Journal of VLSI Signal Processing 27, 7–33, 2001

Quantization Index Modulation Methods for Digital Watermarking and Information Embedding of Multimedia

BRIAN CHEN AND GREGORY W. WORNELL
Department of Electrical Engineering and Computer Science and the Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA, USA

Received July 14, 1999; Revised April 5, 2000

Abstract. Copyright notification and enforcement, authentication, covert communication, and hybrid transmission applications such as digital audio broadcasting are examples of emerging multimedia applications for digital watermarking and information embedding methods, methods for embedding one signal (e.g., the digital watermark) within another "host" signal to form a third, "composite" signal. The embedding is designed to achieve efficient trade-offs among the three conflicting goals of maximizing information-embedding rate, minimizing distortion between the host signal and composite signal, and maximizing the robustness of the embedding.

We present a class of embedding methods called quantization index modulation (QIM) that achieve provably good rate-distortion-robustness performance. These methods, and low-complexity realizations of them called dither modulation, are provably better than both previously proposed linear methods of spread spectrum and nonlinear methods of low-bit(s) modulation against square-error distortion-constrained intentional attacks. We also derive information-embedding capacities for the case of a colored Gaussian host signal and additive colored Gaussian noise attacks. These results imply an information embedding capacity of about 1/3 b/s of embedded digital rate for every Hertz of host signal bandwidth and every dB drop in received host signal quality.

We show that QIM methods achieve performance within 1.6 dB of capacity, and we introduce a form of post-processing we refer to as distortion compensation that, when combined with QIM, allows capacity to be achieved. In addition, we show that distortion-compensated QIM is an optimal embedding strategy against some important classes of intentional attacks as well. Finally, we report simulation results that demonstrate the performance of dither modulation realizations that can be implemented with only a few adders and scalar quantizers.

Keywords: digital watermarking, information embedding, quantization index modulation, dither modulation, distortion compensation

1. Introduction

Digital watermarking and information embedding systems have a number of important multimedia applications [1, 2]. These systems embed one signal, sometimes called an "embedded signal" or "watermark", within another signal, called a "host signal". The embedding must be done such that the embedded signal causes no serious degradation to its host. At the same time, the embedding must be robust to common degradations to the composite host and watermark signal, which in some applications result from deliberate attacks. Ideally, whenever the host signal survives these degradations, the watermark also survives.

One commonly cited application is copyright notification and enforcement for multimedia content such as audio, video, and images that are distributed in digital formats. For example, watermarking techniques have been proposed for enforcing copy-once features in digital video disc recorders [3, 4]. Authentication of, or detection of tampering with, multimedia signals is another application of digital watermarking methods

[5], as is covert communication, sometimes called "steganography" [6] or low probability of detection communication.

Although not yet widely recognized as such, hybrid transmission is yet another group of information embedding applications [7]. In these cases the host signal and embedded signal are two different signals that are transmitted simultaneously over the same channel in the same bandwith. So-called hybrid in-band on-channel digital audio broadcasting (DAB) [8, 9] is an example of such a multimedia application where one may employ information embedding methods to backwards-compatibly upgrade the existing commercial broadcast radio system. In this application one would like to simultaneously transmit a digital signal with existing analog (AM and/or FM) commercial broadcast radio without interfering with conventional analog reception. Thus, the analog signal is the host signal and the digital signal is the watermark. Since the embedding does not degrade the host signal too much, conventional analog receivers can demodulate the analog host signal. In addition, next-generation digital receivers can decode the digital signal embedded within the analog signal. This embedded digital signal may be all or part of a digital audio signal, an enhancement signal used to refine the analog signal, or supplemental information such as station identification. More generally, the host signal in these hybrid transmission systems could be some other type of analog signal such as video [10] or even a digital waveform. For example, a digital pager signal could be embedded within a digital cellular telephone signal.

Another application is automated monitoring of airplay of advertisements. Advertisers can embed a digital watermark within their ads and count the number of times the watermark occurs during a given broadcast period, thus ensuring that their ads are played as often as promised. In this case, however, the watermark is embedded within the baseband source signal (the advertisement), whereas in other hybrid transmission applications the digital signal may be embedded in either the baseband source signal or the passband modulated signal (a passband FM signal, for example).

A number of information-embedding algorithms have been proposed [1, 2] in this still emerging field. One class of nonlinear methods involves a quantize-and-replace strategy: after first quantizing the host signal, these systems change the quantization value to embed information. A simple example of such a system is so-called low-bit(s) modulation (LBM), where the least significant bit(s) in the quantization of the host signal are replaced by binary representation of the embedded signal. These methods range from simple replacement of the least significant bit(s) of the pixels of an image to more sophisticated methods that involve transformation of the host signal before quantization and adjustment of the quantization step sizes [10]. As we will show later, such methods are inherently less efficient than the quantization index modulation methods [7, 11] discussed in this paper in terms of the amount of embedding-induced distortion for a given rate and robustness. Linear classes of methods such as spread-spectrum methods embed information by linearly combining the host signal with a small pseudo-noise signal that is modulated by the embedded signal. Although these methods have received considerable attention in the literature [12–15], linear methods in general and spread-spectrum methods in particular are limited by host-signal interference when the host signal is not known at the decoder, as is typical in many of the applications mentioned above. Intuitively, the host signal in a spread spectrum system is an additive interference that is often much larger, due to distortion constraints, than the pseudo-noise signal carrying the embedded information.

Quantization index modulation (QIM) methods, a class of nonlinear methods that we describe in this paper, reject this host-signal interference. As a result, these methods have very favorable performance characteristics in terms of their achievable trade-offs among the robustness of the embedding, the degradation to the host signal caused by the embedding, and the amount of data embedded.

In Section 2 we formulate a general model of information-embedding problems and provide examples of how the model can be applied to many of the applications discussed above. In Section 3 we show that a very natural way of classifying digital watermarking methods is by whether or not the host signal interferes with watermark extracting. In particular, methods that can reject host-interference are generally preferred, and we discuss one class of host-interference rejecting information-embedding methods in Section 4, namely quantization index modulation. We also discuss distortion-compensated QIM (DC-QIM), a post-processing enhancement of QIM, and dither modulation, a convenient subclass of QIM with several low-complexity realizations, in this section. As we discuss in Section 5, in a fairly general Gaussian case, QIM methods exist that achieve performance within a

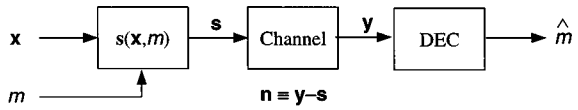


Figure 1. General information-embedding problem model. A message m is embedded in the host signal vector x using some embedding function $\mathbf{s}(x, m)$. A perturbation vector n corrupts the composite signal s. The decoder extracts an estimate $\hat{m}$ of m from the noisy channel output y.

few dB of capacity, and DC-QIM methods exist that achieve capacity. We also discuss the implications for multimedia applications like hybrid transmission and authentication, the main result being that a 3-dB drop in received host signal quality is worth about 1 b/s/Hz in embedded digital rate. Some simulation results are presented in Section 6 and some concluding remarks in Section 7.

2. Problem Models

Although the information-embedding applications described in Section 1 are quite diverse, the simple problem model of Fig. 1 captures most of their fundamental features. We wish to embed some digital information or watermark m in some host signal vector $\mathsf{x} \in \Re^N$. This host signal could be a vector of pixel values or Discrete Cosine Transform (DCT) coefficients from an image, for example. Alternatively, the host signal could be a vector of samples or transform coefficients, such as Discrete Fourier Transform (DFT) or linear prediction coding coefficients, from an audio or speech signal. We wish to embed at a rate of R_m bits per dimension (bits per host signal sample) so we can think of m as an integer, where

$$m \in \{1, 2, \ldots, 2^{NR_m}\}. \tag{1}$$

An embedding function maps the host signal x and embedded information m to a composite signal $\mathsf{s} \in \Re^N$. The embedding should not unacceptably degrade the host signal, so we have some distortion measure $D(\mathsf{s}, \mathsf{x})$ between the composite and host signals. For example, one might choose the square-error distortion measure

$$D(\mathsf{s}, \mathsf{x}) = \frac{1}{N}\|\mathsf{s} - \mathsf{x}\|^2. \tag{2}$$

In some cases we may measure the expected distortion $D_{\mathbf{s}} = E[D(\mathsf{s}, \mathsf{x})]$. The composite signal s is subjected to various common signal processing manipulations such as lossy compression, addition of random noise, and resampling, as well as deliberate attempts to remove the embedded information. These manipulations occur in some channel, which produces an output signal $\mathsf{y} \in \Re^N$. For convenience, we define a perturbation vector $\mathsf{n} \in \Re^N$ to be the difference $\mathsf{y} - \mathsf{s}$. Thus, this model is sufficiently general to include both random and deterministic, and both signal-independent and signal-dependent, perturbation vectors. The decoder forms an estimate $\hat{m}$ of the embedded information m based on the channel output y. The roubustness of the overall embedding-decoding method is characterized by the class of perturbation vectors over which the estimate $\hat{m}$ is reliable, where reliable means either that $\hat{m} = m$ deterministically or that $\Pr[\hat{m} \neq m] < \epsilon$. In some cases, one can conveniently characterize the size of this tolerable class of perturbations, and hence the robustness, with a single parameter. Here are a few examples:

1. **Bounded Perturbation Channels:** In this case we consider the largest perturbation energy per dimension σ_n^2 such that we can guarantee $\hat{m} = m$ for every perturbation vector that satisfies

$$\|\mathsf{n}\|^2 \leq N\sigma_n^2. \tag{3}$$

   This channel model describes a maximum distortion[1] or minimum SNR constraint between the channel input and output and, hence, may be an appropriate model for either the effect of a lossy compression algorithm or attempts by an active attacker to remove the embedded signal, for example.
2. **Bounded Host-Distortion Channels:** Some attackers may work with distortion constraint between the host signal, rather than the channel input, and the channel output since this distortion is the most direct measure of degradation to the host signal. For example, if an attacker has partial knowledge of the host signal, which may be in the form of a probability distribution so that he or she can calculate this distortion then it may be appropriate to bound the expected distortion $D_{\mathbf{y}} = E[D(\mathbf{y}, \mathsf{x})]$, where this expectation is taken over the probability density of x given the channel input s.
3. **Additive Noise Channels:** In this case the perturbation vector n is modeled as random and statistically independent of s. An additive white Gaussian noise (AWGN) channel is an example of such a channel, and the natural robustness measure in this case is

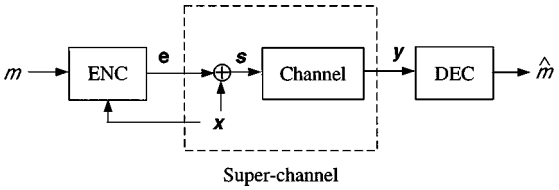


Figure 2. Equivalent super-channel model for information embedding. The composite signal is the sum of the host signal, which is the state of the super-channel, and a host-dependent distortion signal.

the maximum noise variance σ_n^2 such that the probability of error is sufficiently low. As we discuss in Section 5, this additive Gaussian noise channel model may be appropriate for a variety of applications, including hybrid transmission.

The first two channel models are appropriate models for distortion-constrained, intentional attacks and are discussed in detail in [11]. The third model may be appropriate for a number of unintentional or incidental attacks and is the topic of Section 5. In general, one can specify the robustness and class of tolerable perturbation vectors in terms of a conditional probability law $p_{\mathbf{y}|\mathbf{s}}(\mathbf{y} \mid \mathbf{s})$ in the probabilistic case or in terms of a set of possible outputs $\mathcal{P}\{\mathbf{y} \mid \mathbf{s}\}$ for any given input in the deterministic case.

An alternative representation of the model of Fig. 1 is shown in Fig. 2. The two models are equivalent since any embedding function $\mathbf{s}(\mathsf{x}, m)$ can be written as the sum of the host signal x and a host-dependent distortion signal $\mathbf{e}(\mathsf{x}, m)$,

$$\mathbf{s}(\mathsf{x}, m) = \mathsf{x} + \mathbf{e}(\mathsf{x}, m),$$

simply by defining the distortion signal to be $\mathbf{e}(\mathsf{x}, m) \triangleq \mathbf{s}(\mathsf{x}, m) - \mathsf{x}$. Thus, one can view e as the input to a super-channel that consists of the cascade of an adder and the true channel. The host signal x is a state of this super-channel that is known at the encoder. The measure of distortion $D(\mathsf{s}, \mathsf{x})$ between the composite and host signals maps onto a host-dependent measure of the size $P(\mathsf{e}, \mathsf{x}) = D(\mathsf{x} + \mathsf{e}, \mathsf{x})$ of the distortion signal e. For example, square-error distortion (2) equals the power of e,

$$\frac{1}{N}\|\mathsf{s} - \mathsf{x}\|^2 = \frac{1}{N}\|\mathsf{e}\|^2.$$

Therefore, one can view information embedding problems as power-limited communication over a super-channel with a state that is known at the encoder.[2] This view can be convenient for determining achievable rate-distortion-robustness trade-offs of various information embedding and decoding methods, as will become apparent in Section 5.

One desires the embedding system to have high rate, low distortion, and high robustness, but in general these three goals conflict. Thus, the performance of an information embedding system is characterized in terms of its achievable rate-distortion-robustness trade-offs.

3. Classes of Embedding Methods

An extremely large number of embedding methods have been proposed in the literature [1, 2, 6]. Rather than discussing the implementational details of this myriad of specific algorithms, in this section we focus our discussion on the common performance characteristics of broad classes of methods. Because in this paper we often examine watermarking at the highest, most fundamental level, our classification system is based on the types of behaviors that different watermarking systems exhibit as a result of the properties of their respective embedding functions. In particular, our taxonomy of embedding methods includes two classes: (1) host-interference non-rejecting methods and (2) host-interference rejecting methods.

3.1. Host-Interference Non-Rejecting Methods

A large number of embedding algorithms are designed based on the premise that the host signal is like a source of noise or interference. This view arises when one neglects the fact that the encoder in Fig. 2 has access to, and hence can exploit knowledge of, the host signal x.

The simplest of this class have purely additive embedding functions of the form

$$\mathbf{s}(\mathsf{x}, m) = \mathsf{x} + \mathbf{w}(m), \tag{4}$$

where $\mathbf{w}(m)$ is typically a pseudo-noise sequence. Embedding methods in this class are often referred to as spread spectrum methods and some of the earliest examples are given by Tirkel et al. [16, 17], Bender et al. [12], Cox et al. [13, 18], and Smith and Comiskey [14]. (The "Patchwork" algorithm [12] of Bender et al., involves adding a small amount δ to some pseudorandomly chosen host signal samples and subtracting a small amount δ from others. Thus, this method is equivalent to adding a pseudorandom sequence $\mathbf{w}(m)$

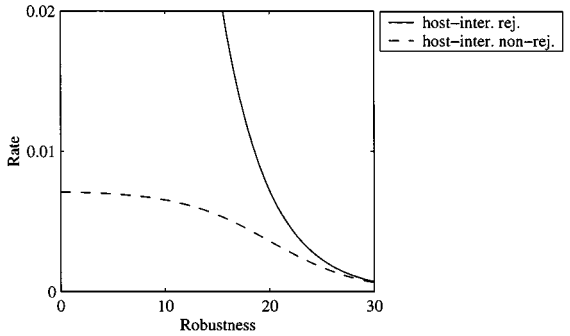


Figure 3. Qualitative behavior of host-interference rejecting and non-rejecting embedding methods. The dashed curve's upper rate threshold at low levels of robustness (low levels of channel interference) indicates host-interference-limited performance.

of $\pm\delta$ to the host signal, and hence, we consider the Patchwork algorithm to be a spread spectrum method.)

