Information Embedding with Distortion Side Information

Ashish Khisti
EECS Dept. MIT
Cambridge, MA, 02139
Email: khisti@mit.edu

Emin Martinian
MERL
Cambridge, MA, 02139
Email: emin@alum.mit.edu

Gregory Wornell
EECS Dept. MIT
Cambridge, MA, 02139
Email: gww@mit.edu

***Abstract*— We use the distortion side information (DSI) framework to study the gains in information embedding when the encoder exploits sensitivity of the source samples. Our study for the Gaussian source model extends the dirty paper coding result by Costa to the case of a weighted power constraint with the weights only known to the transmitter. A coding scheme based on fixed codebook variable-partition codes is presented for this problem. We also present another coding scheme that exploits the knowledge of DSI and is robust against intentional attacks. Finally, we study a related problem of Wyner-Ziv coding with reliability side information (RSI) at the decoder. This latter setup illustrates that fixed codebook variable-partition codes could also be fundamental in systems that rely on conventional distortion measures.**

I. Introduction

The problem of information embedding (IE) has been extensively studied in recent years. See e.g. [1]–[3]. These works consider embedding a message onto a host signal known to the encoder. The embedded signal satisfies a (single-letter) distortion constraint. The focus is to characterize the maximum rate at which information can be embedded so that it can be reliably recovered after an attack. Attacks could be incidental or intentional.

The present work extends these information theoretic models to take into account perceptual factors in the distortion measure. The necessity of such extensions has already been recognized. See e.g. [4]. The natural intuition is that the higher embedding rates can be achieved if the encoder suitably exploits the varying sensitivity of different samples and embeds information accordingly. Our approach is to quantify such gains using the distortion side information (DSI) framework introduced in [5]. In this framework, the DSI sequence Q^n specifies the sensitivity of samples in a host sequence S^n by controlling the distortion measure $d(S_i, \hat{S}_i; q_i)$, $i = 1, 2, \ldots, n$. More sensitive samples naturally incur higher distortion penalty than less sensitive samples.

We first present the (public) IE problem where the encoder has access to a DSI sequence and the host sequence. The decoder does not have access to either of these sequences. We study the achievable rates for the Gaussian special case in detail and observe that it extends of the dirty paper coding problem of Costa [6] to a weighted power constraint, with the weights only known to the transmitter. Not surprisingly, the nested coding framework for this problem relies on using the fixed codebook variable-partition codes introduced (in the quantization context) in [5], [7]. We next consider the formulation where there is an active attacker as considered in [3]. We present another coding scheme that exploits the knowledge of DSI at the encoder and for which the worst case attack can be characterized. Analysis of this scheme reveals that in the high resolution limit, one does not incur significant penalty even in the presence of an intentional attacker.

The information embedding with DSI problem is also closely related to a variant of Wyner-Ziv coding. In this formulation, the decoder has access to a noisy version of the source, where the noise in each sample is a function of a parameter Q_i. We call this the *reliability side information* (RSI). Naturally, this sequence is only known to the decoder. It turns out that the fixed codebook variable-partition codes are also natural for exploiting RSI at the decoder. This setup is particularly interesting since it shows that such codes are fundamental even in scenarios that rely on conventional distortion measures. Indeed we discuss several applications of immediate interest that can benefit from such codebooks.

We note that the information theoretic capacity expressions for our formulations are straightforward extensions of [8], [9]. However, these general expressions conceal the interesting dynamics between the signal side information (e.g. host sequence in IE and noisy source sequence in Wyner-Ziv) and distortion/reliability side information. Our main contribution is to develop an understanding of this interaction by studying the achievable rates and code design of the Gaussian and binary special cases. We note that while efficient codes for dealing with signal side information inherently have a nested structure (see e.g. [10]), efficient codes that take into account either DSI or RSI must additionally support the variable-partitioning property. Furthermore, with DSI (RSI) only known at the encoder (decoder) the achievable rates we present incur a penalty with respect to the capacity (rate-distortion) with global knowledge except in the high SNR (high resolution) limit since the signal side information cannot be appropriately scaled before quantization.

