

Image Adaptive High Volume Data Hiding Based on Scalar Quantization

N. Jacobsen, K. Solanki, U. Madhow, B. S. Manjunath, and S. Chandrasekaran
 Dept. of Electrical and Computer Engineering
 University of California at Santa Barbara
 Santa Barbara, CA 93106

Abstract—

Information-theoretic analyses for data hiding prescribe embedding the hidden data in the choice of quantizer for the host data. In this paper, we consider a suboptimal implementation of this prescription, with a view to hiding high volumes of data in images with low perceptual degradation. The three main findings are as follows:

- (i) Scalar quantization based data hiding schemes incur a $2dB$ penalty from the optimal embedding strategy, which involves vector quantization of the host.
- (ii) In order to limit perceivable distortion while hiding large amounts of data, hiding schemes must use local perceptual criteria in addition to information-theoretic guidelines.
- (iii) Powerful erasures and errors correcting codes provide a flexible framework that allows the data-hider freedom of choice of where to embed without requiring synchronization between encoder and decoder.

I. INTRODUCTION

Our objective is to obtain techniques for embedding high volumes of data in images, in a manner that causes minimal perceptual degradation, and is robust to “benign” JPEG compression as well as more malicious Additive White Gaussian Noise (AWGN) attacks. Information-theoretic treatments of the data hiding problem typically focus on hiding in independent and identically distributed (i.i.d.) Gaussian host samples. The hider is allowed to induce a mean squared error of at most D_1 , while an attacker operating on the host with the hidden data is allowed to induce a mean squared error of at most D_2 . Information-theoretic prescriptions in this context translate, roughly speaking, to hiding data by means of the choice of vector quantizer for the host data, with the AWGN attack being the worst-case under certain assumptions.

The main contributions of the present paper are as follows. First, we motivate the use of scalar quantization based methods by providing an information-theoretic analysis that shows that scalar quantization based strategies come within about $2dB$ (in terms of the ratio of D_1/D_2 required to attain a given hiding capacity) of the optimal vector quantization based strategy for AWGN attacks. Such strategies, in which each host symbol is quantized using a scalar quantizer, whose choice is dictated by the message symbol, were first proposed by Chen and Wornell [1], but the capacity penalty due to the suboptimal embedding was not previously known. Next, we propose practical strategies for embedding high volumes of data in images with low

perceptual degradation. As in many recent papers, the information is embedded in the low and mid frequency bands of the Discrete Cosine Transform (DCT) coefficients of the image, which have higher variance, and can therefore better tolerate the additional distortion due to the embedding. The novelty of our approach lies, however, in that it allows the flexibility of embedding data in designated areas of the image where it would be less noticeable, without requiring any additional side information to be sent to the decoder regarding the location of the embedded message.

Our embedding approach is as follows. Both the encoder and decoder know the set of DCT coefficients in the low and mid frequency bands that are possible candidates for embedding. In addition, the encoder uses local criteria to decide which subset of the coefficients which it will actually embed data in. The decoder employs the same criteria to guess where the encoder has embedded data. The distortion due to attacks may now lead to insertion errors (the decoder guessing that a coefficient has embedded data, when it actually does not) and deletion errors (the decoder guessing that a coefficient does not have embedded data, when it actually does). However, unlike the insertion-deletion channel in which the length of the overall symbol sequence can vary [2], in our situation, the set of candidate coefficients for embedding is the same, and is known to both encoder and decoder. This enables an elegant solution to the problem of synchronizing the encoder and decoder. Use a code on the hidden data that spans the entire set of candidate embedding coefficients, and that can correct both errors and erasures. The subset of these coefficients in which the encoder does not embed can be treated as *erasures at the encoder*. The decoder guesses the erasure locations using the same criteria as the encoder. Insertions now become errors, and deletions become additional erasures. Thus, the use of a suitable error correction code simultaneously yields robustness to attack and solves the synchronization problem between encoder and decoder.

The above coding framework is applied to two embedding strategies that we proposed in earlier work on uncoded image-adaptive embedding [3]. The first is the block-level Entropy Thresholding (ET) method, which decides whether or not to embed data in each 8×8 block of DCT coefficients, depending on the entropy, or energy, within that block. The second is the Selectively Embedding in Coefficients (SEC) method decides whether or not to em-

bed data based on the magnitude of the coefficient. Reed-Solomon codes are a natural choice for the block-based ET scheme, while turbo-like codes are employed for the SEC scheme. We are able to hide high volumes of data under both JPEG and AWGN attacks. Due to the suboptimality of our embedding strategy and the decoding algorithm (which employs hard rather than soft decisions), our results are not directly comparable with information-theoretic estimates of the hiding capacity of the image [4]. However, the amount of hidden data is of the same order of magnitude as these estimates.