From (4), we see that for this class of embedding methods, the host signal x acts as additive interference that inhibits the decoder's ability to estimate m. Consequently, even in the absence of any channel perturbations ($\mathbf{n} = \mathbf{0}$), one can usually embed only a small amount of information. Thus, these methods are useful primarily when either the host signal is available at the decoder or when the host signal interference is much smaller than the channel interference. Indeed, in [18] Cox et al., assume that x is available at the decoder.

The host-interference-limited performance of purely additive (4) embedding methods is embodied in Fig. 3 as the upper limit on rate of the dashed curve, which represents the achievable rate-robustness performance of non-host-interference rejecting methods, at a fixed level of embedding-induced distortion. Although the numerical values on the axes of Fig. 3 correspond to the case of Gaussian host signals and additive white Gaussian noise channels, which are discussed in Section 5,[3] the upper rate threshold of the dashed curve is actually representative of the *qualitative* behavior of host-interference non-rejecting methods in general. Indeed, a similar upper rate threshold was derived by Su [19] for the case of so-called power-spectrum condition-compliant additive watermarks and Wiener attacks.

A common variation of purely additive spread spectrum methods have weighted-additive embedding functions of the form

$$s_i(\mathsf{x}, m) = x_i + a_i(\mathsf{x})w_i(m), \tag{5}$$

where the subscript i denotes the i-th element of the corresponding vector, i.e., the i-th element of $\mathbf{w}(m)$ is weighted with an amplitude factor $a_i(\mathsf{x})$. The amplitude factors $a_i(\mathsf{x})$ account for human perceptual characteristics, and an example of an embedding function within this class is proposed by Podilchuk and Zeng [20], where the amplitude factors $a_i(\mathsf{x})$ are set according to just noticeable difference (JND) levels computed from the host signal.

A special subclass of weighted-additive embedding functions, given in [18], arise by letting the amplitude factors be proportional to x so that

$$a_i(\mathsf{x}) = \lambda x_i,$$

where λ is a constant. Thus, these embedding functions have the property that large host signal samples are altered more than small host signal samples. This special subclass of embedding functions are purely additive in the log-domain since

$$s_i(\mathsf{x}, m) = x_i + \lambda x_i w_i(m) = x_i(1 + \lambda w_i(m))$$

implies that

$$\log s_i(\mathsf{x}, m) = \log x_i + \log(1 + \lambda w_i(m)).$$

Since the log function is invertible, if one has difficulty in recovering m from the composite signal in the log-domain due to host signal interference, then one must also encounter difficulty in recovering m from the composite signal in the non-log-domain. Thus, host-proportional amplitude weighting also results in host signal interference, although the probability distributions of the interference $\log x_i$ and of the watermark pseudo-noise $\log(1 + \lambda w_i(m))$ are, of course, in general different than the probability distributions of x_i and $w_i(m)$. Although in the more general weighted-additive case (5), the encoder in Fig. 2 is not ignoring x since

$$e_i(\mathsf{x}, m) = a_i(\mathsf{x})w_i(m),$$

in general unless the weighting functions $a_i(\mathsf{x})$ are explicitly designed to reject host interference in addition to exploiting perceptual models, host interference will still limit performance and thus this class of systems will still exhibit the qualitative behavior represented by the dashed curve in Fig. 3. We remark that in proposing the weighted-additive and log-additive embedding functions, Podilchuk and Zeng [20] and Cox et al. [18], respectively, were actually considering the case where the host signal was available at the decoder, and hence, host interference was not an issue.

3.2. Host-Interference Rejecting Methods

Having seen the inherent limitations of embedding methods that do not reject host interference by exploiting knowledge of the host signal at the encoder, we now discuss some examples of host-interference rejecting methods. In Section 4 we present a novel subclass of such host-interference rejecting methods called quantization index modulation (QIM). This QIM class of embedding methods exhibits the type of behavior illustrated by the solid curve in Fig. 3, while providing enough structure to allow the system designer to easily trade off rate, distortion, and robustness, i.e., to move from one point on the solid curve of Fig. 3 to another.

3.2.1. Generalized Low-Bit Modulation. Swanson, Zhu, and Tewfik [10] have proposed an example of a host-interference rejecting embedding method that one might call "generalized low-bit modulation (LBM)", although Swanson et al., do not use this term explicitly. The method consists of two steps: (1) linear projection onto a pseudorandom direction and (2) quantization and perturbation, as illustrated in Fig. 4. In the first step the host signal vector x is projected onto a pseudorandom vector $\mathbf{v}$ to obtain

$$\tilde{x} = \mathsf{x}^T\mathbf{v}.$$

Then, information is embedded in $\tilde{x}$ by quantizing it with a uniform, scalar quantizer of step size Δ and perturbing the reconstruction point by an amount that is determined by m. (No information is embedded in components of x that are orthogonal to $\mathbf{v}$.) Thus, the projection $\tilde{s}$ of the composite signal onto $\mathbf{v}$ is

$$\tilde{s} = q(\tilde{x}) + d(m),$$

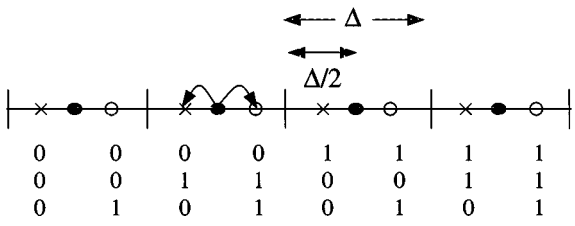


Figure 4. Equivalence of quantization and perturbation to low-bit modulation. Quantizing with step size Δ and perturbing the reconstruction point is equivalent to quantizing with step size $\Delta/2$ and modulating the least significant bit. In general, the defining property of low-bit modulation is that the quantization cells for $\times$ points and $\circ$ points are the same.

where $q(\cdot)$ is a uniform, scalar quantization function of step size Δ and $d(m)$ is a perturbation value, and the composite signal vector is

$$\mathsf{s} = x + (\tilde{s} - \tilde{x})\mathbf{v}.$$

For example, suppose $\tilde{x}$ lies somewhere in the second quantization cell from the left in Fig. 4 and we wish to embed 1 bit. Then, $q(\tilde{x})$ is represented by the solid dot ($\bullet$) in that cell, $d(m) = \pm\Delta/4$, and $\tilde{s}$ will either be the $\times$-point (to embed a 0-bit) or the $\circ$-point (to embed a 1-bit) in the same cell. In [10] Swanson et al., note that one can embed more than 1 bit in the N-dimensional vector by choosing additional projection vectors $\mathbf{v}$. One could also, it seems, have only one projection vector $\mathbf{v}$, but more than two possible perturbation values $d(1), d(2), \ldots, d(2^{NR_m})$.

We notice that all host signal values $\tilde{x}$ that map onto a given $\times$ point when a 0-bit is embedded will map onto the same $\circ$ point when a 1-bit is embedded. As a result of this condition, one can label the $\times$ and $\circ$ points with bit labels such that the embedding function is equivalent to low-bit modulation. Specifically, this quantization and perturbation process is equivalent to the following:

1. Quantize $\tilde{x}$ with a quantizer of step size $\Delta/2$ whose reconstruction points are the union of the set of $\times$ points and set of $\circ$ points. These reconstruction points have bit labels as shown in Fig. 4.
2. Modulate (replace) the least significant bit in the bit label with the watermark bit to arrive at a composite signal bit label. Set the composite signal projection value $\tilde{s}$ to the reconstruction point with this composite signal bit label.

Thus, the quantization and perturbation embedding method in [10] is low-bit modulation of the quantization of $\tilde{x}$.

An earlier paper [21] by Swanson et al., gives another example of generalized low-bit modulation, where a data bit is repeatedly embedded in the DCT coefficients of a block rather than in the projections onto pseudorandom directions. One can view the DCT basis vectors, then, as the projection vectors $\mathbf{v}$ in the discussion above. The actual embedding occurs through quantization and perturbation, which we now recognize as low-bit modulation.

Some people may prefer to use the term "low-bit modulation" only to refer to the modulation of the least

significant bits of pixel values that are already quantized, for example, when the host signal is an 8-bit grayscale image. This corresponds to the special case when the vectors $\mathbf{v}$ are "standard basis" vectors, i.e., $\mathbf{v}$ is a column of the identity matrix, and $\Delta = 2$. To emphasize that the quantization may occur in any domain, not just in the pixel domain, and that one may adjust the step size Δ to any desired value, we used the term "generalized LBM" above when first introducing the technique of Swanson et al. However, in this paper the term LBM, even without the word "generalized" in front of it, refers to low-bit modulation in its most general sense.

In general, low-bit modulation methods have the defining property that the embedding intervals, the set of host signal values that map onto a composite signal value, for the $\times$ points and $\circ$ points are the same. For example, in Fig. 4 *every* host signal value that maps onto the $\times$ point labeled "010" when a 0-bit is embedded maps onto the $\circ$ point labeled "011" (as opposed to one of the other $\circ$ points) when a 1-bit is embedded. On the other hand, suppose that the embedding interval of the 010-point intersected the embedding intervals of both the 011-point and the 001-point. Then, no low-bit modulation method could have the equivalent embedding function (equivalent embedding intervals and composite signal values) since the bit labels of the 001-point and 011-point in Fig. 4 cannot both simultaneously differ from the bit label of the 010-point in only the least significant bit.

Because the $\times$ and $\circ$ points in Fig. 4 are separated by some nonzero distance, we see that these LBM methods do, in fact, reject host-signal interference. The host signal $\tilde{x}$ determines the particular $\times$ or $\circ$ point that is chosen as the composite signal value $\tilde{s}$, but does not inhibit the decoder's ability to determine whether $\tilde{s}$ is a $\times$ point or a $\circ$ point, and hence, determine whether the embedded bit is a 0-bit or 1-bit.

However, the defining property of LBM methods that the embedding intervals for the $\times$ points and $\circ$ points are the same is an unnecessary constraint on the embedding function $\mathbf{s}(x, m)$. As discussed in Section 4.5, and in [7, 11, 22], by removing this constraint, one can find embedding functions that result in better rate-distortion-robustness performance than that obtainable by LBM.

3.2.2. Other Host-Interference Rejecting Methods. Another host-interference rejecting method is disclosed in a recently issued patent [23]. Instead of embedding information in the quantization levels, information is embedded in the number of host signal "peaks" that lie within a given amplitude band. For example, to embed a 1-bit one may force the composite signal to have exactly two peaks within the amplitude band. To embed a 0-bit, the number of peaks is set to less than two. Clearly, the host signal does not inhibit the decoder's ability to determine how many composite signal peaks lie within the amplitude band. The host signal does, however, affect the amount of embedding-induced distortion that must be incurred to obtain a composite signal with a given number of peaks in the amplitude band. For example, suppose the host signal has a large number of peaks in the amplitude band. If one tries to force the number of peaks in the band to be less than two in order to embed a 0-bit, then the distortion between the resulting composite signal and host signal may be quite significant. Thus, even though this method rejects host-interference, it is not clear that it exhibits the desired behavior illustrated by the solid curve in Fig. 3. For example, to achieve a high rate when the channel noise is low, one needs to assign at least one number of signal peaks to represent $m = 1$, another number of signal peaks to represent $m = 2$, another number of signal peaks to represents $m = 3$, etc. Thus, one could potentially be required to alter the number of host signal peaks to be as low as 1 or as high as 2^{NR_m}. It is unclear whether or not one can alter the number of host signal peaks within the amplitude band by such a large amount without incurring too much distortion.

4. Quantization Index Modulation Methods

One class of embedding methods that achieves very good, and in some cases optimal, rate-distortion-robustness trade-offs are so-called quantization index modulation (QIM) methods [11]. In this section, we describe the basic principles behind this class of methods, present some low-complexity realizations, and point out some known attractive performance features of these methods. In later sections we develop additional insights into the performance capabilities of these methods.

4.1. Basic Principles

One can view the embedding function $\mathbf{s}(x, m)$ as an ensemble of functions of x, each function in the ensemble

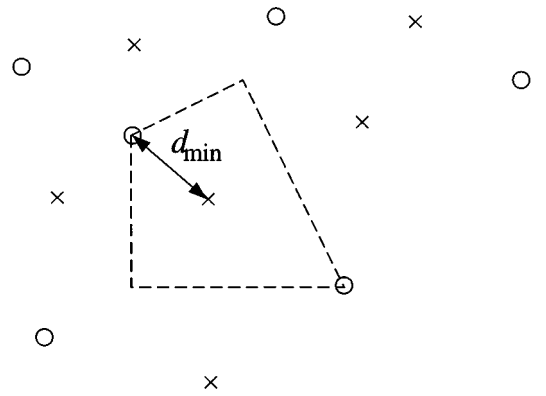


Figure 5. Quantization index modulation for information embedding. The points marked with $\times$'s and $\circ$'s belong to two different quantizers, each with its associated index. The minimum distance $d_{\min}$ measures the robustness to perturbations, and the sizes of the quantization cells, one of which is shown in the figure, determine the distortion. If $m = 1$, the host signal is quantized to the nearest $\times$. If $m = 2$, the host signal is quantized to the nearest $\circ$.

indexed by m . We denote the functions in this ensemble as $\mathbf{s}(\mathsf{x}; m)$ to emphasize this view. If the embedding-induced distortion is to be small, then each function in the ensemble must be close to an identity function in some sense so that

$$\mathbf{s}(\mathsf{x}; m) \approx \mathsf{x}, \quad \forall m.$$

If all of these approximate identity functions are quantizers, then the embedding method is a QIM method.

Thus, quantization index modulation refers to embedding information by first modulating an index or sequence of indices with the embedded information and then quantizing the host signal with the associated quantizer or sequence of quantizers. Figure 5 illustrates QIM in the case where one bit is to be embedded so that $m \in \{1, 2\}$. Thus, we require two quantizers, and their corresponding sets of reconstruction points in $\Re^N$ are represented in Fig. 5 with $\times$'s and $\circ$'s. If $m = 1$, for example, the host signal is quantized with the $\times$-quantizer, i.e., s is chosen to be the $\times$ closest to x. If $m = 2$, x is quantized with the $\circ$-quantizer. The sets of reconstruction points are non-intersecting as no $\times$ point is the same as any $\circ$ point. This non-intersection property leads to host-signal interference rejection. As x varies, the composite signal value s varies from one $\times$ point ($m = 1$) to another or from one $\circ$ point ($m = 2$) to another, but it never varies between a $\times$ point and a $\circ$ point. Thus, even with an infinite energy host signal, one can determine m if channel perturbations are not too severe. The $\times$ points and $\circ$ points are both quantizer reconstruction points for x and signal constellation points for communicating m. (One *set* of points, rather than one individual point, exists for each possible value of m). Thus, we may view design of QIM systems as the simultaneous design of an ensemble of quantizers (or source codes) and signal constellations (or channel codes).