A different generalization of the classical model appears in [11], [12]. Here a *vector* i.i.d. Gaussian source is considered

This work was supported in part by NSF Grant No. CCF-0515109, and by the HP/MIT Alliance.

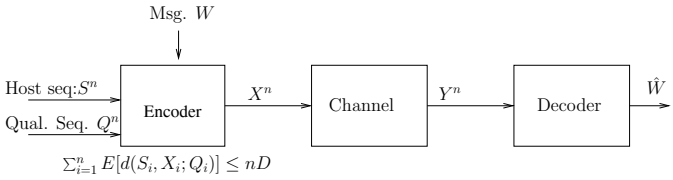

Fig. 1. Information Embedding System Diagram. The encoder has access to the host sequence and the DSI sequence. It embeds a message W and outputs X^n, subject to a distortion constraint. The channel represents either a memoryless channel or an intentional attacker.

which models, for example the block transform coefficients in the images and a quadratic distortion measure is used. Other authors (see e.g. [13]) have explored how classical quantization index modulation codes could be modified to account for perceptual measures when such information is available to both the encoder and decoder.

The information embedding with DSI problem has also been recently proposed independently in [14] as a byproduct of their analysis on coding for the deterministic broadcast channels. While the authors only report one special example for the IE problem, our correspondence with them [15] revealed that they were aware of the broader implications some of which appear in Section II in the present paper. Our investigation for the case of an intentional attacker in Section III as well as the formulation of Wyner-Ziv with RSI problem in Section IV have not been considered before to the best of our knowledge.

II. Information Embedding: Incidental Attacks

In this section, we present the information embedding problem assuming that the channel is memoryless. We assume that the host sequence S^n is drawn i.i.d. from distribution $p_S(s)$ and is independent of the DSI sequence Q^n drawn i.i.d. according to $p_Q(q)$. As shown in Figure 1, the encoder maps the state sequence S^n, the DSI sequence Q^n and the message W into a sequence X^n subject to the distortion constraint: $E[\frac{1}{n}d(S^n, X^n; Q^n)] = \frac{1}{n}\sum_{i=1}^n E[d(S_i, X_i; Q_i)] \leq D$. The channel memoryless with a transition probability $p(y|x)$. The decoder attempts to decode the message W from Y^n.

We note that our model makes a simplistic assumption that the DSI sequence Q^n is i.i.d. and independent of the host sequence. In practice the DSI sequence is context dependent and such assumptions may not be always justified. While it may be possible to extend our results to the case when the sequence Q^n is not i.i.d. we will note that even the i.i.d. model is both challenging and interesting while studying the Gaussian source models. Ultimately the model considered in this paper could be a useful first step in quantifying the fundamental gains from exploiting sensitivity of source samples.

We begin by writing down the capacity expression of our information embedding with DSI setup. The result is an immediate consequence of the Gelfand-Pinsker [8] result, taking (Q^n, S^n) as a composite state sequence.

Claim 1: The capacity of information embedding system with distortion side information at the encoder is given by

$$C_{\text{enc}} = \max \{I(U;Y) - I(U;S,Q)\} \tag{1}$$

where the maximum is taken over all distributions $p(U|S,Q)$ and functions $X = g(U,S,Q)$ that satisfy the distortion constraint $E[d(X,S;Q)] \leq D$. The alphabet $\mathcal{U}$ of U satisfies appropriate cardinality bounds and the Markov relation $(U,S,Q) \to X \to Y$ holds.

It turns out in some situations that the IE capacity in (1) is same as the capacity when the decoder is provided with the additional knowledge of (S^n, Q^n). One example is provided in [14] where a specific choice of Q and i.i.d. Gaussian source model is considered. In what follows, we explore more such situations.