II. QUANTIZATION BASED DATA HIDING

A. Embedding data in choice of quantizer

As in [1], data is embedded in the host medium through the choice of scalar quantizer. For example, consider a uniform quantizer of step size Δ , used on the host's coefficients in some transform domain. Let odd reconstruction points represent a hidden data bit '1'. Likewise, even multiples of Δ are used to embed '0'. Thus, depending on the bit value to be embedded, one of two uniform quantizers of step size 2Δ is chosen. Moreover, the quantizers can be pseudo-randomly dithered, where the chosen quantizers are shifted by a pseudo-random sequence available only to encoder and decoder. As such, the embedding scheme is not readily decipherable to a third party observer, without explicit knowledge of the dither sequence.

Hard decision decoding in this context is performed by quantizing the received coefficient to the nearest reconstruction point of all quantizers. An even reconstruction point indicates that a '0' has been hidden. Likewise, if a reconstruction point lies on an odd quantizer, a '1' has been hidden. However, if more information regarding the statistics of the attack is available, soft decisions can be used to further improve performance. In Section II-B, we compute the capacity of scalar quantization based hiding for the specific case of AWGN attacks. Implicit in our formulation is the use of soft decisions that account for both the quantization noise and the AWGN.

B. Capacity of scalar quantization based data hiding

While our scalar quantization based scheme is well matched to JPEG compression attacks, we now show that it incurs roughly a $2dB$ penalty for the worst-case AWGN attack. Letting D_1 and D_2 denote the mean squared embedding induced distortion and mean squared attack distortion, the hiding capacity with AWGN attack is given by [5], [6] $C = \frac{1}{2} \log(1 + \frac{D_1}{D_2})$, in the small D_1, D_2 regime that typical data hiding systems operate. We compare this "vector capacity" (termed thus because the optimal strategy involves vector quantization of the host) to that of a scalar quantizer embedding scheme with soft decision decoding.

Consider a data hiding system where the information symbol to be embedded is taken from an alphabet \mathcal{X} . The host's original uniform quantizer is divided into M uniform sub-quantizers (each with quantization interval $M\Delta$),

where $M = |\mathcal{X}|$, a power of two. Thus, we have that $\log_2 M$ bits are hidden per host symbol.

We consider the distortion-compensated quantization embedding scheme of [1] with soft decision decoding. Here, the uniform quantizer is scaled by $\alpha \in (0, 1)$, increasing the distance between adjacent quantizers to Δ/α . As such, the embedding robustness is increased by a factor $1/\alpha^2$ (in the squared minimum distance sense), and embedding induced distortion is increased by the same factor. Encoding the information symbol as a linear combination of the host symbol and its quantized value, as in the following, compensates for the additional distortion. Denoting the host symbol by H , and the hidden message symbol by X , the decoder receives the following symbol:

$$\begin{aligned} Y &= \alpha q_X(H) + (1 - \alpha)H + W \\ &= q_X(H) + (1 - \alpha)(H - q_X(H)) + W \end{aligned} \quad (1)$$

where $q_x(\cdot)$ the scaled uniform quantizer used to embed the information symbol x (with quantization interval $M\Delta/\alpha$), and W the AWGN attack (i.e. $W \sim \mathcal{N}(0, D_2)$). The parameter α achieves a tradeoff between uniform quantization noise and AWGN. The optimal value for α for maximizing the signal-to-noise ratio (SNR) at the decoder, which we have found numerically also to maximize the mutual information $I(X; Y)$, is [1]

$$\alpha_{opt} = \frac{D_1}{D_1 + D_2}$$

The probability density function of the combined additive interferers, $N = (1 - \alpha)Z + W$, where $Z \equiv H - q_X(H)$ is the uniform quantization noise, is given by convolving the uniform and Gaussian densities:

$$f_N(x) = \frac{\alpha(2\pi D_2)^{-\frac{1}{2}}}{(1 - \alpha)M\Delta} \int_{-\frac{(1-\alpha)M\Delta}{2\alpha}}^{\frac{(1-\alpha)M\Delta}{2\alpha}} \exp\left(-\frac{(x - \tau)^2}{2D_2}\right) d\tau \quad (2)$$

We compute the mutual information $I(X; Y) = H(X) - H(X|Y)$ for X uniform over its M -ary alphabet as an estimate of the capacity with scalar quantization based embedding. Thus, $H(X) = \log_2 M$. To find, $H(X|Y)$, we now compute $p_{X|Y}$, the conditional probability mass function of X given Y , and f_Y , the probability density function of Y .