The structure of QIM systems is convenient from an engineering perspective since properties of the quantizer ensemble can be connected to the performance parameters of rate, distortion, and robustness. For example, the number of quantizers in the ensemble determines the number of possible values of m, or equivalently, the rate. The sizes and shapes of the quantization cells, one of which is represented by the dashed polygon in Fig. 5, determines the amount of embedding-induced distortion, all of which arises from quantization error. Finally, for many classes of channels, the minimum distance $d_{\min}$ between the sets of reconstruction points of different quantizers in the ensemble determines the robustness of the embedding. We define the minimum distance to be

$$d_{\min} \stackrel{\Delta}{=} \min_{(i,j):i\neq j} \min_{(\mathbf{x}_i,\mathbf{x}_j)} \big\|\mathbf{s}(\mathbf{x}_i; i) - \mathbf{s}(\mathbf{x}_j; j)\big\|. \qquad (6)$$

Alternatively, if the host signal is known at the decoder, as is the case in some applications of interest, then the relevant minimum distance may be more appropriately defined as either

$$d_{\min}(\mathbf{x}) \stackrel{\Delta}{=} \min_{(i,j):i\neq j} \big\|\mathbf{s}(\mathbf{x}; i) - \mathbf{s}(\mathbf{x}; j)\big\|, \qquad (7)$$

or

$$d_{\min} \stackrel{\Delta}{=} \min_{\mathbf{x}} \min_{(i,j):i\neq j} \big\|\mathbf{s}(\mathbf{x}; i) - \mathbf{s}(\mathbf{x}; j)\big\|. \qquad (8)$$

The important distinction between the definition of (6) and the definitions of (7) and (8) is that in the case of (7) and (8) the decoder knows x and, thus, needs to decide only among the reconstruction points of the various quantizers in the ensemble corresponding to the particular value of x. In the case of (6), however, the decoder needs to choose from all reconstruction points of the quantizers.

Intuitively, the minimum distance measures the size of perturbation vectors that can be tolerated by the system. For example, in the case of the bounded perturbation channel, the energy bound of (3) implies that a

minimum distance decoder is guaranteed to not make an error as long as

$$\frac{d_{\min}^2}{4N\sigma_n^2} > 1. \tag{9}$$

In the case of an additive white Gaussian noise channel with a noise variance of σ_n^2, at high signal-to-noise ratio the minimum distance also characterizes the error probability of the minimum distance decoder [24],

$$\Pr[\hat{m} \neq m] \sim Q\left(\sqrt{\frac{d_{\min}^2}{4\sigma_n^2}}\right).$$

The minimum distance decoder to which we refer simply chooses the reconstruction point closest to the received vector, i.e.,

$$\hat{m}(\mathsf{y}) = \arg\min_{m} \min_{\mathbf{x}} \|\mathsf{y} - \mathbf{s}(\mathbf{x}; m)\|. \tag{10}$$

If, which is often the case, the quantizers $\mathbf{s}(\mathbf{x}; m)$ map $\mathbf{x}$ to the nearest reconstruction point, then (10) can be rewritten as

$$\hat{m}(\mathsf{y}) = \arg\min_{m} \|\mathsf{y} - \mathbf{s}(\mathsf{y}; m)\|. \tag{11}$$

Alternatively, if the host signal $\mathbf{x}$ is known at the decoder,

$$\hat{m}(\mathsf{y}, \mathbf{x}) = \arg\min_{m} \|\mathsf{y} - \mathbf{s}(\mathbf{x}; m)\|.$$

4.2. *Distortion-Compensated QIM*

Distortion compensation is a type of post-quantization processing that can improve the achievable rate-distortion-robustness trade-offs of QIM methods. We explain the basic principles behind distortion compensation in this section.

As explained above, increasing the minimum distance between quantizers leads to greater robustness to channel perturbations. For a fixed rate and a given quantizer ensemble, scaling all quantizers by $\alpha \leq 1$ (If a reconstruction point is at $\mathbf{q}$, it is scaled by α by moving it to $\mathbf{q}/\alpha$.) increases $d_{\min}^2$ by a factor of $1/\alpha^2$. However, the embedding-induced distortion also increases by a factor of $1/\alpha^2$. Adding back a fraction $1-\alpha$ of the quantization error to the quantization value removes, or compensates for, this additional distortion. The resulting embedding function is

$$\mathbf{s}(\mathsf{x}, m) = \mathbf{q}(\mathsf{x}; m, \Delta/\alpha) + (1-\alpha)[\mathsf{x} - \mathbf{q}(\mathsf{x}; m, \Delta/\alpha)], \tag{12}$$

where $\mathbf{q}(\mathsf{x}; m, \Delta/\alpha)$ is the m-th quantizer of an ensemble whose reconstruction points have been scaled by α so that two reconstruction points separated by a distance Δ before scaling are separated by a distance Δ/α after scaling. The first term in (12) represents normal QIM embedding. We refer to the second term as the distortion-compensation term.

Typically, the probability density functions of the quantization error for all quantizers in the QIM ensemble are similar. In these cases, the distortion compensation term in (12) is statistically independent or nearly statistically independent of m and can be treated as noise during decoding. Thus, decreasing α leads to greater minimum distance, but for a fixed embedding-induced distortion, the distortion-compensation interference at the decoder increases. One optimality criterion for choosing α is to maximize a "signal-to-noise ratio" at the decision device,

$$\mathrm{SNR}(\alpha) = \frac{d_1^2/\alpha^2}{(1-\alpha)^2\frac{D_{\mathbf{s}}}{\alpha^2} + \sigma_n^2} = \frac{d_1^2}{(1-\alpha)^2 D_{\mathbf{s}} + \alpha^2\sigma_n^2},$$

where this SNR is defined as the ratio between the squared minimum distance between quantizers and the total interference energy from both distortion-compensation interference and channel interference. Here, d_1 is the minimum distance when $\alpha = 1$ and is a characteristic of the particular quantizer ensemble. The optimal scaling parameter α that maximizes this SNR is

$$\alpha_{\mathrm{opt}} = \frac{\mathrm{DNR}}{\mathrm{DNR}+1}, \tag{13}$$

where DNR is the (embedding-induced) distortion-to-noise ratio $D_{\mathbf{s}}/\sigma_n^2$. Such a choice of α also maximizes the information-embedding capacity when the channel is an additive Gaussian noise channel and the host signal x is Gaussian, as discussed in Section 5.3.

4.3. *Low-Complexity Realizations*

As mentioned in Section 4.1, design of QIM embedding systems involves constructing quantizer ensembles

whose reconstruction points also form a good signal constellation. In this section, we discuss several realizations of such ensembles that involve low-complexity embedding functions and decoders. Post-quantization distortion compensation may be combined with each of these realizations.

These realizations, which are called dither modulation, revolve around so-called dithered quantizers [25, 26], which have the property that the quantization cells and reconstruction points of any given quantizer in the ensemble are shifted versions of the quantization cells and reconstruction points of any other quantizer in the ensemble. In non-watermarking contexts, the shifts typically correspond to pseudorandom vectors called dither vectors. In dither modulation, the dither vector is instead modulated with the embedded signal, i.e., each possible embedded signal maps uniquely onto a different dither vector $\mathbf{d}(m)$. The host signal is quantized with the resulting dithered quantizer to form the composite signal. Specifically, we start with some base quantizer $\mathbf{q}(\cdot)$, and the embedding function is

$$\mathbf{s}(\mathsf{x}; m) = \mathbf{q}(\mathsf{x} + \mathbf{d}(m)) - \mathbf{d}(m).$$

4.3.1. Basic Dither Modulation Realization. Coded binary dither modulation with uniform, scalar quantization is a low-complexity realization of such a dither modulation system. (By scalar quantization, we mean that the high dimensional base quantizer $\mathbf{q}(\cdot)$ is the Cartesian product of scalar quantizers.) We assume that $1/N \leq R_m \leq 1$. The dither vectors in a coded binary dither modulation system are constructed in the following way:

- The NR_m information bits $\{b_1, b_2, \ldots, b_{NR_m}\}$ representing the embedded message m are error correction coded using a rate-k_u/k_c code to obtain a coded bit sequence $\{z_1, z_2, \ldots, z_{N/L}\}$, where

$$L = \frac{1}{R_m}(k_u/k_c).$$

  (In the uncoded case, $z_i = b_i$ and $k_u/k_c = 1$.) We divide the host signal x into N/L nonoverlapping blocks of length L and embed the i-th coded bit z_i in the i-th block, as described below.
- Two length-L dither sequences $d[k, 0]$ and $d[k, 1]$ and one length-L sequence of uniform, scalar quantizers with step sizes $\Delta_1, \ldots, \Delta_L$ are constructed with the constraint

$$d[k, 1] = \begin{cases} d[k, 0] + \Delta_k/2, & d[k, 0] < 0 \\ d[k, 0] - \Delta_k/2, & d[k, 0] \geq 0 \end{cases}, \quad k = 1, \ldots, L,$$

  This constraint ensures that the two corresponding L-dimensional dithered quantizers are the maximum possible distance from each other. For example, a pseudorandom sequence of $\pm\Delta_k/4$ and its negative satisfy this constraint. One could alternatively choose $d[k, 0]$ pseudorandomly with a uniform distribution over $[-\Delta_k/2, \Delta_k/2]$.[4] Also, the two dither sequences need not be the same for each length-L block.
- The i-th block of x is quantized with the dithered quantizer using the dither sequence $d[k, z_i]$.

A block diagram of this embedding process is shown in Fig. 6, where we use the sequence notation $x[k]$ to denote the k-th element of the host signal vector x. The actual embedding of the coded bits z_i requires only two adders and a uniform, scalar quantizer.

A block diagram of one implementation of the corresponding minimum distance decoder (11) is shown in Fig. 7. One can easily find the nearest reconstruction sequence of each quantizer (the 0-quantizer and the 1-quantizer) to the received sequence $y[k]$ using a few adders and scalar quantizers. For hard-decision forward error correction (FEC) decoding, one can make

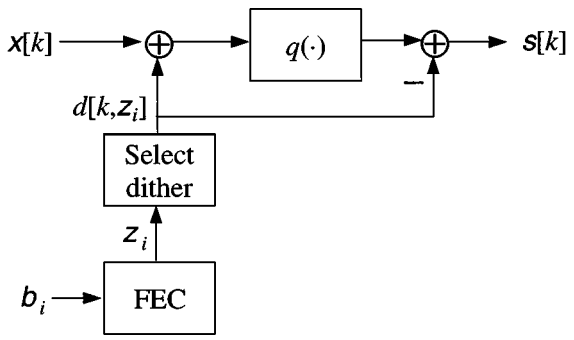


Figure 6. Embedder for coded binary dither modulation with uniform, scalar quantization. The only required computation beyond that of the forward error correction (FEC) code is one addition, one scalar quantization, and one subtraction per host signal sample.

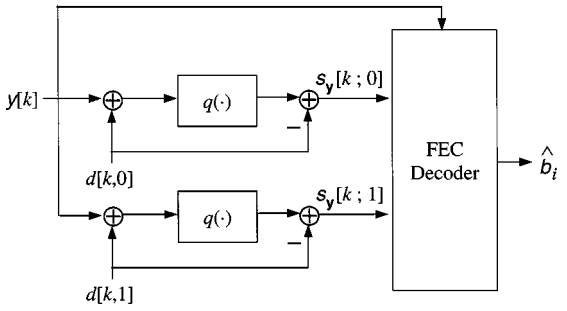


Figure 7. Decoder for coded binary dither modulation with uniform, scalar quantization. The distances between the received sequence $y[k]$ and the nearest quantizer reconstruction sequences $s_y[k;0]$ and $s_y[k;1]$ from each quantizer are used for either soft-decision or hard-decision forward error correction (FEC) decoding.

decisions on each coded bit z_i using the rule:

$$\hat{z}_i = \arg\min_{l\in\{0,1\}} \sum_{k=(i-1)L+1}^{iL} (y[k] - s_y[k;l])^2, \qquad i = 1, \ldots, N/L.$$

Then, the FEC decoder can generate the decoded information bit sequence $\{\hat{b}_1, \ldots, \hat{b}_{NR_m}\}$ from the estimates of the coded bits $\{\hat{z}_1, \ldots, \hat{z}_{N/L}\}$. Alternatively, one can use the metrics

$$\text{metric}(i,l) = \sum_{k=(i-1)L+1}^{iL} (y[k] - s_y[k;l])^2, \qquad i = 1, \ldots, N/L.$$

for soft-decision decoding. For example, one can use these metrics as branch metrics for a minimum squared Euclidean distance Viterbi decoder [24], as is done for the convolutional code simulations of Section 6.1.

4.3.2. Spread-Transform Dither Modulation. Spread-transform dither modulation (STDM) is a special case of coded binary dither modulation in which only projections of the host signal along certain (usually pseudorandomly chosen) orthogonal vectors v_i are quantized. In the case where each of the N/L coded bits z_i are embedded in a different projection $\tilde{x}_i$, one can replace the original host signal samples $x[k]$ in Fig. 6 with the projections $\{\tilde{x}_1, \ldots, \tilde{x}_{N/L}\}$ to generate the composite signal projections $\{\tilde{s}_1, \ldots, \tilde{s}_{N/L}\}$. These composite signal projections are combined with the non-quantized components of the host signal (the components of the host signal orthogonal to the space spanned by $\{v_1, \ldots, v_{N/L}\}$) to generate the overall composite signal. Quantizing only a subset of host signal components instead of all host signal components has some important performance advantages, as discussed in Section 6.2. (See also [7, 11] for additional perspectives.)

4.3.3. Amplitude-Scaling Invariant Dither Modulation. One can view the projection operations of STDM as a type of preprocessing of the host signal, or equivalently, as choosing an alternative representation of the host signal. (In the problem models of Section 2, the host signal can be any collection of real numbers, and need not be time, spatial, nor frequency domain samples.) In some applications one may wish to choose a host signal representation that is invariant or insensitive to amplitude scalings introduced by the channel. For example, in the FM digital audio broadcasting application discussed in Section 1, one may wish to embed information only in the phase of the host analog FM signal so that the receiver will not need to estimate changes in amplitude due to multipath fading. In this case, one can replace the host signal samples $x[k]$ in Fig. 6 with phase samples (or differences in phase from one sample to the next, if the receiver is not capable of recovering absolute phase).

Analog FM signals have constant amplitude, and thus, an example of a resulting signal constellation and/or ensemble of quantizer reconstruction points is shown in Fig. 8. The coded bit z_i that is to be embedded in $x[k]$ determines which subset of constellation points, the $\times$-subset or the $\circ$-subset, is used. The host signal value $x[k]$ determines which point within the subset is chosen as the composite signal value $s[k]$. If the error correction code that produces z_i is a convolutional code, then this information-embedding strategy is very similar to classical trellis coded modulation [27], treating the "uncoded bits", the bits that determine which point within the subset is chosen, as being determined by the quantization of the host signal $x[k]$. One difference, however, is that these uncoded bits are a function of both $x[k]$ and the coded bit z_i since the quantization intervals of the $\times$ and $\circ$ quantizers are different, i.e., because the quantization intervals for the two quantizers are different, the method is not a LBM method. As a result, the method is similar, but not equivalent, to trellis coded modulation treating z_i as coded bits and using (only) $x[k]$ to determine the uncoded bits.