A. Binary Case

Suppose that $S^n, X^n, Y^n \in \{0,1\}^n$ and $p_S(0) = p_S(1) = 1/2$. The channel is a binary symmetric channel with crossover probability p. Moreover, Q is binary as well with $p_Q(0) = \varepsilon, p_Q(1) = 1-\varepsilon$ and that $d(s,x;q) = q(s \oplus x)$ i.e. if $q = 0$, we do not incur any penalty in flipping the host sample, while if $q = 1$, we incur a unit penalty. We refer to such a distortion as erasure-Hamming distortion. Assume throughout that $D/(1-\varepsilon) \geq 1-2^{-h(p)}$ so that time-sharing is not required to achieve the information embedding capacity [2]. The IE capacity of this system is given by:

$$C_{\text{enc}}^{\text{B}} = C_{\text{full}}^{\text{B}} = \varepsilon(1-H(p))+(1-\varepsilon)\left(H\left(\frac{D}{(1-\varepsilon)}\right) - H(p)\right). \tag{2}$$

where $C_{\text{full}}^{\text{B}}$ denotes the IE capacity with (S^n, Q^n) also known to the decoder. Note that when the decoder has this extra information, the encoder and decoder can without loss in optimality use a different codebook for each value of Q. For $Q = 0$, the IE rate is $1 - H(p)$ while for $Q = 1$ the IE rate is $H(D/(1-\varepsilon)) - H(p)$. Multiplexing the two rates establishes the the expression for $C_{\text{full}}^{\text{B}}$. The achievability of $C_{\text{enc}}^{\text{B}}$ follows by evaluating (1) with $X = U = V \oplus S$, where V is independent of S with conditional distribution $p_V(0|Q=0) = p_V(1|Q=0) = 1/2$ and $p_V(1|Q=1) = 1-p_V(0|Q=1) = D/(1-\varepsilon)$. We omit this simple calculation.

Note that the test channel $U = V \oplus S$ is also the optimal test channel for quantizing a binary symmetric source with respect to an erasure-Hamming distortion [5]. This observation suggests a natural counterpart to the nested coding framework introduced in [2], [10]. The base code is a rate-distortion optimal DSI-quantization code. Indeed a *random linear code* of rate $R_Q \geq 1 - \varepsilon - (1-\varepsilon)H(D/(1-\varepsilon))$ can be used for this purpose. Cosets of this code can be used for information embedding. The total number of codewords must not exceed 2^{nR_C}, where $R_C < 1 - H(p)$ so that successful decoding is possible. The achievable IE rate $R_C - R_Q$ approaches (2).

B. Gaussian case

The host sequence is sampled i.i.d. $\mathcal{N}(0, \sigma_s^2)$. The distortion function is given by $d(s,x,q) = q(s-x)^2$. The information embedding channel is an AWGN channel $Y = X + Z$, where $Z \sim \mathcal{N}(0, \sigma_z^2)$. The alphabet of Q can be either continuous or discrete with the corresponding density $p_Q(\cdot)$. We assume that the minimum value of Q, $Q_{\min}$ is strictly greater than 0 to avoid certain technical difficulties.

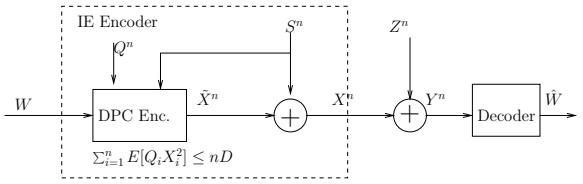

Fig. 2. Dirty paper coding channel equivalent of the Gaussian IE problem with DSI. The sequence Q^n is only revealed to the encoder and controls its power according to $\frac{1}{n}\sum_{i=1}^n E[Q_i X_i^2] \le nD$.

It is well known (see e.g. [3]) that the Gaussian information embedding setup with quadratic distortion is identical to the celebrated dirty paper coding setup of Costa [6]. If we define $\tilde{X} \triangleq X - S$, the channel model is given by $Y = \tilde{X} + S + Z$ with $E[\tilde{X}^2] \le D$. In our DSI-IE extension, the channel model is also given by $Y = \tilde{X}+S+Z$, but the input power constraint is of the form $E[Q\tilde{X}^2] \le D$. See Figure 2.