Consider the quantization interval in which the received symbol Y appears, and define its midpoint as the origin. Letting y denote the abscissa, the nearest quantizers appear at $y = \pm \frac{\Delta}{2\alpha}$. Conditioned on the input $X = x$ and host coefficient $H = h$, the distribution of Y is given by $f_{Y|X,H}(y|x, h) = f_N(y - m_x \frac{\Delta}{2\alpha} - k_h \frac{M\Delta}{\alpha})$, with f_N as in (2). Here, $m_x \in \mathcal{M} = \{\pm 1, \pm 3, \dots, \pm 2M - 1\}$ is uniquely determined by the information symbol x , $k_h \in \mathbb{Z}$ by the host coefficient h , and the hidden quantized host coefficient $q_x(h)$ by the pair (m_x, k_h) . Thus we have

$$\begin{aligned} f_{Y|X}(y|x) &= \int_{\mathcal{H}} f_{Y|X,H}(y|x, h) f_H(h) dh \\ &\propto \sum_{k \in \mathbb{Z}} f_N\left(y - m_x \frac{\Delta}{2\alpha} - k \frac{M\Delta}{\alpha}\right) \end{aligned} \quad (3)$$

$$\begin{aligned}
f_Y(y) &= \sum_{x \in \mathcal{X}} f_{Y|X}(y|x) p_X(x) \\
&\propto \sum_{m \in \mathcal{M}} \sum_{k \in \mathbb{Z}} f_N(y - m \frac{\Delta}{2\alpha} - k \frac{M\Delta}{\alpha}) \quad (4)
\end{aligned}$$

where we have assumed that the host H and message X are statistically independent, and that the host's density f_H is roughly constant on an interval around Y , an assumption that is reasonable in the low distortion regime, where the quantization interval is small with respect to variations in the host's distribution.

Since the density of Y is $\frac{\Delta}{\alpha}$ -periodic, it suffices to restrict attention to the interval $[-\frac{\Delta}{2\alpha}, \frac{\Delta}{2\alpha}]$, with f_Y normalized accordingly. Applying Bayes' theorem, the distribution of X given Y is

$$p_{X|Y}(x|y) = \frac{f_{Y|X}(y|x) p_X(x)}{f_Y(y)} \quad (5)$$

so that we can now compute

$$H(X|Y) = \int_{\mathcal{Y}} \sum_{x \in \mathcal{X}} p_{X|Y}(x|y) \log p_{X|Y}(x|y) f_Y(y) dy$$

and hence $I(X; Y)$.

Due to the exponential decay of the Gaussian density, the summation in (3) is well approximated with only the $k = 0$ term (α near one), i.e. the nearest quantization point explaining a transmitted x . Figure 1 plots the mutual information obtained with 2, 4 and 8-ary signaling, as well as vector capacity. We observe roughly a $2dB$ loss due to the suboptimal scalar quantization encoding strategy.

We conclude our analysis by noting that the soft decision statistic, used by an iterative decoder, is the log likelihood ratio (LLR), given in the following for the case of binary signaling.

$$\Lambda(y) = \log \frac{p_{X|Y}(0|y)}{p_{X|Y}(1|y)} = \log \frac{f_{Y|X}(y|0)}{f_{Y|X}(y|1)} \quad (6)$$

When $\alpha = 1$ and (3) approximated as above, the LLR reduces to

$$\Lambda(y) = \log \frac{f_W(y - \frac{\Delta}{2})}{f_W(y + \frac{\Delta}{2})} = \frac{y\Delta}{D_2} \quad (7)$$

III. IMAGE ADAPTIVE DATA HIDING

Most prior image-based data hiding schemes use global criteria regarding where to hide the data, such as statistical criteria independent of the image (e.g. embedding in mid-frequency bands), or criteria matched to a particular image (e.g. embedding in high-variance bands). These are consistent with information theoretic guidelines [4], which call for hiding in "channels" in which the host coefficients have high variance. However, in practice, hiding based on such global statistical criteria can lead to significant perceptual degradation. We present examples of such effects at [7]. This motivates the novel hiding framework presented here,