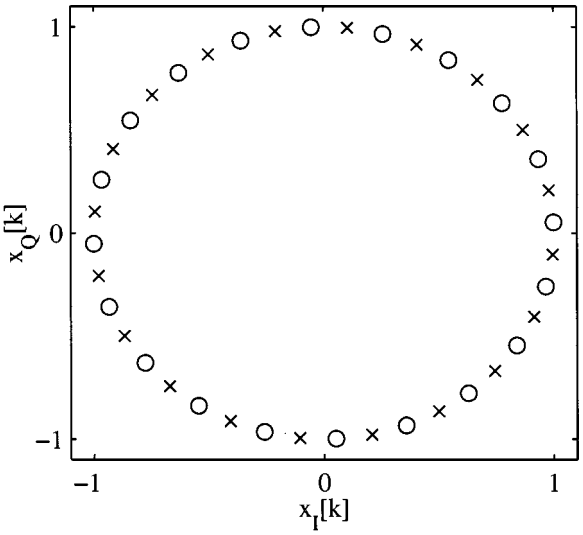


Figure 8. Signal constellation and quantizer reconstruction points for phase quantization and dither modulation of analog FM signals. $x_I[k]$ and $x_Q[k]$ are the in-phase and quadrature signal components, respectively. The quantizer step size Δ is $\pi/10$. The $\times$-quantizer dither value is $\Delta/3$. The $\circ$-quantizer dither value is $-\Delta/6$.

4.4. SNR Analysis

The host signal interference rejection properties of QIM embedding methods, and by extension dither modulation realizations, lead to a number of significant performance advantages over host-interference non-rejecting methods. One can illustrate many of these perhaps most easily by exploiting the close coupling between STDM and a class of spread spectrum methods that we term amplitude-modulation spread spectrum (AM-SS). AM spread spectrum methods have embedding functions of the form

$$\mathbf{s}_{\text{AM-SS}}(\mathsf{x}, m) = \mathsf{x} + a(m)\mathsf{v},$$

and examples of methods within this class can be found in [12, 15]. Here, v is a pseudo-random vector that plays the same role as the STDM projection vectors in Section 4.3.2.

We consider embedding one bit in a length-L block $\mathbf{x}$ using STDM and AM-SS methods with the same spreading vector $\mathbf{v}$, which is of unit length. Because the embedding occurs entirely in the projections of x onto $\mathbf{v}$, the problem is reduced to a one-dimensional problem with the AM-SS embedding function being

$$\tilde{s} = \tilde{x} + a(m)$$

and the STDM embedding function being

$$\tilde{s} = q(\tilde{x} + d(m)) - d(m).$$

For AM-SS, $a(m) = \pm\sqrt{LD_{\mathbf{s}}}$ so that

$$|a(1) - a(2)|^2 = 4LD_{\mathbf{s}}, \tag{14}$$

while for STDM

$$|d(1) - d(2)|^2 = \Delta^2/4 = 3LD_{\mathbf{s}}, \tag{15}$$

where $\Delta = \sqrt{12LD_{\mathbf{s}}}$ so that the expected distortion in both cases is the same. Also, because all of the embedding-induced distortion occurs only in the direction of $\mathbf{v}$, the distortion in both cases also has the same time or spatial distribution and frequency distribution. Thus, one would expect that any perceptual effects due to time/space masking or frequency masking are the same in both cases. Therefore, mean-square distortion may be a more meaningful measure of distortion when comparing STDM with AM-SS than one might expect in other more general contexts where mean-square distortion may fail to capture certain perceptual effects.

The decoder in both cases makes a decision based on $\tilde{y}$, the projection of the channel output $\mathbf{y}$ onto $\mathbf{v}$. In the case of AM-SS,

$$\tilde{y} = a(m) + \tilde{x} + \tilde{n},$$

while in the case of STDM,

$$\tilde{y} = \tilde{s}(\tilde{x}, d(m)) + \tilde{n},$$

where $\tilde{n}$ is the projection of the perturbation vector n onto $\mathbf{v}$. We let $P(\cdot)$ be some measure of energy. For example, $P(x) = x^2$ in the case of a deterministic variable x, or $P(x)$ equals the variance of the random variable x. The energy of the interference or "noise" is $P(\tilde{x} + \tilde{n})$ for AM-SS, but only $P(\tilde{n})$ for STDM, i.e., the host signal interference for STDM is zero. Thus, the signal-to-noise ratio at the decision device is

$$\text{SNR}_{\text{AM-SS}} = \frac{4LD_{\mathbf{s}}}{P(\tilde{x} + \tilde{n})}$$

for AM-SS and

$$\text{SNR}_{\text{STDM}} = \frac{3LD_{\mathbf{s}}}{P(\tilde{n})},$$

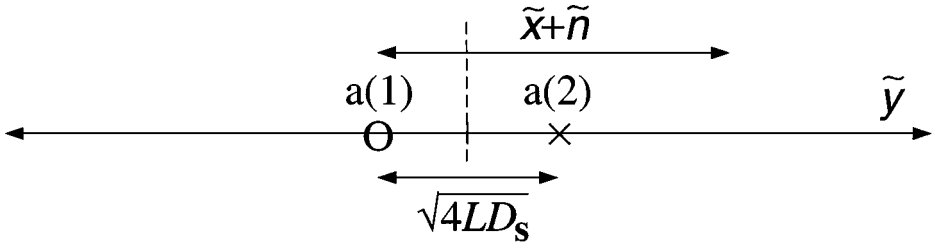


Figure 9. Decoder decision regions for amplitude-modulation spread spectrum. Both host ($\tilde{x}$) and channel perturbation ($\tilde{n}$) are interference sources.

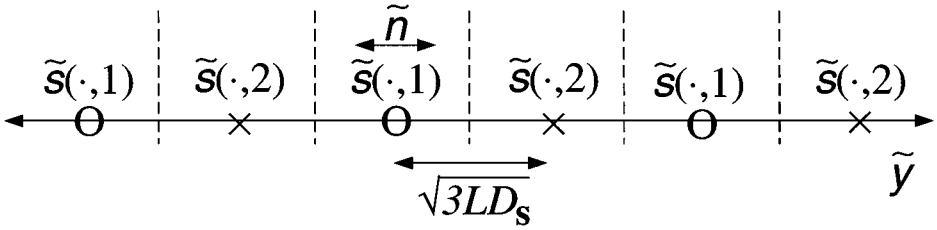


Figure 10. Decoder decision regions for spread-transform dither modulation. Only the channel perturbation ($\tilde{n}$), and not the host ($\tilde{x}$), is an interference source.

where the "signal" energies $P(a(1)-a(2))$ and $P(d(1)-d(2))$ are given by (14) and (15). The decision regions of the decision devices are shown in Figs. 9 and 10 for AM-SS and STDM, respectively. Thus, the advantage of STDM over AM-SS is

$$\frac{\text{SNR}_{\text{STDM}}}{\text{SNR}_{\text{AM-SS}}} = \frac{3}{4}\frac{P(\tilde{x}+\tilde{n})}{P(\tilde{x})}, \tag{16}$$

which is typically very large since the channel perturbations $\tilde{n}$ are usually much smaller than the host signal $\tilde{x}$ if the channel output $\tilde{y}$ is to be of reasonable quality. For example, if the host signal-to-channel noise ratio is 30 dB and $\tilde{x}$ and $\tilde{n}$ are uncorrelated, then the SNR advantage (16) of STDM over AM spread spectrum is 28.8 dB.

Furthermore, although the SNR gain in (16) is less than 0 dB ($3/4 = -1.25$ dB) when the host signal interference is zero ($\tilde{x} = 0$), for example, such as would be the case if the host signal x had very little energy in the direction of **v**, STDM may not be worse than AM-SS even in this case since (16) applies only when $\tilde{x}$ is approximately uniformly distributed across the STDM quantization cell so that $D_s = \Delta^2/(12L)$. If $\tilde{x} = 0$, however, and one chooses the dither signals to be $d(m) = \pm\Delta/4$, then the distortion is only $D_s = \Delta^2/(16L)$ so that STDM is just as good as AM-SS in this case.

We now comment on some additional insights that one can obtain from the SNR analysis in this section, particularly Figs. 9 and 10. First, we consider "requantization" attacks on STDM, where if $\tilde{s}$ is a $\times$ point in Fig. 10, then the attacker quantizes the signal to a $\circ$ point, for example. From Fig. 10, we see that this attack is an additive noise attack where $P(\tilde{n}) = 3LD_s$. (The noise value is $\pm\sqrt{3LD_s}$.) The attack is suboptimal since the resulting perturbation is actually twice as long as it needs to be to cause an error. Also, the attacker requires knowledge of the projection vector **v**. If the attacker knows this projection vector, he or she can equivalently attack the AM-SS system illustrated in Fig. 9 by adding a perturbation with the same energy. Again, in addition to this perturbation, the host signal will add to the total interference at the AM-SS decision device and the resulting SNR advantage of STDM over AM-SS is given by (16).

As a final example of an insight that one can gleam from Figs. 9 and 10, we observe a threshold effect in both cases. If the interference at the decoder is smaller than some threshold, then the systems successfully decode the message. However, if the interference is larger than the threshold, then the systems fail. This property is inherent to digital communication systems, in general. One solution, of course, is to choose the rate low enough (choose L high enough) so that the worst case interference, either $\tilde{x}+\tilde{n}$ or $\tilde{n}$ for AM-SS and STDM,

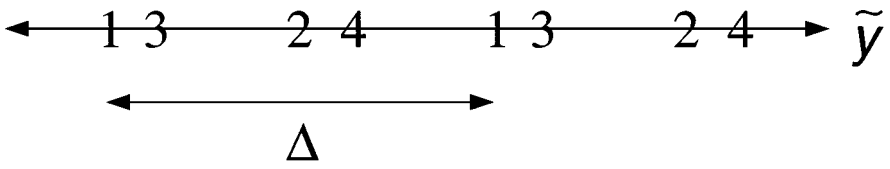


Figure 11. Broadcast or multirate digital watermarking with spread-transform dither modulation. In high-noise scenarios the decoder determines if m is even or odd to extract one bit. In low-noise scenarios the decoder determines the precise value of m to extract two bits and, hence, double the rate.

respectively, is below the failure threshold. However, if the interference turns out to be smaller than the worst case amount, then one might desire that the decoder have the capability to extract more than this minimum rate of embedded information. To accommodate such "graceful degradation" (or "graceful improvement", depending on one's perspective) in rate, one can replace the $\times$ and $\circ$ points in Figs. 9 and 10 with "clouds" of points, as described in [28, 29] for broadcast communication in non-watermarking contexts.

An example of such a "broadcast" or multirate STDM quantizer ensemble for digital watermarking is shown in Fig. 11. The reconstruction points of four quantizers are labeled 1, 2, 3, and 4, respectively. The minimum distance between an even and an odd point is larger than the minimum distance between any two points and is set large enough such that the decoder can determine if an even or an odd quantizer was used, and hence extract one bit, even under worst-case channel noise conditions. However, if the channel noise is smaller, then the decoder can determine the precise quantizer used, and hence, extract two bits. Of course, one could use a similar broadcast method for AM-SS, but in the AM-SS case one would encounter host-interference as well as channel noise. Thus, STDM has an SNR advantage over AM-SS in the case of uncertain channel noise levels as well as in the case of a known, single channel noise level.

4.5. Other Performance Properties

As discussed in Section 2, the bounded perturbation channel and bounded host-distortion channel are two models that may be appropriate when facing the worst-case active distortion-constrained attacks.[5] In the case of the bounded perturbation channel, it can be shown [7, 11] that the error-free decoding condition (9) implies that coded binary dither modulation with uniform scalar quantization can achieve the following rate-distortion-robustness trade-offs:

$$R_m < \gamma_c \frac{3}{4} \frac{D_{\mathbf{s}}}{N\sigma_n^2}, \tag{17}$$

where γ_c is the error correction coding gain (the product of the Hamming distance and rate of the error correction code). This expression gives an achievable set of embedding rates for a given expected distortion $D_{\mathbf{s}}$ and channel perturbation energy per dimension σ_n^2 when one wishes to deterministically guarantee error-free decoding with finite length signals. Thus, one can view (17) as a deterministic counterpart to the conventional, information-theoretic notion of the capacity [30] of a random channel. Spread spectrum methods in contrast offer no such guaranteed robustness to bounded perturbation attacks, and the achievable rate-distortion-robustness trade-offs of coded LBM with uniform scalar quantization are 2.43 dB worse than those of (17) [7, 11]. For bounded host-distortion channels, it can be shown [7, 11] that an in-the-clear attacker, one who knows everything about the embedding and decoding processes including any keys, can remove spread spectrum and LBM embedded watermarks and improve the signal quality ($D_{\mathbf{y}} \leq D_{\mathbf{s}}$) at the same time. In contrast, to remove a watermark embedded with QIM methods (including coded binary dither modulation with uniform scalar quantization), the in-the-clear attacker's distortion $D_{\mathbf{y}}$ must be greater than the embedding-induced distortion $D_{\mathbf{s}}$.

A number of capacity results are also developed in [11] for the case of AWGN channels and white, Gaussian host signals. For example, results in [31] are applied to show that the information-embedding capacity, the maximum achievable embedding rate R_m for a given expected distortion $D_{\mathbf{s}}$ and noise variance σ_n^2, is

$$C_{\text{AWGN}} = \frac{1}{2}\log_2(1 + \text{DNR}), \tag{18}$$

where, again, DNR is the distortion-to-noise ratio $D_{\mathbf{s}}/\sigma_n^2$. Remarkably, the capacity is the same as the

case when the host signal is known at the decoder, implying that an infinite energy host signal causes no decrease in capacity in this Gaussian case. (Moulin and O'Sullivan [32] have extended this result to the case of intentional square-error distortion-constrained attacks, where the optimal attacks turns out to be multiplication by a constant followed by addition of Gaussian noise.) QIM methods exist that achieve performance within 4.3 dB of capacity, i.e., they achieve the same rate (18) with at most 4.3 dB additional DNR. Furthermore, the QIM gap to capacity goes to 0 dB asymptotically at high rates, and the gap to capacity of distortion-compensated QIM is 0 dB at any rate, i.e., no embedding method exists that can achieve better performance than the best possible distortion-compensated QIM method. The low-complexity, binary dither modulation with uniform scalar quantization methods described in Section 4.3 can achieve performance within 13.6 dB of capacity even with *no error correction coding* and no distortion compensation. In contrast, the gap to capacity of *coded spread* spectrum is $1+\mathrm{SNR}_x$, where SNR_x is the ratio between the host signal variance σ_x^2 and the noise variance σ_n^2. Again, SNR_x is typically quite large since the channel is not supposed to degrade the host signal too much. Thus, even with very high-complexity error correction codes, the gap between a spread spectrum system and capacity is typically very large.

5. General Gaussian Capacities

In this section, we develop capacity results for the more general Gaussian case, where both the host signal and channel noise are colored. Thus, these results apply to a wider variety of channel degradations than the results cited above for the case of white host signals and white channel noise. We also discuss the implications for some multimedia applications.

We consider the super-channel model of Fig. 2 with the further assumptions that x and n are statistically independent and can be decomposed into

$$\mathsf{x} = [x_1 \cdots x_{N/L}]^T \quad \text{and} \quad \mathsf{n} = [n_1 \cdots n_{N/L}]^T,$$

where the x_i are independent and identically distributed (iid), L-dimensional, zero-mean, Gaussian vectors with covariance matrix K_x and the n_i are iid, L-dimensional, zero-mean, Gaussian vectors with covariance matrix K_n. This model is appropriate when the channel is an additive (colored) Gaussian noise channel, the host signal is colored and Gaussian, but the power spectra of the host signal and channel noise are sufficiently smooth that one can decompose the channel into L parallel, narrowband subchannels, over each of which the host signal and channel noise power spectra are approximately flat. Many hybrid transmission applications are examples of such a scenario, and this model may also apply to optimal, i.e., rate-distortion achieving [30], lossy compression of a Gaussian source. As discussed in [7, 11], the super-channel model of information-embedding allows one to use earlier results on the capacity of channels with random states [33] to show that the information-embedding capacity is

$$C = \max_{p_{u,e|x}(u,e|x)} I(u; y) - I(u; x), \tag{19}$$

where $I(\cdot;\cdot)$ denotes mutual information [30], u is an auxiliary random variable, and the maximization is subject to a distortion constraint, or equivalently an energy constraint on e.