If both the encoder and decoder have access to the DSI sequence, the capacity is given by

$$C_{\text{full}}^G = E\left[\frac{1}{2}\log\left(1+\frac{D_Q^*}{\sigma_z^2}\right)\right], \tag{3}$$

where the expression for D_Q^* is implicitly given by the waterfilling equation $D_Q^* = \left[1/\lambda Q - \sigma_z^2\right]^+$ and λ is selected to satisfy $E[QD_Q^*] = D$. If neither the encoder or decoder know the DSI sequence then necessarily $\tilde{X}$ is independent of Q and our setup reduces to that of Costa with power constraint $E[\tilde{X}^2] \le D/E[Q]$. The corresponding capacity is given by

$$C_{\text{none}}^G = \frac{1}{2}\log\left(1+\frac{D}{E[Q]\sigma_z^2}\right). \tag{4}$$

Characterizing the exact capacity expression when only the encoder has knowledge of the DSI sequence is difficult even when $S \equiv 0$. Hence we provide bounds on achievable performance with encoder only DSI.

Proposition 1: Suppose that D_Q is a function of Q such that $E[QD_Q] \le D$. Then,

$$C_{\text{enc}}^{\text{G}} \ge R_{\text{enc}}^{\text{G}} = E\left[\frac{1}{2}\log\frac{D_Q}{\sigma_z^2}\right] + \frac{1}{2}\log\left(1+\frac{\sigma_z^2}{E[D_Q]}\right). \tag{5}$$

Proof: We set $U = \tilde{X} + \alpha S$, where $p(\tilde{X}|q) = \mathcal{N}(0, D_q)$ and $\tilde{X}$ is independent of S. The distortion constraint $E[Q\tilde{X}^2] \le D$ is satisfied by our assumption on D_Q. With $\alpha = E[D_Q]/(\sigma_z^2 + E[D_Q])$ we have,

$$\begin{aligned}
C_{\text{enc}} &\ge I(U;Y) - I(U;Q,S)\\
&= h(U|Q,S) - h(U|Y)\\
&= h(\tilde{X}|Q) - h(\tilde{X}+\alpha S|\tilde{X}+S+Z)\\
&= \frac{1}{2}E\log 2\pi e D_Q - h((1-\alpha)\tilde{X}+\alpha Z|\tilde{X}+S+Z)\\
&\ge \frac{1}{2}E\log 2\pi e D_Q - h((1-\alpha)\tilde{X}+\alpha Z)\\
&\ge \frac{1}{2}E\log 2\pi e D_Q - \frac{1}{2}\log 2\pi e E((1-\alpha)^2\tilde{X}^2+\alpha^2\sigma_z^2)\\
&= E\left[\frac{1}{2}\log\left(\frac{D_Q}{\sigma_Z^2}\right)\right] + \frac{1}{2}\log\left(1+\frac{\sigma_Z^2}{E[D_Q]}\right) = R_{\text{enc}}^{\text{G}}.
\end{aligned}$$

■

The expression for R_{enc} in (5) consists of two terms. The first term is similar to the expression for C_{full} in (3) but without the "1" in the logarithm. This is attributed to the 'shaping-loss" because the decoder does not have the knowledge of Q^n and hence cannot perform the appropriate MMSE scaling for each component (which depends on D_Q). However, part of shaping-loss can be recovered by a choice of α, independent of Q. This gain is represented by the second term in (5). We can show that in high SNR, DSI knowledge only at the encoder is as good as knowing it at both the encoder and the decoder and strictly better than not knowing it at the encoder.

$$\begin{aligned}
&\lim_{\sigma_z^2\to 0} C_{\text{full}}^{\text{G}} - C_{\text{enc}}^{\text{G}} = 0\\
&\lim_{\sigma_z^2\to 0} C_{\text{enc}}^{\text{G}} - C_{\text{none}}^{\text{G}} \ge \frac{1}{2}E\left[\log\frac{E[Q]}{Q}\right]
\end{aligned} \tag{6}$$

Our achievability proof in Proposition 1 lends itself to a nested coding framework. Figure 3 shows such a code in two dimensions. The left figure shows a DSI-Quantization code which supports variable-partition regions. If the horizontal coordinate is more sensitive, the quantization regions marked by the dashed line will used; if the vertical coordinate is more sensitive the regions marked by the solid line will be used. The figure on the right shows the fine code formed from the union of four cosets of the quantization code. The encoder selects one of the four cosets for quantization and thus embeds two bits of information. The decoder simply maps the received symbol vector to the nearest point in the fine code. Note that the fine code has good minimum distance. Higher dimensional constructions can also be obtained by a similar coset extension of the quantization codes presented in [7].

