results in a maximal feasible transmission rate $\widetilde{R_2}$ given, as before, by $\widetilde{R_2} = \max_{\alpha_2} I(r, W_2)$. However, the corresponding scale parameter α_2 is set this time to its optimal choice, i.e, $\widetilde{\alpha_2} = \sqrt{\frac{P_2}{P_2+2.71(N+P_1)}}$. The resulting transmission rate pair $(\widetilde{R_1}, \widetilde{R_2})$ is represented by the corner point (B') in Fig.2.

Practical Achievable Rates Region: Reversing the roles of $\mathbf{X}_1$ and $\mathbf{X}_2$, the joint design also pushes out the corner point (C1') 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 can be easily shown that the practically feasible achievable rates region is given by the closure of all rate pairs $(\widetilde{R_1}, \widetilde{R_2})$ satisfying

$$\widetilde{R_1} \le \max_{0\le\alpha_1\le 1} I(\mathbf{r}_1, W_1), \text{ with } \mathbf{r}_1 = \mathcal{Q}_{\Delta_1}(\mathbf{y}_1) - \mathbf{y}_1, \quad (6a)$$

$$\widetilde{R_2} \le \max_{0\le\alpha_2\le 1} I(\mathbf{r}_2, W_2), \text{ with } \mathbf{r}_2 = \mathcal{Q}_{\Delta_2}(\mathbf{y}_2) - \mathbf{y}_2, \quad (6b)$$

$$\widetilde{R_1}+\widetilde{R_2} \le \max_{0\le\alpha_1\le 1} I(\mathbf{r}_1, W_1) + \max_{0\le\alpha_2\le 1} I(\bar{\mathbf{r}}_2, W_2). \quad (6c)$$

with $\bar{\mathbf{r}}_2 = \mathcal{Q}_{\Delta_2}(\mathbf{y}) - \mathbf{y}$. Fig.2 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 $\widetilde{R_2}$ of W_2 the maximal transmission rate at which W_1 can be sent is larger and it is equivalently for W_2. Note also that the gap to the theoretical limit can be reduced by use of sufficiently large size alphabets $\mathcal{M}_1$ and $\mathcal{M}_2$ as shown in Fig.3. 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 to clean up the channel before decoding W_1, by subtracting-off the codeword $\mathbf{U}_2$. Thus, the transmission of W_2 suffers from the additional noise $\mathbf{x}_1$. The corresponding Signal-to-Noise Ratios (per-bit) SNR1 and SNR2 are given by SNR1 $= \frac{P_1}{R_1+N}$ [dB] and SNR2 $= \frac{P_2}{R_2(N+P_1)}$ [dB]. Thus, the BER curve corresponding to the transmission of W_2 can be obtained by translating to the right that of W_1, by $\beta(R_1,R_2) = \frac{R_1P_2N}{R_2P_1(N+P_1)}$[dB]. The upper curve in Fig.4 depicts the error probability relative to the transmission of W_1 using binary alphabets. Note however that, in practice, $\mathbf{U}_2$ is provided by an estimation procedure. The estimation error represents an additional noise source at the decoder. At high SNR2, the estimation $\widehat{\mathbf{U}}_2$ of codeword $\mathbf{U}_2$ 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.2 and corresponding to the sample-wise joint scalar DPC can be partially bridged up using finite-dimensional lattice-based codebooks. Each index in $W_1 \in \mathcal{M}_1$ is assigned to a vector in a certain set of vectors $\mathcal{C}_{w_1} = \{\mathbf{c}_{w_1} : w_1 \in \mathcal{M}_1\}$, and similarly for the set of indexes $W_2 \in \mathcal{M}_2$. We focus on the improvement of the feasible rate pair $(R_1(\Lambda), R_2(\Lambda))$ brought by the use of lattice codebooks $\mathcal{C}_{w_i}$, $i=1,2$, with comparison to the baseline scalar codebooks considered in section 4.

Paralleling the development made in [10], this achievable rates region using the modulo reduction with respect to the lattice Λ straightforwardly generalizes (6) and is given by the closure of all rates $(R_1(\Lambda), R_2(\Lambda))$ simultaneously satisfying

$$R_1(\Lambda) \le \max_{0\le\alpha_1\le 1} \frac{1}{n}\left(\log_2(V(\Lambda)) - h(\widetilde{\mathbf{V}_1})\right), \quad (7a)$$

$$R_2(\Lambda) \le \max_{0\le\alpha_2\le 1} \frac{1}{n}\left(\log_2(V(\Lambda)) - h(\widetilde{\mathbf{V}_2})\right), \quad (7b)$$

$$R_1(\Lambda)+R_2(\Lambda) \le \max_{0\le\alpha_1\le 1} \frac{1}{n}\left(\log_2(V(\Lambda)) - h(\widetilde{\mathbf{V}_1})\right) + \max_{0\le\alpha_2\le 1} \frac{1}{n}\left(\log_2(V(\Lambda)) - h(\widetilde{\mathbf{V}})\right). \quad (7c)$$

where $\widetilde{\mathbf{V}_i} = (\alpha_i\mathbf{Z} - (1-\alpha_i)\mathbf{X}_i) \mod \Lambda$, $i=1,2$ and $\widetilde{\mathbf{V}} = (\alpha_2(\mathbf{Z}+\mathbf{X}_1) - (1-\alpha_2)\mathbf{X}_2) \mod \Lambda$.