Below, we first determine the capacity when the host signal is colored, but the channel noise is white. Then, we use this result to determine capacities when both the host signal and channel noise are colored. Finally, we give examples of how one might apply these results to several multimedia hybrid transmission applications.

5.1. Colored Host, White Noise

We consider the case where the host signal is colored with covariance matrix $K_x = Q_x \Lambda_x Q_x^T$, where the columns of the orthogonal matrix Q_x are the eigenvectors of K_x and Λ_x is a diagonal matrix of the corresponding eigenvalues, and the channel noise is white with covariance matrix $K_n = \sigma_n^2 I$. The distortion constraint is

$$\frac{L}{N} \sum_{i=1}^{N/L} e_i^T e_i \le L D_{\mathbf{s}}, \tag{20}$$

and the corresponding constraint on $p_{u,e|x}(u, e|x)$ in (19) is $E[e^T e] \le L D_{\mathbf{s}}$. Thus, $L D_{\mathbf{s}}$ is the maximum average energy of the L-dimensional vectors e_i, so $D_{\mathbf{s}}$ is still the maximum average energy per dimension.

One way to determine the capacity in this case is to consider embedding in a linear transform domain, where the covariance matrix of the host signal is diagonal. Because the transform is linear, the transformed

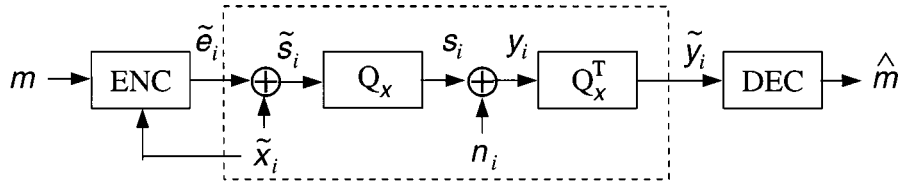


Figure 12. Embedding in transform domain for colored host signal and white noise. The dashed box is the equivalent transform-domain channel.

host signal vector remains Gaussian. One such orthogonal transform is the well-known Karhunen-Loeve transform [34], and the resulting transformed host signal vector is

$$\tilde{x} = Q_x^T x,$$

with covariance matrix $K_{\tilde{x}} = \Lambda_x$. The distortion constraint (20) in the transform domain on the vectors $\tilde{e} = Q_x^T e$ is

$$\frac{L}{N} \sum_{i=1}^{N/L} \tilde{e}_i^T \tilde{e}_i \leq LD_{\mathbf{s}},$$

since

$$\tilde{e}_i^T \tilde{e}_i = e_i^T Q_x Q_x^T e_i = e_i^T e_i.$$

An overall block diagram of the transformed problem is shown in Fig. 12. The transform-domain channel output $\tilde{y}$ is

$$\tilde{y} = \tilde{e} + \tilde{x} + \tilde{n},$$

where the transform-domain noise $\tilde{n}$ has the same covariance matrix as n,

$$K_{\tilde{n}} = Q_x^T (\sigma_n^2 I) Q_x = \sigma_n^2 I = K_n.$$

Since both $K_{\tilde{x}}$ and $K_{\tilde{n}}$ are diagonal, in the transform domain we have L parallel, *independent* subchannels, each of which is an AWGN channel with noise variance σ_n^2 and each of which has a white, Gaussian host signal. Thus, as we show formally in App. A, the overall capacity is simply the sum of the capacities of the individual subchannels (18),

$$\begin{aligned} C_L &= \sum_{i=1}^{L} \frac{1}{2} \log_2(1 + \mathrm{DNR}) \\ &= \frac{L}{2} \log_2(1 + \mathrm{DNR}). \end{aligned} \tag{21}$$

This capacity is in bits per L-dimensional host signal vector, so the capacity in bits per dimension is

$$C = \frac{1}{2} \log_2(1 + \mathrm{DNR}), \tag{22}$$

the same as the capacity when the host signal is white (18). Thus, not only is the capacity independent of the host signal power for white Gaussian host signals as discussed above in Section 4.5, but in the more general Gaussian case where the host signal has any arbitrary covariance matrix, the capacity is independent of *all* host signal statistics. (The statistics of a Gaussian random vector are completely characterized by its mean and covariance.)

5.2. Colored Host, Colored Noise

We now extend our results to the case where both the host signal and the noise are colored. The host signal covariance matrix is the same as above, $K_x = Q_x \Lambda_x Q_x^T$. However, the noise covariance matrix takes the form $K_n = Q_n \Lambda_n Q_n^T$, where Q_n is an orthogonal matrix of the eigenvectors of K_n and Λ_n is a diagonal matrix of its eigenvalues, all of which are assumed to be non-zero, i.e., we assume K_n is invertible.

Because the channel noise is not white, issues arise as to how to measure distortion and how to define distortion-to-noise ratio. One may want to make the embedding-induced distortion "look like" the channel noise so that as long as the channel noise does not cause too much perceptible degradation to the host signal, then neither does the embedding-induced distortion. One can impose this condition by choosing distortion measures that favor relatively less embedding-induced distortion in components where the channel noise is relatively small and allow relatively more distortion in components where the channel noise is relatively large. Then, the embedding-induced distortion will look like a scaled version of the channel noise, with the DNR as the scaling factor. If the DNR is chosen small enough,

then the embedding-induced distortion will be "hidden in the noise".

Below, we consider two such ways to measure distortion and DNR and show that in each case when we impose this constraint that the embedding-induced distortion signal look like a scaled version of the channel noise, the information-embedding capacity is independent of the host and noise statistics and depends only on the DNR. In the first case, we constrain the weighted average square-error distortion, more heavily weighting or penalizing distortion in components where the channel noise is small. In the second case, we use separate, simultaneous distortion constraints on each of the components, allowing more distortion where the channel noise is large and less distortion where the channel noise is small.

5.2.1. Weighted Square-Error Distortion. One natural distortion measure and constraint is

$$\frac{L}{N}\sum_{i=1}^{N/L} e_i^T K_n^{-1} e_i \le L\,\mathrm{DNR}, \tag{23}$$

so that the corresponding constraint on $P_{u,e|x}(u, e \mid x)$ in (19) is $E[e^T K_n^{-1} e] \le L\,\mathrm{DNR}$. As desired, the weighting matrix K_n^{-1} more heavily penalizes distortion in the directions of eigenvectors corresponding to small eigenvalues (noise variances). Thus, the embedding-induced distortion will tend to be large only in those components where the channel noise is also large, and the distortion will tend to be small in the components where the channel noise is also small. As we show below, this case is equivalent to the colored host and white noise case discussed in the last section, and therefore, the capacity is also given by (22). This equivalence will be made apparent through an invertible, linear transform.

The transform required in this case not only diagonalizes the noise covariance matrix, but also makes the transformed noise samples equivariant. Specifically, the transform matrix is $\Lambda_n^{-1/2} Q_n^T$, and the transformed host signal vector

$$\tilde{x} = \Lambda_n^{-1/2} Q_n^T x$$

has covariance matrix

$$K_{\tilde{x}} = \Lambda_n^{-1/2} Q_n^T K_x Q_n \Lambda_n^{-1/2}.$$

A block diagram for the overall problem is similar to the one in Fig. 12, with the transform matrix Q_x^T replaced by $\Lambda_n^{-1/2} Q_n^T$ and the inverse transform matrix Q_x replaced by $Q_n \Lambda_n^{1/2}$. Because the transform is invertible, there is no loss of optimality from embedding in this transform domain. The transform-domain channel output $\tilde{y}$ is

$$\tilde{y} = \tilde{e} + \tilde{x} + \tilde{n},$$

where the transform-domain noise $\tilde{n}$ has covariance matrix

$$K_{\tilde{n}} = \Lambda_n^{-1/2} Q_n^T \big(Q_n \Lambda_n Q_n^T\big) Q_n \Lambda_n^{-1/2} = I. \tag{24}$$

Thus, the components of $\tilde{n}$ are uncorrelated (and independent since $\tilde{n}$ is Gaussian) and have unit variance.

The distortion constraint (23) in the transform domain is

$$\frac{L}{N}\sum_{i=1}^{N/L} \tilde{e}_i^T \tilde{e}_i^T \le L\,\mathrm{DNR}$$

since

$$\begin{aligned} e_i^T K_n^{-1} e_i &= e_i^T \big(Q_n \Lambda_n^{-1} Q_n^T\big) e_i \\ &= \big(e_i^T Q_n \Lambda_n^{-1/2}\big)\big(\Lambda_n^{-1/2} Q_n^T e_i\big) \\ &= \tilde{e}_i^T \tilde{e}_i. \end{aligned}$$

Thus, the transform domain distortion constraint in this case is the same as the non-transform domain distortion constraint (20) of the last section. In both cases the host signal is colored and Gaussian, and the channel noise is white and Gaussian. Thus, the capacity in both cases is the same (22),

$$C = \frac{1}{2}\log_2(1 + \mathrm{DNR}), \tag{25}$$

and was determined in the last section.

5.2.2. Multiple, Simultaneous Square-Error Distortion. An alternative, and more restrictive, distortion constraint to (23) arises by strictly requiring that the embedding-induced distortion in components corresponding to small noise eigenvalues be small rather than simply weighting these distortions more heavily. Specifically, we consider the set of constraints

$$\frac{L}{N}\sum_{i=1}^{N/L} \big(q_j^T e_i\big)^2 \le \mathrm{DNR}\,\lambda_j, \quad j = 1, \ldots, L, \tag{26}$$

where q_j and λ_j are the j-th eigenvector and eigenvalue, respectively, of K_n. Any distortion signal that satisfies (26) also satisfies (23) since

$$\begin{aligned}\frac{L}{N}\sum_{i=1}^{N/L} e_i^T K_n^{-1} e_i &= \frac{L}{N}\sum_{i=1}^{N/L} \left(Q_n^T e_i\right)^T \Lambda_n^{-1}\left(Q_n^T e_i\right) \\ &= \frac{L}{N}\sum_{i=1}^{N/L}\sum_{j=1}^{L} \left(q_j^T e_i\right)^2 \frac{1}{\lambda_j} \\ &= \sum_{j=1}^{L}\left[\frac{L}{N\lambda_j}\sum_{i=1}^{N/L}\left(q_j^T e_i\right)^2\right] \\ &\le L\,\mathrm{DNR},\end{aligned}$$

where the first line follows from the factorization $K_n^{-1} = Q_n\Lambda_n^{-1}Q_n^T$ and where the final line follows from (26). Thus, the constraint (26) is indeed more restrictive than (23).

To determine the information-embedding capacity in this case, we again consider the noise-whitening linear transform $\Lambda_n^{-1/2}Q_n^T$. The j-th component of the transform-domain distortion vector $\tilde{e}_i = \Lambda_n^{-1/2}Q_n^T e_i$ is

$$[\tilde{e}_i]_j = \frac{1}{\sqrt{\lambda_j}} q_j^T e_i.$$

Thus, the transform-domain distortion constraint equivalent to (26) is

$$\frac{L}{N}\sum_{i=1}^{N/L}[\tilde{e}_i]_j^2 \le \mathrm{DNR}, \quad j = 1, \ldots, L. \tag{27}$$

By (24), the transform-domain noise covariance matrix is the identity matrix. Thus, if we treat each of the L subchannels independently, each with its own distortion constraint (27) and a noise variance of unity, then on the j-th subchannel we can achieve a rate

$$C_j = \frac{1}{2}\log_2(1 + \mathrm{DNR}),$$

so the total rate across all L channels in bits per dimension is

$$C = \frac{1}{L}\sum_{j=1}^{L} C_j = \frac{1}{2}\log_2(1 + \mathrm{DNR}). \tag{28}$$

Since this rate equals the capacity (25) corresponding to a less restrictive distortion constraint (23), we cannot hope to achieve a rate higher than this one. Thus, treating the L subchannels independently does not result in any loss of optimality, and the achievable rate (28) is indeed the capacity.

Thus, for Gaussian host signals and additive Gaussian noise channels, with the constraint that the embedding-induced distortion signal "look like" the channel noise, the information-embedding capacity is independent of the host and noise covariance matrices (Since the signals are Gaussian, the capacity is actually independent of all host signal and noise statistics.) and is given by (18), (22), (25), and (28).

5.3. Capacities for Multimedia Host Signals

The capacity expressions in Section 5.1 and Section 5.2 apply to arbitrary host and noise covariance matrices and, thus, these achievable rate-distortion-robustness expressions are quite relevant to many of the multimedia applications mentioned in Section 1, especially those where one faces incidental channel degradations. For example, these capacities do not depend on the power spectrum of the host signal and thus these results apply to audio, video, image, speech, analog FM, analog AM, NTSC television, and coded digital signals, to the extent that these signals can be modeled as Gaussian. Also, the additive Gaussian noise with arbitrary covariance model may be applicable to lossy compression, printing and scanning noise, thermal noise, adjacent channel and co-channel interference (which may be encountered in DAB applications, for example), and residual noise after appropriate equalization of intersymbol interference channels or slowly varying fading channels. Furthermore, when considering the amount of embedding-induced distortion, in many applications one is most concerned with the quality of the *received* host signal, i.e., the channel output, rather than the quality of the composite signal. For example, in FM digital audio broadcasting applications, conventional receivers demodulate the host analog FM signal from the channel output, not from the composite signal, which is available only at the transmitter. Similarly, in many authentication applications, the document carrying the authentication signal may be transmitted across some channel to the intended user. In these cases one can use the capacity expressions of the last section to conveniently determine the achievable embedded rate per unit of host signal bandwidth and per unit of received host signal degradation, as we show in this section.

In each of the cases considered in Section 5.1 and Section 5.2, the measure of distortion, and hence the DNR, is defined to make the embedding-induced

distortion signal "look like" the channel noise, the idea being that if channel noise distortion to the host signal is perceptually acceptable, then an embedding-induced distortion signal of the same power spectrum will also be perceptually acceptable. As discussed in those sections, one can view the DNR as the amount by which one would have to amplify the noise to create a noise signal with the same statistics as the embedding-induced distortion signal. Thus, if one views the received channel output as a noise-corrupted version of the host signal, then the effect of the embedding is to create an additional noise source DNR times as strong as the channel noise, and therefore, the received signal quality drops by a factor of $(1 + \text{DNR})$ or

$$10 \log_{10}(1 + \text{DNR}) \text{ dB}. \tag{29}$$

Since the capacity in bits per dimension (bits per host signal sample) is given by (28), and there are two independent host signal samples per second for every Hertz of host signal bandwidth, the capacity in bits per second per Hertz is

$$C = \log_2(1 + \text{DNR}) \text{ b/s/Hz}. \tag{30}$$

Taking the ratio between (30) and (29), we see that the "value" in embedded rate of each dB drop in received host signal quality is

$$\begin{aligned} C &= \frac{\log_2(1 + \text{DNR})}{10 \log_{10}(1 + \text{DNR})} \\ &= \frac{1}{10} \log_2 10 \approx 0.3322 \text{ b/s/Hz/dB} \end{aligned} \tag{31}$$

Thus, the available embedded digital rate in bits per second depends only on the bandwidth of the host signal and the tolerable degradation in received host signal quality. Information-embedding capacities for several types of host signals are shown in Table 1.