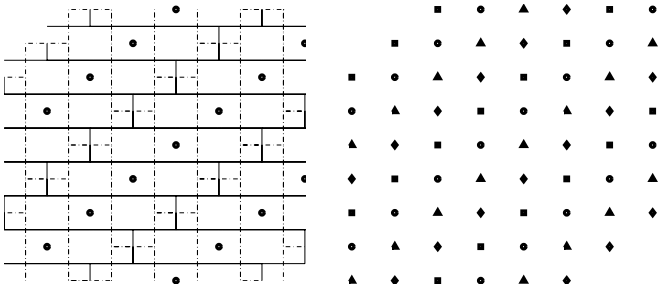

Fig. 3. Nested Coding structure for IE-DSI. The left figure shows a fixed codebook variable partition code. The quantization regions for this code can be adjusted depending on whether the horizontal or vertical coordinate is more sensitive. The corresponding quantization regions are shown by the dashed and solid lines respectively. The right figure shows the 'fine' code formed from the union of four cosets of this code. Notice that the fine code is a good channel code.

III. Watermarking: Intentional Attacks

We use a game theoretic model to study the achievable rates in the presence of intentional attacks. Accordingly, we replace the "channel" in Figure 1 with an active attacker who observes the sequence X^n and produces an output $Y^n = A_n(X^n; \Theta_A)$ where Θ_A is a source of randomness available to the attacker. The attack function must almost surely satisfy a distortion constraint $\frac{1}{n}\sum_{i=1}^n d(X_i, Y_i; Q_i) \le D_A$. We also assume that attacker is ignorant of the codebook. The attack function can

be arbitrary apart from these two constraints. Our model is along the lines of [3].

We note that the coding scheme for the binary setup in previous section the rate in (2) is also achievable in the presence of intentional attacks. It can be easily shown (along the lines by Cohen [16, sec. 6.2.2]) that the optimal attack is indeed modelled by a BSC with crossover probability $D_A/(1-\varepsilon)$.

On the other hand, the analysis of the coding scheme in Proposition 1 for the Gaussian model is difficult in the presence of intentional attacks because a) The codewords are not Gaussian since $U = \tilde{X} + \alpha S$ where $\tilde{X}$ is a Gaussian mixture; b) the transmitted sequence X^n is not statistically independent of Q^n, so the attacker can learn it upon observing X^n and use its knowledge to attack the less sensitive samples. Hence we propose and analyze another coding scheme for which the worst cast attack model can be found more easily.

Proposition 2: For the Gaussian model in Proposition 1, suppose we constrain U and X in Claim 1 as follows i) U is Gaussian ii) X is statistically independent of Q. For any D_Q such that $E[QD_Q] \leq D$ and for σ_s^2 larger than $\sup_Q D_Q$, the following rate is achievable:

$$R_{\text{enc,G}} = E\left[\frac{1}{2}\log\frac{D_Q}{\sigma_z^2}\right] + E\left[\frac{1}{2}\log\left(1-\frac{D_Q}{4\sigma_s^2}\right)\right]. \quad (7)$$

Proof: First note that since $Q_{\min} > 0$, $\sup_Q D_Q < \infty$ so the set of valid σ_s^2 is non-empty. We set $X = U = \gamma_Q S + V$, where $\gamma_Q = 1 - D_Q/2\sigma_s^2$ and V is independent of S with $p(V|q) = \mathcal{N}(0, \beta_q)$, for $\beta_Q = D_Q\left(1 - D_Q/4\sigma_s^2\right)$. Note that both $\gamma_q \geq 0$ and $\beta_q \geq 0$ by our assumption on σ_s^2.

$$E[Q(X-S)^2] = E[Q((\gamma_Q - 1)S + V)^2]$$
$$= E[Q((\gamma_Q-1)^2\sigma_s^2 + \beta_Q)] = E[QD_Q] \leq D$$