Bit Error Rate Analysis and Discussion: The improvement brought by lattice coding is illustrated in Fig.4 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 $\gamma_c(\Lambda)$) and introducing the shaping (shaping gain $\gamma_s(\Lambda) = 1/12G(\Lambda)$). $G(\Lambda)$ is the second moment of the lattice. A full focus on lattices can be found in [11]. In Fig.4, we use the lattices (i) Cubic: $G(\mathbb{Z}^n) = 1/12$, $\gamma_s(\mathbb{Z}^n) = 0$[dB], (ii) Hexagonal ($A_2$), $G(\Lambda) = \frac{5}{36\sqrt{(3)}}$, $\gamma_s(\Lambda)[db] = 0.17$, $\gamma_s(\Lambda)$[bit per dimension] $= 0.028$, (ii) 4D Checkerboard lattice, $G(\Lambda) = 0.0766$, $\gamma_s(\Lambda)[db] = 0.37$ and $\gamma_s(\Lambda)$[bit per dimension] $= 0.061$. Fig.4 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 $E_b(\Lambda)$ to transmit one bit of information per-dimension. Denoting by SNR1 and SNR2 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. Some MAC-like information embedding situations are outlined. Based on this equivalence, a practically feasible scalar scheme for simultaneously embedding two messages into the same host signal is proposed (referred to as MAC-aware). This scheme carefully 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 corresponding intuitive scheme, obtained through superimposition of the single user schemes QIM and SCS (referred 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 vec

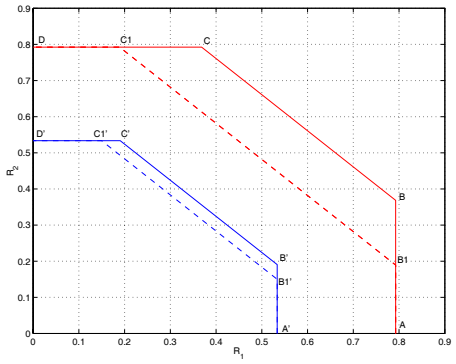

Fig. 2. Comparison joint scalar DPC with two Double DPCs for binary alphabets. Solid line delineates the capacity region of both ideal (upper) and practical coding (lower). Dashed line delineates the achievable rates with the Double DPC for both ideal (upper) and practical coding.

7. REFERENCES

[1] M. H. M. Costa, "Writing on dirty papers," *IEEE Trans. on IT*, vol. IT-29, pp. 439–441, may 1983.

[2] R. Tzschoppe, R. Bäuml, R. Fischer, J. Huber, and A. Kaup, "Additive non-gaussian noise attacks on the scalar costa scheme (scs)," in *Proc. of SPIE & IST*, San Joze, CA, USA, January 2005, pp. 114–123.

[3] P. Moulin and R. Koetter, "Data-hiding codes," in *IEEE Int. Conference on Image Processing*, Singapore, October 2004.

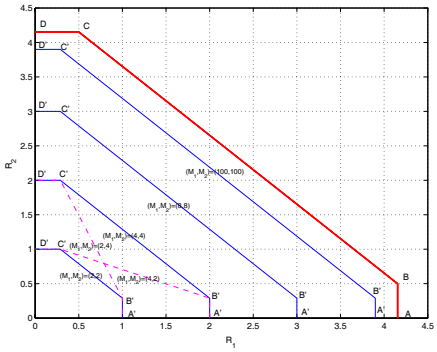

Fig. 3. Achievable rates with the joint scalar DPCs for M_1-ary and M_2-ary alphabets.

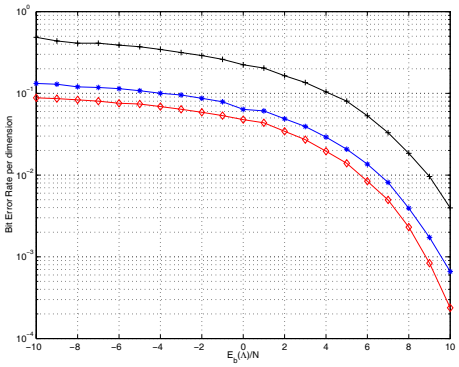

Fig. 4. Bit Error Probability v.s. (per-dimension per-bit) SNR SNR1 $= E_b(\Lambda)/N$ for QIM-embedding message W_1. From bottom to top: lattices Checkerboard D_4, Hexagonal A_2 and Cubic $\mathbb{Z}$.

[4] A. Zaidi and P. Duhamel, "Modulo lattice additive noise channel for QIM watermarking," in *proc of Int. Conf. Image Processing ICIP*, Genova, Italy, september 2005.

[5] ——, "Source-channel coding for lattice watermarking," in *proc. of European Signal Processing Conf. EUSIPCO*, Antalya, Turkey, september 2005.

[6] A. Zaidi, J. P. Pablo, and P. Duhamel, "Scalar scheme for multiple user information embedding," in *proc of IEEE Int. Conf. on Acoustics, Speech and Signal Processing, ICASSP*, Philadelphia, USA, March 18-23 2005, pp. 5–8.

[7] B. Chen and G. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information Theory*, vol. 47, pp. 1423–1443, may 2001.

[8] J. J. Eggers, R. Bäuml, R. Tzschoppe, and B. Girod, "Scalar costa scheme for information embedding," *IEEE Transactions on Signal Processing*, pp. 1003–10 019, 2003.

[9] Y.-H. Kim, A. Sutivong, and S. Sigurjonsson, "Multiple user writing on dirty paper," in *Proc. ISIT 2004*, Chicago-USA, June 2004, p. 534.

[10] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Transactions on Information Theory*, vol. IT-48, pp. 1250–1276, June 2002.

[11] J. H. Conway and N. J. A. Sloane, *Sphere Packing, Lattices and Groups*. New York: third edition, John Willey & Sons INC., 1988.