Table 1. Information-embedding capacities for transmission over additive Gaussian noise channels for various types of host signals. Capacities are in terms of achievable embedded rate per dB drop in received host signal quality.

Host signal	Bandwidth	Capacity
NTSC video	6 MHz	2.0 Mb/s/dB
Analog FM	200 kHz	66.4 kb/s/dB
Analog AM	30 kHz	10.0 kb/s/dB
Audio	20 kHz	6.6 kb/s/dB
Telephone voice	3 kHz	1.0 kb/s/dB

It is shown in [11] that for white, Gaussian host signals and AWGN channels, there exist distortion-compensated QIM methods, with distortion-compensation parameter α given by (13), that can achieve capacity (18). The results of Moulin and O'Sullivan [32] imply that, in the case of arbitrary square-error distortion-constrained attacks, distortion-compensated QIM with a different value of α can achieve capacity, although Moulin and O'Sullivan do not explicitly state this observation. Their results also imply that in the case of non-Gaussian host signals, distortion-compensated QIM can achieve capacity asymptotically with small embedding-induced distortion and attacker's distortion, which is the limiting case of interest in high fidelity applications. The connection between capacity and distortion compensation in these cases is explained in more detail in App. B.

Since the colored Gaussian cases considered in this section can be transformed into a case of independent, parallel AWGN channels with white host signals, capacity-achieving distortion-compensated QIM methods also exist for these cases. Similarly, it is also shown in [7, 11] that regular QIM methods exist that achieve performance within 1.6 dB of capacity. For example, referring to Table 1, to embed 200 kb/s in a 200-kHz analog FM signal with a capacity-achieving method requires that we accept a 3-dB drop in received host signal quality. Therefore, there exists a QIM method that can achieve an embedding rate of 200 kb/s with at most a $(3 + 1.6)$-dB $= 4.6$-dB drop in received host signal quality.

6. Simulation Results

In Section 5 we established the existence of capacity-achieving and near capacity-achieving embedding and decoding methods within the distortion-compensated QIM and regular QIM classes, respectively, for Gaussian embedding problems. In Section 4.3 we presented low-complexity realizations of QIM involving dither modulation and uniform, scalar quantization. These realizations could also be combined with distortion compensation. Several simulation results for dither modulation implementations are reported below for both Gaussian and non-Gaussian channels.

6.1. Gaussian Channel

It can be shown fairly easily [7, 11] that for additive white Gaussian noise (AWGN) channels and $R_m < 1$,

the bit-error probability P_b of the *uncoded* spread-transform dither modulation (STDM) with uniform, scalar quantization method discussed in Section 4.3 is upper bounded by

$$P_b \leq 2Q\left(\sqrt{\frac{3}{4}\mathrm{DNR}_{\mathrm{norm}}}\right), \tag{32}$$

where $\mathrm{DNR}_{\mathrm{norm}}$ is the rate-normalized distortion-to-noise ratio

$$\mathrm{DNR}_{\mathrm{norm}} \stackrel{\Delta}{=} \frac{\mathrm{DNR}}{R_m} \tag{33}$$

For example, one can achieve a bit-error probability of about 10^{-6} at a $\mathrm{DNR}_{\mathrm{norm}}$ of 15 dB. Thus, no matter how noisy the AWGN channel, one can reliably embed using uncoded STDM by choosing sufficiently low rates,

$$R_m \leq \frac{\mathrm{DNR}}{\mathrm{DNR}_{\mathrm{norm}}}.$$

This case is illustrated in Fig. 13, where despite the fact that the channel has degraded the composite image by over 12 dB, all 512 embedded bits are recovered without any errors from the 512-by-512 image. The actual bit-error probability is about 10^{-6}.

One can improve performance significantly using error correction coding and distortion compensation. In fact, from the capacity expressions (18) and (22) for the case of white, Gaussian noise, we see that reliable information embedding is possible if

$$R_m \leq C = \frac{1}{2}\log_2(1 + \mathrm{DNR})$$

or, equivalently,

$$\frac{\mathrm{DNR}}{2^{2R_m} - 1} \geq 1.$$

For small R_m, $2^{2R_m} - 1 \approx 2R_m \ln 2$, so this condition becomes

$$\mathrm{DNR}_{\mathrm{norm}} \geq 2\ln 2 \approx 1.4 \text{ dB}.$$

Since, as stated above, uncoded STDM with uniform, scalar quantization requires a $\mathrm{DNR}_{\mathrm{norm}}$ of 15 dB for a bit-error probability of 10^{-6}, there is a gap to capacity of about 13.6 dB.

We now report the results of one experiment designed to investigate how much of this gap can be closed with practical error correction codes and distortion compensation. In our experiment we embedded 10^7 bits in a pseudorandom white Gaussian host using memory-8, rate-1/2 and rate-1/4, convolutional codes with maximal free distance. Table 2 contains the generators and free distances of these codes [35, Tbl. 11.1]. Experimentally measured bit-error rate (BER) curves are plotted in Fig. 14. We observe an error correction coding gain of about 5 dB at a BER of 10^{-6}. Distortion compensation provides an additional 1-dB gain.

From the definition of $\mathrm{DNR}_{\mathrm{norm}}$ (33), we see these gain factors translate directly into

Table 2. Convolutional code parameters. Each code has a memory of 8 (constraint length of 9).

Rate (R_{conv})	Generators (octal)	d_{free}
1/2	561, 753	12
1/4	463, 535, 733, 745	24

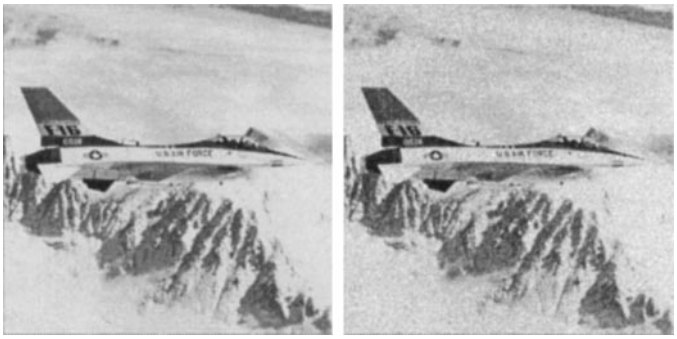


Figure 13. Composite (left) and AWGN channel output (right) images. The composite and channel output images have peak signal-to-distortion ratios of 34.9 dB and 22.6 dB, respectively. DNR $= -12.1$ dB, yet all bits were extracted without error. $R_m = 1/512$ and $\mathrm{DNR}_{\mathrm{norm}} = 15.0$ dB so the actual bit-error probability is 10^{-6}.

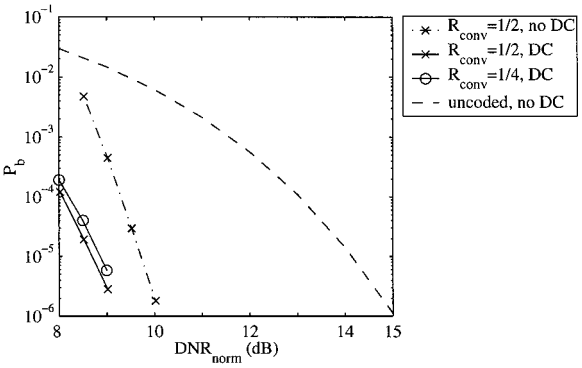


Figure 14. Error-correction coding and distortion-compensation (DC) gains. With common, memory-8 convolutional codes one can obtain gains of about 5 dB over uncoded STDM. Distortion compensation yields about 1 dB additional gain.

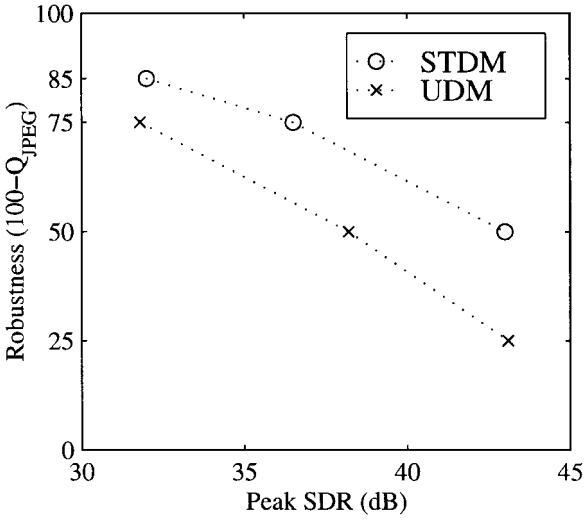


Figure 15. Achievable robustness-distortion trade-offs of dither modulation on the JPEG channel. $R_m = 1/320$. The bit-error rate is less than 5×10^{-6}.

1. a factor increase in rate for fixed levels of embedding-induced distortion and channel noise (robustness), or
2. a factor reduction in distortion for a fixed rate and robustness, or
3. a factor increase in robustness for a fixed rate and distortion.

Thus, the minimum $\mathrm{DNR}_{\mathrm{norm}}$ required for a given bit-error rate is, indeed, the fundamental parameter of interest and, as one can see from (32), in the Gaussian case the $\mathrm{DNR}_{\mathrm{norm}}$ also completely determines the bit-error probability for uncoded STDM for $R_m \leq 1$.

6.2. JPEG Channel

The robustness of digital watermarking algorithms to common lossy compression algorithms such as JPEG is of considerable interest. A natural measure of robustness is the worst tolerable JPEG quality factor (The JPEG quality factor is a number between 0 and 100, 0 representing the most compression and lowest quality, and 100 representing the least compression and highest quality.) for a given bit-error rate at a given distortion level and embedding rate. We experimentally determined achievable rate-distortion-robustness operating points for particular uncoded implementations of both STDM and unspread dither modulation (UDM), where all host signal components were quantized with the same step size.

These achievable distortion-robustness trade-offs at an embedding rate of $R_m = 1/320$ bits per grayscale pixel are shown in Fig. 15 at various JPEG quality factors ($\mathrm{Q}_{\mathrm{JPEG}}$). The peak signal-to-distortion ratio (SDR) is defined as the ratio between the square of the maximum possible pixel value and the average embedding-induced distortion per pixel. The host and composite signals, both 512-by-512 images, are shown in Fig. 16. The actual embedding is performed in the DCT domain using 8-by-8 blocks ($f_1, f_2 \in \{0, 1/16, \ldots, 7/16\}$) and low frequencies ($\sqrt{f_1^2 + f_2^2} \leq 1/4$), with 1 bit embedded across 5 DCT blocks. STDM is better than unspread dither modulation by about 5 dB at ($100 - \mathrm{Q}_{\mathrm{JPEG}}$) of 50 and 75. One explanation for this performance advantage is given in [11] in terms of the number of "nearest neighbors", or the number of directions in which large perturbation vectors can cause decoding errors.

Although no bit errors occurred during the simulations used to generate Fig. 15, we estimate the bit-error rate to be at most 5×10^{-6}. At an embedding rate of $1/320$, one can only embed 819 bits in the host signal image, which is not enough to measure bit-error rates this low. However, one can estimate an upper bound on the bit-error rate by measuring the bit-error rate ϵ at an embedding rate five times higher ($R_m = 1/64$) and calculating the coded bit-error probability of a rate-$1/5$ repetition code when the uncoded error probability is ϵ assuming independent errors, which can approximately be obtained by embedding the repeated bits in spatially separated places in the image. This coded

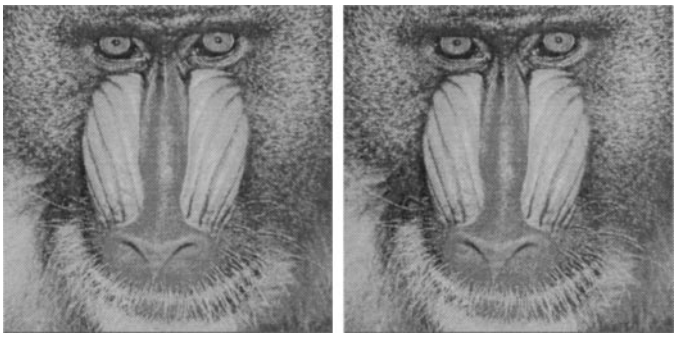


Figure 16. Host (left) and composite (right) image. After 25%-quality JPEG compression of the composite image, all bits were extracted without error. $R_m = 1/320$. Peak SDR of composite image is 36.5 dB.

bit-error probability is

$$P_{\text{rep}} = \sum_{k=3}^{5} \binom{5}{k} \epsilon^k (1-\epsilon)^{5-k} \tag{34}$$

If $\epsilon \leq 32/4096$, then (34) implies $P_{\text{rep}} \leq 4.7 \times 10^{-6}$. Thus, to obtain Fig. 15, we first embedded at a rate of $1/64$ adjusting the SDR until $\epsilon \leq 32/4096$. Then, we embedded at a rate of $1/320$ using a rate-$1/5$ repetition code to verify that no bit errors occurred.

A similar set of experiments was performed to illustrate to advantages of distortion-compensated STDM over regular STDM against JPEG compression attacks. Again, a rate-$1/5$ repetition code was used to embed 1 bit in the low frequencies of five 8-by-8 DCT blocks for an overall embedding rate of $1/320$. Using Fig. 15, we chose a low enough distortion level (SDR = 43 dB) such that we would be able to observe errors in the 819 decoded bits after 25-percent quality JPEG compression. Then, we measured the decoded bit-error rate with different distortion compensation parameters α (12). The results are shown in Fig. 17.

We see that distortion compensation is helpful, provided that one chooses α to obtain an efficient trade-off between minimum distance and distortion-compensation interference, both of which are increased by decreasing α, as discussed in Section 4.2. The measured distortion-to-noise ratios in the projections of the received signals onto the STDM pseudorandom vectors were between 3.2 dB and 3.6 dB. For DNRs in this range, the α given by (13), which maximizes "SNR at the decision device" and is optimal for AWGN channels, is between 0.67 and 0.69. Although the measured bit-rate error in Fig. 17 is lower for $\alpha = 0.8$ than for $\alpha = 0.7$ (21/819 vs. 24/819), these measurements are within statistical uncertainty.

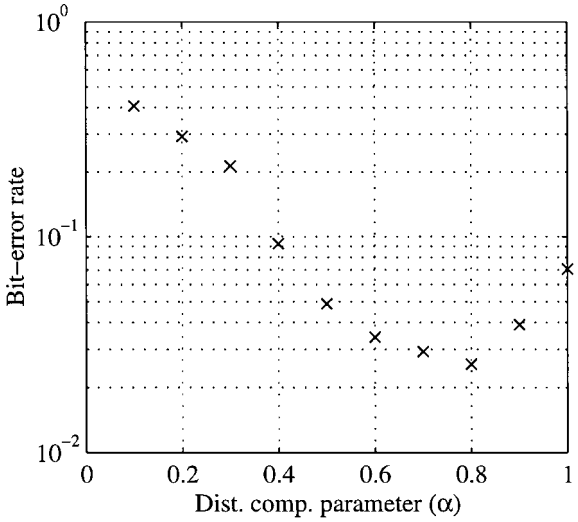


Figure 17. Bit-error rate for various distortion compensation parameters for JPEG compression channel of 25%-quality. $R_m = 1/320$. The peak SDR, between 43.3–43.4 dB, is chosen high enough to obtain a measurable bit-error rate.