Thus the distortion constraint is satisfied. Also since $E[U^2|Q] = E[(\gamma_Q S + V)^2|Q] = \gamma_Q^2\sigma_s^2 + \beta_Q = \sigma_s^2$ we have that $p(U|q) \sim \mathcal{N}(0, \sigma_s^2)$ and thus U (and hence X) are independent of Q. Finally we evaluate:

$$I(U;Y) - I(U;Q,S) = h(U|Q,S) - h(U|Y)$$
$$= h(V|Q) - h(U|U+N) \geq h(V|Q) - h(N) = R_{\text{enc,G}}$$

■

In the above analysis we use the bound $h(U|U+N) < h(N) = 1/2\log 2\pi e\sigma_z^2$ to get the achievability rate. While it is possible to tighten this step, we instead note that the above rate is also achievable for a different channel model.

Corollary 1: For the Gaussian channel model in Proposition 1, consider instead a channel $Y = \beta_1 X + N_1$, where $\beta_1 = 1 - \sigma_z^2/\sigma_s^2$ and $N_1 \sim \mathcal{N}(0, \sigma_z^2\beta_1)$. Then the rate $R_{\text{enc,G}}$ is still achievable using the same choice of U and X.

Proof: Note that $h(U|Y) = h(U|\beta_1 U + N_1) = 1/2\log 2\pi e\sigma_z^2$. So $I(U;Y) - I(U;S,Q)$ still evaluates to $R_{\text{enc,G}}$. ■

We can now analyze the worst case attack for the under the constraints in Proposition 2. Note that since X is independent of Q, Y is necessarily independent of Q. With some effort, we can show that if Q is over a discrete alphabet, the attacker needs to satisfy the distortion constraint $\sum_{i=1}^n (X_i - Y_i)^2 \leq nD_A/E[Q]$ almost surely. The Gaussian coding scheme in Proposition 2 can be modified for analysis for the worst case attack by using the approach of Cohen and Lapidoth [3]. By introducing an equivalent encoder with codewords selected uniformly on a n-dimensional sphere of radius $\sqrt{n\sigma_s^2}$ and a decoder that selects the codeword with maximum inner product with the received sequence, we can show that the worst attack is given by $Y = (1 - \sigma_z^2/\sigma_s^2)X + Z$, where $Z \sim \mathcal{N}(0, \sigma_z^2(1-\sigma_z^2/\sigma_s^2)$ and $\sigma_z^2 = D_A/E[Q]$. Since this is precisely the channel analyzed in Corollary 1, $R_{\text{enc,G}}$ is also achievable in the presence of an active attacker.

As a final comment note that $\lim_{\sigma_z^2\to 0} C_{\text{full}}^G - R_{\text{enc,G}} = E\left[-1/2\log\left(1 - D_Q/4\sigma_s^2\right)\right] > 0$.Thus there is a loss in the achievable rate in the presence of an active attacker even in the high SNR limit. However in the regime $\sigma_s^2 \to \infty$ which is often of practical interest, the loss approaches zero.

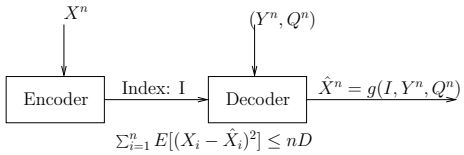

Fig. 4. Wyner-Ziv coding with reliability side information at the decoder. The source X is i.i.d. $\mathcal{N}(0, \sigma_s^2)$. (X, Y) are jointly Gaussian given the reliability parameter Q. The realization of Q^n is only known to the decoder. The lattice coding framework for this problem relies on the use of variable-partition quantizers.

IV. Wyner-Ziv coding with RSI

We now consider a related problem involving Wyner-Ziv coding illustrated in figure 4. The source sequence X^n is i.i.d. $\mathcal{N}(0, \sigma_s^2)$ which needs to be described to the decoder with a quadratic distortion $\sum_{i=1}^n E[(X_i - \hat{X}_i)^2] \leq nD$ where $\hat{X}^n$ is the reconstruction at the decoder. The decoder observes a "noisy" version of the source, say Y^n where the noise is governed by a reliability side information (RSI) sequence Q^n. We assume that conditioned on Q, X and Y are jointly Gaussian, i.e. $X = \gamma_Q Y + V$, where $p(V|q) \sim \mathcal{N}(0, \beta_q)$ is independent of Y given Q. Furthermore Q^n is i.i.d. drawn from distribution $p_Q(\cdot)$ and is independent of X^n. Also assume that $\beta_{\inf} = \inf_q \beta_q > 0$.

There are several natural applications where the decoder has access to reliability side information. For example the Wyner-Ziv video codec (see e.g. [17]) uses the previous frames as side information. The decoder can naturally estimate the relative motion in different parts of the frame and this governs the reliability of side information. As another example, sensor networks collecting data in a time varying environment may have some additional information in the background noise and may estimate the reliability of different samples.

If (Q^n, Y^n) are also available to the encoder, then the encoder simply needs to describe V^n with quadratic distortion D. The $R(D)$ curve is obtained via classical water-filling solution. In particular, if $D \leq \beta_{\inf}$, we have

$$R_{\text{full}} = E\left[\frac{1}{2}\log\frac{\beta_Q}{D}\right], \qquad \text{if } D \leq \beta_{\inf} \quad (8)$$

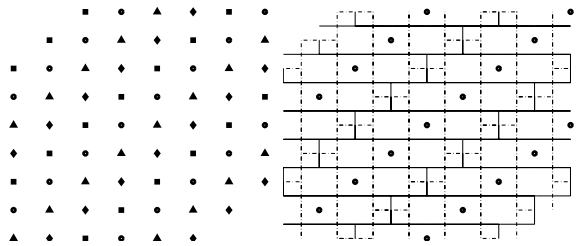

Fig. 5. Fixed-codebook variable partition codes for the Wyner-Ziv with RSI scenario. The fine quantization code on the left is a union of four cosets of a variable partition codes on the right. The construction is dual to the IE-DSI problem in Figure 3.

To develop an achievable rate for the case when only the decoder knows (Q^n, Y^n), we first note the rate distortion function of this setup in the general discrete memoryless case which is a straightforward extension of the Wyner-Ziv scheme [9].

Claim 2: The rate distortion function for Wyner-Ziv coding with reliability side information at the decoder is given by:

$$R_{\mathrm{WZ}}(D) = \min I(X; U|Y, Q) \tag{9}$$

where the minimization is over all probability distributions $p(U|X)$ and function $g(U, Y, Q)$ such that $E[d(X, g(U, Y, Q))] \leq D$. The cardinality of the alphabet of U is suitably upper bounded and $U \to X \to (Y, Q)$ holds.

To evaluate an achievable rate for the Gaussian case, we set $U = \alpha X + E$, where $\alpha = 1 - D/E[\beta_Q]$ and $E \sim \mathcal{N}(0, \alpha D)$ is independent of X. It suffices to set $g(U, Y, Q) = U$ since $E[(U - X)^2] = E[((\alpha - 1)X + E)^2] = D$.

$$\begin{aligned} R_{\mathrm{dec}} &= h(U|Q, Y) - h(U|X) = h(\alpha V + E|Q) - h(E) \\ &= E\left[\frac{1}{2}\log\left(\frac{\beta_Q}{D} + 1 - \frac{\beta_Q}{E[\beta_Q]}\right)\right] \end{aligned}$$

We note that the above scheme is optimal in high-resolution

$$\lim_{D \to 0} R_{\mathrm{dec}} - R_{\mathrm{full}} = 0. \tag{10}$$

The result in Claim 2 relies on the decoder finding a U^n jointly typical with (Y^n, Q^n) in the bin index specified by the encoder. How can the decoder exploit the knowledge of Q^n in the lattice framework? The natural solution is to use a fixed codebook variable-partition codes. Figure 5 illustrates such a code in two dimensions. The fine quantization code on the left is a union of four cosets of a variable partition codebook on the right. The encoder quantizes the source symbol pair (X_1, X_2) to the nearest point in the fine lattice and sends the coset index of this point. The decoder upon receiving the coset index, constructs the partition regions of the corresponding lattice using the knowledge of (Q_1, Q_2). It creates the regions marked by the solid lines if the vertical coordinate is more reliable or the regions marked by the dashed lines if the horizontal coordinate is more reliable. It reconstructs the center of the cell in which (Y_1, Y_2) lies as the corresponding reconstruction point.