7. Concluding Remarks

We have presented a class of information embedding methods called quantization index modulation (QIM) along with several low complexity realizations based on dither modulation and uniform scalar quantization. These methods can also be combined with suitable preprocessing and postprocessing steps such as distortion compensation. It is shown in [7, 11] that these methods achieve provably better rate-distortion-robustness trade-offs than previously proposed classes of methods such as spread spectrum and low-bit(s) modulation against worst-case square-error distortion-constrained intentional attacks, which may be encountered in a

number of copyright, authentication, and covert communication multimedia applications.

In this paper we have determined information-embedding capacities in the case of Gaussian host signals and additive Gaussian noise with arbitrary statistics. The capacities in these cases equal that of the white host signal and white noise case, which are presented in [11]. When applied to multimedia applications such as hybrid transmission and embedding of authentication signals, these results imply a capacity of about 1/3 b/s for every Hertz of host signal bandwidth and dB drop in received host signal quality. QIM methods exist that achieve performance within 1.6 dB of these capacities, and even this small gap can be eliminated with distortion compensation.

Finally, we have implemented a number of dither modulation examples and demonstrated their performance against Gaussian noise and JPEG compression attacks. Other attacks such as those arising from geometric distortions are left for future work.

Appendix A. Formal Capacity Proof: Colored Host, White Noise

In this appendix we formally complete the derivation of capacity (22) that is sketched in Section 5.1 for the case of a colored Gaussian host signal and white Gaussian noise. As described in that section, our goal is to find a probability density function (pdf) $p_{\tilde{u},\tilde{e}|\tilde{x}}(\tilde{u}, \tilde{e} \mid \tilde{x})$ that maximizes the transform-domain version of (19),

$$C = \max_{p_{\tilde{u},\tilde{e}|\tilde{x}}(\tilde{u},\tilde{e}|\tilde{x})} I(\tilde{u};\tilde{y}) - I(\tilde{u};\tilde{x}), \tag{35}$$

subject to the constraint

$$E[\tilde{e}^T \tilde{e}] \le LD_{\mathbf{s}}. \tag{36}$$

Our strategy is to hypothesize a pdf $p_{\tilde{u},\tilde{e}|\tilde{x}}(\tilde{u}, \tilde{e} \mid \tilde{x})$ and show that with this choice of pdf $I(\tilde{u};\tilde{y}) - I(\tilde{u};\tilde{x})$ in (35) equals the expression in (21). Since this expression is also the capacity in the case when the host signal is known at the decoder [11], we cannot hope to achieve a higher rate, and hence, this pdf must indeed maximize (35).

We consider the pdf corresponding to the case where

$$\tilde{u} = \tilde{e} + \alpha\tilde{x}, \quad \tilde{e} \sim \mathcal{N}(0, D_{\mathbf{s}}I), \tag{37}$$

$\tilde{e}$ and $\tilde{x}$ are statistically independent, and α is given by (13). (The notation $v \sim \mathcal{N}(\mu, K)$ means that v is a Gaussian random vector with mean μ and covariance matrix K.) Clearly, this choice of pdf satisfies the distortion constraint (36). Also, as explained in Section 5.1, $\tilde{x} \sim \mathcal{N}(0, \Lambda_x)$ so $\tilde{u} \sim \mathcal{N}(0, D_{\mathbf{s}}I + \alpha^2\Lambda_x)$. The differential entropy $h(v)$ of an L-dimensional Gaussian random vector $v \sim \mathcal{N}(\mu, K)$ is [30]

$$\frac{1}{2}\log_2(2\pi e)^L |K|,$$

which for diagonal covariance matrices $K = \mathrm{diag}(k_1, \ldots, k_L)$ reduces to

$$\sum_{i=1}^{L} \frac{1}{2}\log_2(2\pi e k_i). \tag{38}$$

Therefore,

$$\begin{aligned} I(\tilde{u};\tilde{x}) &\stackrel{\Delta}{=} h(\tilde{u}) - h(\tilde{u} \mid \tilde{x}) \\ &= h(\tilde{u}) - h(\tilde{e}) \\ &= \sum_{i=1}^{L} \frac{1}{2}\log_2[2\pi e(D_{\mathbf{s}} + \alpha^2\lambda_{x,i})] \\ &\quad - \sum_{i=1}^{L} \frac{1}{2}\log_2(2\pi e D_{\mathbf{s}}) \\ &= \sum_{i=1}^{L} \frac{1}{2}\log_2 \frac{D_{\mathbf{s}} + \alpha^2\lambda_{x,i}}{D_{\mathbf{s}}}, \end{aligned} \tag{39}$$

where $\lambda_{x,i}$ denotes the i-th diagonal entry of Λ_x. The second line follows from (37) and the statistical independence of $\tilde{e}$ and $\tilde{x}$, and the third line follows since $\tilde{u}$ and $\tilde{e}$ have diagonal covariance matrices and, hence, have entropies of the form (38). Thus, all that remains is to compute $I(\tilde{u};\tilde{y})$ in (35).

The transform-domain channel output $\tilde{y} = \tilde{e} + \tilde{x} + \tilde{n}$ has a diagonal covariance matrix $K_{\tilde{y}} = D_{\mathbf{s}}I + \Lambda_x + \sigma_n^2 I$ and via (37) can be written in the form

$$\tilde{y} = \tilde{u} + (1-\alpha)\tilde{x} + \tilde{n}. \tag{40}$$

Thus, the differential entropy of $\tilde{y}$ is given by (38)

$$h(\tilde{y}) = \sum_{i=1}^{L} \frac{1}{2}\log_2\left[2\pi e\left(D_{\mathbf{s}} + \lambda_{x,i} + \sigma_n^2\right)\right]. \tag{41}$$

One can similarly determine $h(\tilde{y} \mid \tilde{u})$ after determining $K_{\tilde{y}|\tilde{u}}$. Since $\tilde{y}$ and $\tilde{u}$ are jointly Gaussian vectors, the conditional density of $\tilde{y}$ is Gaussian with conditional covariance matrix [34, (Eq. 1.150)]

$$K_{\tilde{y}|\tilde{u}} = K_{\tilde{y}} - K_{\tilde{y}\tilde{u}}K_{\tilde{u}}^{-1}K_{\tilde{y}\tilde{u}}^T. \tag{42}$$

From (40) and (37), one can infer that

$$K_{\tilde{y}} = K_{\tilde{u}} + (1-\alpha)^2 K_{\tilde{x}} + K_{\tilde{n}} + (1-\alpha)\big(K_{\tilde{x}\tilde{u}} + K_{\tilde{x}\tilde{u}}^T\big)$$

and

$$\begin{aligned} K_{\tilde{y}\tilde{u}} K_{\tilde{u}}^{-1} K_{\tilde{y}\tilde{u}}^T &= \big[K_{\tilde{u}} + (1-\alpha)K_{\tilde{x}\tilde{u}}\big] K_{\tilde{u}}^{-1} \big[K_{\tilde{u}} + (1-\alpha)K_{\tilde{x}\tilde{u}}^T\big] \\ &= K_{\tilde{u}} + (1-\alpha)\big(K_{\tilde{x}\tilde{u}} + K_{\tilde{x}\tilde{u}}^T\big) \\ &\quad + (1-\alpha)^2 K_{\tilde{x}\tilde{u}} K_{\tilde{u}}^{-1} K_{\tilde{x}\tilde{u}}^T. \end{aligned}$$

Inserting these expressions into (42), we obtain

$$K_{\tilde{y}|\tilde{u}} = K_{\tilde{n}} + (1-\alpha)^2 \big[K_{\tilde{x}} - K_{\tilde{x}\tilde{u}} K_{\tilde{u}}^{-1} K_{\tilde{x}\tilde{u}}^T\big],$$

which is a diagonal matrix since $K_{\tilde{n}}$, $K_{\tilde{x}}$, $K_{\tilde{x}\tilde{u}}$, and $K_{\tilde{u}}$ are all diagonal. The i-th diagonal entry is

$$\begin{aligned} [K_{\tilde{y}|\tilde{u}}]_{ii} &= \sigma_n^2 + (1-\alpha)^2 \left[\lambda_{x,i} - \frac{\alpha^2 \lambda_{x,i}^2}{D_{\mathbf{s}} + \alpha^2 \lambda_{x,i}}\right] \\ &= \frac{\sigma_n^2 (D_{\mathbf{s}} + \alpha^2 \lambda_{x,i}) + (1-\alpha)^2 \lambda_{x,i} D_{\mathbf{s}}}{D_{\mathbf{s}} + \alpha^2 \lambda_{x,i}} \end{aligned}$$

Thus, the conditional entropy (38) of this conditionally Gaussian random vector is

$$h(\tilde{y} \mid \tilde{u}) = \sum_{i=1}^{L} \frac{1}{2} \log_2 \left[2\pi e \frac{\sigma_n^2 (D_{\mathbf{s}} + \alpha^2 \lambda_{x,i}) + (1-\alpha)^2 \lambda_{x,i} D_{\mathbf{s}}}{D_{\mathbf{s}} + \alpha^2 \lambda_{x,i}}\right], \tag{43}$$

and taking the difference between (41) and (43), one obtains

$$I(\tilde{u}; \tilde{y}) = \sum_{i=1}^{L} \frac{1}{2} \log_2 \left[\frac{\big(D_{\mathbf{s}} + \lambda_{x,i} + \sigma_n^2\big)(D_{\mathbf{s}} + \sigma^2 \lambda_{x,i})}{\sigma_n^2 (D_{\mathbf{s}} + \alpha^2 \lambda_{x,i}) + (1-\alpha)^2 \lambda_{x,i} D_{\mathbf{s}}}\right]. \tag{44}$$

Substituting (44) and (39) into (35) yields

$$\begin{aligned} &I(\tilde{u}; \tilde{y}) - I(\tilde{u}; \tilde{x}) \\ &\quad = \sum_{i=1}^{L} \frac{1}{2} \log_2 \left[\frac{D_{\mathbf{s}}(D_{\mathbf{s}} + \lambda_{x,i} + \sigma_n^2)}{\sigma_n^2 (D_{\mathbf{s}} + \alpha^2 \lambda_{x,i}) + (1-\alpha)^2 \lambda_{x,i} D_{\mathbf{s}}}\right] \\ &\quad = \sum_{i=1}^{L} \frac{1}{2} \log_2 \left[\mathrm{DNR} \frac{1 + \mathrm{DNR} + \mathrm{SNR}_{x,i}}{\mathrm{DNR} + \alpha^2 \mathrm{SNR}_{x,i} + (1-\alpha)^2 \mathrm{DNR}\, \mathrm{SNR}_{x,i}}\right], \end{aligned}$$

where $\mathrm{SNR}_{x,i} = \lambda_{x,i}/\sigma_n^2$ is the host signal-to-noise ratio in the i-th channel. Finally, substituting (13) into this expression yields

$$\begin{aligned} &I(\tilde{u}; \tilde{y}) - I(\tilde{u}; \tilde{x}) = \sum_{i=1}^{L} \frac{1}{2} \log_2 \\ &\quad \left[(1+\mathrm{DNR})^2 \mathrm{DNR} \times \frac{1 + \mathrm{DNR} + \mathrm{SNR}_{x,i}}{\mathrm{DNR}(1+\mathrm{DNR})^2 + \mathrm{DNR}^2\, \mathrm{SNR}_{x,i} + \mathrm{DNR}\, \mathrm{SNR}_{x,i}}\right] \\ &\quad = \sum_{i=1}^{L} \frac{1}{2} \log_2 \left[(1+\mathrm{DNR})^2 \frac{1 + \mathrm{DNR} + \mathrm{SNR}_{x,i}}{(1+\mathrm{DNR})^2 + \mathrm{SNR}_{x,i}(1+\mathrm{DNR})}\right] \\ &\quad = \sum_{i=1}^{L} \frac{1}{2} \log_2 (1+\mathrm{DNR}), \end{aligned}$$

which equals the desired expression (21).

Appendix B. Distortion Compensation and Capacity

Distortion-compensated QIM (DC-QIM) can achieve capacity in a number of important scenarios as we discuss in this appendix. Indeed, as we show below, there exists a capacity-achieving DC-QIM method whenever the maximizing distribution $p_{u,e|x}(u, e \mid x)$ in (19) is of a form such that

$$u = e + \alpha x. \tag{45}$$

This condition is satisfied in at least three important cases: (1) the case of a Gaussian host signal and an additive Gaussian noise channel [11]; (2) the case of a Gaussian host signal and arbitrary square-error distortion-constrained attacks [32]; and (3) the case of arbitrary square-error distortion-constrained attacks, a zero-mean, finite variance host signal whose probability density function is bounded and continuous, and asymptotically small embedding-induced distortion $D_{\mathbf{s}}$ and channel perturbation (attacker's distortion) σ_n^2 [32].

To understand why a distribution that satisfies the condition (45) implies the optimality of DC-QIM, we first discuss the achievability of (19). Our discussion of achievability here is basically a summary of Gel'fand and Pinsker's capacity-achievability proof [33], with added interpretation in terms of quantization (source coding). Suppose, we draw the codewords u (reconstruction vectors) of our QIM quantizer ensemble from the iid distribution $p_u(u)$, which is the marginal distribution corresponding to the host signal distribution $p_x(x)$ and the maximizing conditional distribution $p_{u,e|x}(u, e \mid x)$ from (19). We draw

$2^{N(I(U;Y)-\epsilon)}$ total codewords and assign an equal number of them to each of $2^{N(C-2\epsilon)}$ quantizers. Thus, since $C = I(U;Y) - I(U;X)$, each quantizer has $2^{N(I(U;X)+\epsilon)}$ codewords. The encoder finds a vector u_0 in the m-th quantizer's codebook that is jointly distortion-typical with $\alpha\mathsf{x}$ and generates $\mathsf{e}(\mathsf{u}_0, \mathsf{x})$. (From convexity properties of mutual information, one can deduce that the maximizing distribution in (19) always has the property that e is a deterministic function of (u, x) [33]. If the maximizing distribution satisfies (45), for example, then $\mathsf{e} = \mathsf{u}_0 - \alpha\mathsf{x}$.) Since the m-th quantizer's codebook contains $2^{N(I(U;X)+\epsilon)} = 2^{N(I(U;\alpha X)+\epsilon)}$ vectors, the probability that there is no u_0 that is jointly distortion-typical with $\alpha\mathsf{x}$ is small. (This is one of the main ideas behind the rate-distortion theorem [30, Ch. 13].) The decoder finds a u that is jointly typical with the channel output y and declares $\hat{m} = i$ if this u is in the i-th quantizer's codebook. Because the total number of vectors u is $2^{N(I(U;Y)-\epsilon)}$, the probability that a u other than the u_0 is jointly typical with y is small. Also, the probability that y is jointly typical with u_0 is close to 1. (These are two of the main ideas behind the classical channel coding theorem [30, Ch. 8].) Thus, the probability of error $\Pr[\hat{m} \neq m]$ is small, and we can indeed achieve the capacity (19).