Note that this code construction is the dual of the information embedding with DSI problem. Another situation where fixed codebook variable partition codes are used is fading channels with receiver only channel state information [18, sec 5.4.4]. Indeed efficient practical code constructions for such channels is an active area of research.

V. Conclusion

We have extended the framework of distortion side information and fixed codebook variable partition codes, originally proposed for quantization problems in [5] to information embedding with distortion side information and Wyner-Ziv coding with reliability side information. Our analysis for information embedding under a Gaussian source model extends Costa's dirty paper coding result to the case of a weighted power constraint with weights only known to the encoder. Coding schemes which exploit encoder only DSI and are robust against intentional attackers are also developed. The Wyner-Ziv problem with reliability side information at the decoder reveals the importance of variable-partition codebooks in situations which rely on conventional distortion measures. We discuss some immediate applications of this setting and hope that it sparks further interest in understanding the structure and properties of fixed codebook variable-partition codes.

References

[1] P. Moulin and J. O'Sullivan, "Information-theoretic analysis of information hiding," *IEEE Trans. Inform. Theory*, vol. 49, pp. 563–593, Mar. 2003.

[2] R. J. Barron, B. Chen, and G. W. Wornell, "The duality between information embedding and source coding with side information and some applications," *IEEE Trans. Inform. Theory*, vol. 49, 2003.

[3] A. S. Cohen and A. Lapidoth, "The Gaussian watermarking game," *IEEE Trans. Inform. Theory*, vol. 48, pp. 1639–1667, June 2002.

[4] A. Sequeira and D. Kundur, "Communication and Information Theory in Watermarking: A survey," in *SPIE*, Denver, Aug. 2001, pp. 216–227.

[5] E. Martinian, G. W. Wornell, and R. Zamir, "Source Coding with Encoder Side Informaton," *submitted to IEEE Trans. Inform. Theory*, Dec. 2004. [Online]. Available: http://arxiv.org/abs/cs.IT/0412112

[6] M. H. Costa, "Writing on dirty paper," *IEEE Trans. Inform. Theory*, vol. 29, pp. 439–441, May 1983.

[7] E. Martinian, "Dynamic information and constraints in source and channel coding," Ph.D. dissertation, Mass. Instit. of Tech., 2004.

[8] S. I. Gel'fand and M. S. Pinsker, "Coding for channels with random parameters," *Problems of Control and Information Theory*, vol. 9, pp. 19–31, 1980.

[9] A. D. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inform. Theory*, vol. 22, pp. 1–10, Jan. 1976.

[10] R. Zamir, S. Shamai, and U. Erez, "Nested codes: an algebraic binning scheme for noisy multiterminal networks," *IEEE Trans. Inform. Theory*, vol. 42, June 2002.

[11] M. Mihack and P. Moulin, "The parallel-Gaussian watermarking game," *IEEE Trans. Inform. Theory*, vol. 50, pp. 272–289, Feb. 2004.

[12] A. Cohen and A. Lapidoth, "The capacity of the vector Gaussian watermarking game," in *Proc. Int. Symp. Inform. Theory*, Washington DC, June 2001, p. 4.

[13] C. K. Wang, M. L. Miller, and I. J. Cox, "Using perceptual distance to improve the selection of dirty paper trellis codes for watermarking," in *IEEE Int. Workshop on Multimedia Signal Processing*, 2004, pp. 147–150.

[14] E. Haim and R. Zamir, "Quantization with variable resolution and coding for deterministic broadcast channels," in *Allerton Conference on Communication, Control, and Computing*, 2005.

[15] R. Zamir, "Personal communication." 2006.

[16] A. Cohen, "Information theoretic analysis of watermarking systems," Ph.D. dissertation, Mass. Instit. of Tech., 2001.

[17] R. Puri and K. Ramchandran, "PRISM: A video coding paradigm based on motion-compensated prediction at the decoder," *IEEE Trans. on Image Processing*, submitted.

[18] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.