To see that DC-QIM can achieve capacity when the maximizing pdf in (19) satisfies (45), we show that one can construct an ensemble of random DC-QIM codebooks that satisfy (45). First, we observe that quantizing x is equivalent to quantizing αx with a scaled version of the quantizer and scaling back, i.e.,

$$\mathbf{q}(\mathsf{x}; m, \Delta/\alpha) = \frac{1}{\alpha}\mathbf{q}(\alpha\mathsf{x}; m, \Delta). \tag{46}$$

This identity simply represents a change of units to "units of $1/\alpha$" before quantization followed by a change back to "normal" units after quantization. For example, if $\alpha = 1/1000$, instead of quantizing x volts we quantize $\alpha\mathsf{x}$ kilovolts (using the same quantizer, but relabeling the reconstruction points in kilovolts) and convert kilovolts back to volts by multiplying by $1/\alpha$. Then, rearranging terms in the DC-QIM embedding function (12) and substituting (46) into the result, we obtain

$$\begin{aligned}\mathbf{s}(\mathsf{x}, m) &= \mathbf{q}(\mathsf{x}; m, \Delta/\alpha) + (1-\alpha)[\mathsf{x} - \mathbf{q}(\mathsf{x}; m, \Delta/\alpha)] \\ &= \alpha\mathbf{q}(\mathsf{x}; m, \Delta/\alpha) + (1-\alpha)\mathsf{x} \\ &= \mathbf{q}(\alpha\mathsf{x}; m, \Delta) + (1-\alpha)\mathsf{x}. \end{aligned} \tag{47}$$

We construct our random DC-QIM codebooks by choosing the codewords of $\mathbf{q}(\cdot; m, \Delta)$ from the iid distribution $p_U(u)$, the one corresponding to (45). (Equivalently, we choose the codewords of $\mathbf{q}(\cdot; m, \Delta/\alpha)$ in (12) from the distribution of U/α, i.e., the iid distribution $\alpha p_U(\alpha u)$.) Our quantizers $\mathbf{q}(\cdot; m, \Delta)$ choose a codeword $\mathbf{u}_0$ that is jointly distortion-typical with αx. The decoder looks for a codeword in all of the codebooks that is jointly typical with the channel output. Then, following the achievability argument given above at the beginning of this appendix, we can achieve a rate $I(U;Y) - I(U;X)$. From (47), we see that

$$\mathbf{s}(\mathsf{x}, m) = \mathsf{x} + [\mathbf{q}(\alpha\mathsf{x}; m, \Delta) - \alpha\mathsf{x}] = \mathsf{x} + (\mathbf{u}_0 - \alpha\mathsf{x}).$$

Since $\mathbf{s}(\mathsf{x}, m) = \mathsf{x} + \mathsf{e}$, we see that $\mathbf{e} = \mathbf{u_0} - \alpha\mathsf{x}$. Thus, if the maximizing distribution in (19) satisfies (45), our DC-QIM codebooks can also have this distribution and, hence, achieve capacity (19).

Thus, indeed, capacity-achieving DC-QIM methods exist whenever the capacity-achieving probability distribution has a form satisfying (45). In the case of a Gaussian host signal and an additive Guassian noise channel, the optimal distortion compensation parameter is [11]

$$\alpha = \frac{\mathrm{DNR}}{\mathrm{DNR}+1}.$$

This value of α is also asymptotically optimal with small embedding-induced distortion and attacker's distortion for the case of arbitrary square-error distortion-constrained attacks and non-Gaussian host signals with zero-mean, finite variance, and a bounded and continuous probability density function [32]. In this case the DNR is defined as the ratio between the embedding-induced distortion and the attacker's distortion (as opposed to additive noise variance). With this definition of DNR, the optimal (even non-asymptotically) α in the case of arbitrary square-error distortion-constrained attacks with a Gaussian host signal is [32]

$$\alpha = \frac{\mathrm{DNR}}{\mathrm{DNR}+\beta}, \quad \beta = \frac{\mathrm{SNR}_x + \mathrm{DNR}}{\mathrm{SNR}_x + \mathrm{DNR} - 1},$$

where SNR_x is defined as the ratio between the host signal variance and the attacker's distortion.

Acknowledgments

This work has been supported in part by the Office of Naval Research under Grant No. N00014-96-1-0930, by the Air Force Office of Scientific Research under Grant No. F49620-96-1-0072, by the MIT Lincoln Laboratory Advanced Concepts Committee, and by a National Defense Science and Engineering Graduate Fellowship. The authors would also like to thank Amos

Lapidoth, of MIT and ETH Zurich, for calling our attention to the paper by Costa [31].

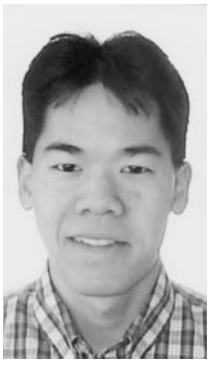
Notes

1. Some types of distortion, such as geometric distortions can be large in terms of square error, yet still be small perceptually. However, in some cases these distortions can be mitigated either by pre-processing at the decoder or by embedding information in parameters of the host signal that are less affected (in terms of square error) by these distortions. For example, a simple delay or shift may cause large square error, but the magnitude of the DFT coefficients are relatively unaffected.
2. The duality between this problem and the problem of source coding with side information at the *decoder* is explored in [36].
3. To generate the curve, robustness is measured by the ratio in dB between noise variance and square-error embedding-induced distortion, the rate is the information-theoretic capacity (Eq. (18) and [37, Eq. (16)] for host-interference rejecting and non-rejecting, respectively) in bits per host signal sample, and the ratio between the host signal variance and the square-error embedding-induced distortion is fixed at 20 dB.
4. A uniform distribution for the dither sequence implies that the quantization error is statistically independent of the host signal and leads to fewer "false contours", both of which are generally desirable properties from a perceptual viewpoint [25].
5. By worst case, we mean the case where the attacker knows everything about the embedding function, i.e., a no-key scenario. Moulin and O'Sullivan [32] have examined "optimal" attacks relative to a randomized *set* of codebooks (embedding functions), which may be interpreted as a private-key scenario. We discuss implications of their results later in this paper.

References

1. F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," *Proceedings of the IEEE*, vol. 87, 1999, pp. 1079–1107.
2. M.D. Swanson, M. Kobayashi, and A.H. Tewfik, "Multimedia Data-Embedding and Water-Marking Technologies," *Proceedings of the IEEE*, vol. 86, 1998, pp. 1064–1087.
3. I.J. Cox and J.-P.M.G. Linnartz, "Some General Methods for Tampering with Watermarks," *IEEE Journal on Selected Areas in Communications*, vol. 16, 1998, pp. 587–593.
4. J.-P. Linnartz, T. Kalker, and J. Haitsma, "Detecting Electronic Watermarks in Digital Video," in *Proc. of the 1999 IEEE International Conference on Acoustics, Speech, and Signal Processing*, Phoenix, AZ, March 1999, vol. 4, pp. 2071–2074.
5. D. Kundur and D. Hatzinakos, "Digital Watermarking for Telltale Tamper Proofing and Authentication," *Proceedings of the IEEE*, vol. 87, 1999, pp. 1167–1180.
6. F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Information Hiding—A Survey," *Proceedings of the IEEE*, vol. 87, 1999, pp. 1062–1078.
7. B. Chen, "Design and Analysis of Digital Watermarking, Information Embedding, and Data Hiding Systems," Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, June 2000.
8. H.C. Papadopoulos and C.-E.W. Sundberg, "Simultaneous Broadcasting of Analog FM and Digital Audio Signals by Means of Adaptive Precanceling Techniques," *IEEE Transactions on Communications*, vol. 46, 1998, pp. 1233–1242.
9. B. Chen and C.-E.W. Sundberg, "Broadcasting Data in the FM Band by Means of Adaptive Contiguous Band Insertion and Precancelling Techniques," in *Proceedings of 1999 IEEE International Conference on Communications*, Vancouver, Canada, June 1999, vol. 2, pp. 823–827.
10. M.D. Swanson, B. Zhu, and A.H. Tewfik, "Data Hiding for Video-in-Video," in *Proceedings of the 1997 IEEE International Conference on Image Processing*, Piscataway, NJ, 1997, vol. 2, pp. 676–679.
11. B. Chen and G.W. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding," To appear, *IEEE Transactions on Information Theory*, accepted for publication.
12. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for Data Hiding," *IBM Systems Journal*, vol. 35, no. 3/4, 1996, pp. 313–336.
13. I.J. Cox, J. Killian, T. Leighton, and T. Shamoon, "A Secure, Robust Watermark for Multimedia," in *Information Hiding. First International Workshop Proceedings*, June 1996, pp. 185–206.
14. J.R. Smith and B.O Comiskey, "Modulation and Information Hiding in Images," in *Information Hiding. First International Workshop Proceedings*, June 1996, pp. 207–226.
15. J.R. Hernandez, F. Perez-Gonzalez, J.M. Rodriguez, and G. Nieto, "Performance Analysis of a 2-D-Multipulse Amplitude Modulation Scheme for Data Hiding and Watermarking of Still Images," *IEEE Journal on Selected Areas in Communications*, vol. 16, 1998, pp. 510–524.
16. A.Z. Tirkel, G.A. Rankin, R. van Schyndel, W.J. Ho, N.R.A. Mee, and C.F. Osborne, "Electronic Water Mark," in *Proceedings of Digital Image Computing, Technology and Applications*, Sydney, Australia, Dec. 1993, pp. 666–672.
17. R. van Schyndel, A.Z. Tirkel, and C.F. Osborne, "A Digital Watermark," in *Proceedings of the First IEEE International Conference on Image Processing*, Austin, TX, Nov. 1994, vol. 2, pp. 86–90.
18. I.J. Cox, J. Killian, F.T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, vol. 6, pp. 1673–1687, 1997.
19. J.K. Su, "Power-Spectrum Condition-Complaint Watermarking," DFG V^3D^2 Watermarking Workshop, Oct. 1999. Abstract and transparencies from this talk were obtained from `http://www.lnt.de/~watermarking`.
20. C.I. Podilchuk and W. Zeng, "Image-Adaptive Watermarking Using Visual Models," *IEEE Journal on Selected Areas in Communications*, vol. 16, 1998, pp. 525–539.
21. M.D. Swanson, B. Zhu, and A.H. Tewfik, "Robust Data Hiding for Images," in *Proceedings of the 1996 IEEE Digital Signal Processing Workshop*, Loen, Norway, Sept. 1996, pp. 37–40.
22. B. Chen and G.W. Wornell, "Dither Modulation: A New Approach to Digital Watermarking and Information Embedding," in *Proceedings of SPIE: Security and Watermarking of Multimedia Contents*, San Jose, CA, Jan. 1999, vol. 3657, pp. 342–353.
23. J. Wolosewicz and K. Jemili, "Apparatus and Method for Encoding and Decoding Information in Analog Signals," United States Patent #5,828,325, Oct. 1998.
24. E.A. Lee and D.G. Messerschmitt, *Digital Communication*, 2nd edn., Boston, MA: Kluwer Academic Publishers, 1994.

25. N.S. Jayant and P. Noll, *Digital Coding of Waveforms: Principles and Applications to Speech and Video*, Englewood Cliffs, NJ: Prentice-Hall, 1984.
26. R. Zamir and M. Feder, "On Lattice Quantization Noise," *IEEE Transactions on Information Theory*, vol. 42, 1996, pp. 1152–1159.
27. G. Ungerboeck, "Channel Coding With Multilevel/Phase Signals," *IEEE Transactions on Information Theory*, vol. 28, 1982, pp. 55–67.
28. T.M. Cover, "Broadcast Channels," *IEEE Transactions on Information Theory*, vol. 18, 1972, pp. 2–14.
29. K. Ramchandran, A. Ortega, K.M. Uz, and M. Vetterli, "Multiresolution Broadcast for Digital HDTV Using Joint Source/Channel Coding," *IEEE Journal on Selected Areas in Communications*, vol. 11, 1993, pp. 6–23.
30. T.M. Cover and J.A. Thomas, *Elements of Information Theory*, New York, NY: John Wiley & Sons, 1991.
31. M.H.M. Costa, "Writing on Dirty Paper," *IEEE Transactions on Information Theory*, vol. IT-29, 1983, pp. 439–441.
32. P. Moulin and J.A. O'Sullivan, "Information-theoretic analysis of information hiding," Preprint, 1999.
33. S.I. Gel'fand and M.S. Pinsker, "Coding for Channel with Random Parameters," *Problems of Control and Information Theory*, vol. 9, no. 1, 1980, pp. 19–31.
34. A.S. Willsky, G.W. Wornell, and J.H. Shapiro, "Stochastic Processes, Detection and Estimation," MIT 6.432 Supplementary Course Notes, Cambridge, MA, 1996.
35. S. Lin and D.J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, Englewood Cliffs, NJ: Prentice-Hall, 1983.
36. R.J. Barron, B. Chen, and G.W. Wornell, "The Duality Between Information Embedding and Source Coding with Side Information and Its Implications and Applications," *IEEE Transactions on Information Theory*, submitted.
37. B. Chen and G.W. Wornell, "Provably Robust Digital Watermarking," in *Proceedings of SPIE: Multimedia Systems and Applications II*, Boston, MA, Sept. 1999, vol. 3845, pp. 43–54.



Brian Chen was born in Warren, MI, and received the B.S.E. degree from the University of Michigan, Ann Arbor, in 1994, and the S.M. degree from the Massachusetts Institute of Technology (MIT), Cambridge, in 1996, both in electrical engineering. He has submitted his doctoral thesis and will formally receive the Ph.D. degree in electrical engineering and computer science from MIT, Cambridge, in June 2000.

He currently holds the position of Chief Technology Officer and Vice President of Technology of Chinook Communications, Inc., Somerville, MA. Since 1994 he has also been affiliated with the Department of Electrical Engineering and Computer Science and the Research Laboratory of Electronics, MIT, Cambridge, where he has held a National Defense Science and Engineering Graduate Fellowship and has served as both a Teaching Assistant and a Research Assistant. During 1996 and 1997, he was also with Lucent Technologies, Bell Laboratories, Murray Hill, NJ, both as a Member of Technical Staff—Level 1 and as a Consultant, developing signal design and channel coding technologies for digital audio broadcasting. His current research interests lie in the broad areas of communications and signal processing, with particular emphasis on information embedding, digital watermarking, and other multimedia communications topics. He has eleven patents pending.

He is a member of Eta Kappa Nu, Tau Beta Pi, and IEEE. He has received the University of Michigan Regents-Alumni Scholarship, the William J. Branstrom Freshman Prize, and the Henry Ford II Prize from the University of Michigan.

Gregory W. Wornell received the B.A.Sc. degree (with honors) from the University of British Columbia, Canada, and the S.M. and Ph.D. degrees from the Massachusetts Institute of Technology, all in electrical engineering, in 1985, 1987 and 1991, respectively.

Since 1991 he has been on the faculty of the Department of Electrical Engineering and Computer Science at MIT, where he is currently an Associate Professor. He has spent leaves at the University of California, Berkeley, CA, in 1999–2000 and at AT&T Bell Laboratories, Murray Hill, NJ, in 1992–93. His research interests span signal processing, and wireless, broadband, and multimedia communications. He is author of the monograph *Signal Processing with Fractals: A Wavelet-Based Approach* and co-editor of the volume *Wireless Communications: Signal Processing Perspectives* (Prentice-Hall). Within the IEEE he is currently Associate Editor for the communications area for *Signal Processing Letters*, and serves on the Communications Technical Committee of the Signal Processing Society. He is also a consultant to industry and an inventor on numerous issued and pending patents.

Among the awards he has received for teaching and research are the MIT Goodwin Medal for "conspicuously effective teaching" (1991), the ITT Career Development Chair at MIT (1993), an NSF Faculty Early Career Development Award (1995), an ONR Young Investigator Award (1996), the MIT Junior Bose Award for Excellence in Teaching (1996), the Cecil and Ida Green Career Development Chair at MIT (1996), and an MIT Graduate Student Council Teaching Award (1998). Dr. Wornell is also a member of Tau Beta Pi and Sigma Xi.