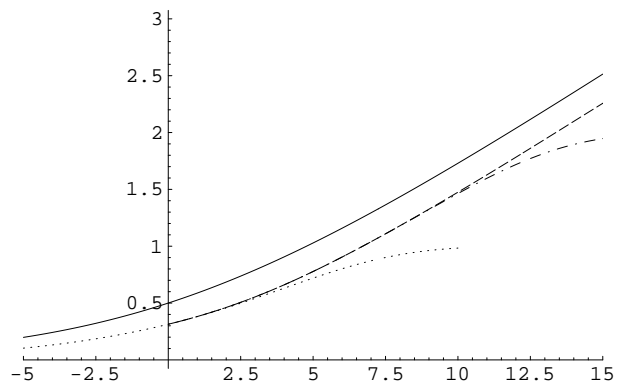


Fig. 1. Gap between scalar [binary: dot, 4-ary: dash-dot, 8-ary: dash] and vector [solid] quantizer data hiding systems. Capacity is in bits per source symbol, DNR in dB.

which affords the flexibility of adapting to local characteristics within a particular image, thus significantly reducing the perceptual degradation due to the hidden data. While we use specific criteria for such local adaptation, our coding framework, which obviates the need for synchronization between encoder and decoder, applies for any other scheme for locally adaptive hiding.

We now describe and extend two image-adaptive hiding techniques, which we had first proposed for uncoded hidden data in [3].

A. Entropy Thresholding scheme

The entropy thresholding scheme uses the energy (or 2-norm entropy) of an 8×8 block to decide whether to embed in the block or not. The entropy is computed as follows.

$$E = \sum_{i,j} \|x_{ij}\|^2, \quad (i,j) \neq (0,0) \quad (8)$$

Only those blocks whose entropy exceeds a predetermined threshold are used to hide data. Likewise, the decoder checks the entropy of each 8×8 block to decide whether data has been hidden.

The embedding procedure is based on JPEG. The image is divided into 8×8 non-overlapping blocks, the energy of the blocks is evaluated, and an 8×8 DCT of the qualifying blocks is taken. The coefficient blocks are divided by the JPEG quantization matrix according to the design quality factor, and finally, bits are hidden using choice of scalar quantizer. Low frequency coefficients are used to embed in qualifying blocks. Embedding in these coefficients induces minimal distortion due to JPEG's finer quantization in this range. Thus, this scheme employs a statistical criterion by hiding in the frequency subbands of large variance, while satisfying a local perceptual criterion via the block entropy threshold.

B. Selectively Embedding in Coefficients scheme

Now, instead of deciding where to embed at the block level, we do a coefficient-by-coefficient selection, with the goal of embedding in those coefficients that cause minimal perceptual distortion.

Here too, an 8×8 DCT of non-overlapping blocks is taken and the coefficients are divided by the JPEG quantization matrix at design quality factor. These coefficient values are quantized to the nearest integer for further processing. We embed in a given coefficient only if the magnitude exceeds a positive integer threshold. As this threshold increases, fewer coefficients qualify for embedding, and hence less data can be hidden, which provides a tradeoff between hiding rate and perceptual quality. For thresholds beyond 3, it gets difficult for a human observer to distinguish between the original and composite 512×512 image, while embedding more than 4000 bits reliably.

The simplest SEC scheme is the zero-threshold SEC scheme, where the coefficients that are not quantized to zero, are used to embed information. Quantization embedding is performed as usual when embedding a '1'. If a '0' is to be embedded, the coefficients are quantized to even reconstruction values. However, if this results in quantization to zero, we leave it as such and the same '0' is embedded in the next coefficient satisfying the non-zero criterion. The decoder simply disregards all coefficients that quantize to zero. Otherwise, decoding is performed as usual.

High embedding rates are achieved using this zero-threshold SEC scheme with very low perceptual degradation, which resembles JPEG compression. To understand this intuitively, it should be noted that there are many image coefficients that are very close to zero once divided by the JPEG quantization matrix, and would be quantized to zero upon JPEG compression. Embedding '1' in such coefficients introduces a large amount of distortion relative to the original coefficient size, a factor that seems to be perceptually important. This is avoided by choosing not to use zeros for embedding.

IV. CODING FOR INSERTIONS AND DELETIONS

In the previous section, it was demonstrated that use of image adaptive criteria is necessary when hiding high volumes of data into images. As discussed in Section I, any embedding scheme that employs local perceptual criterion will suffer from insertion/deletion problems, causing the catastrophic loss of synchronization between encoder and decoder. In the ET scheme, insertions and deletions are observed when the attack quality factor is mismatched with the design quality factor for JPEG attack. However, there are no insertions or deletions for most of the images under matched or mismatched JPEG attacks, for the SEC scheme. Both the ET and SEC schemes have insertions/deletions under AWGN attacks.

A. Coding Framework

The bit stream to be hidden is coded, using a low rate code, assuming that all host coefficients that meet the global criterion will actually be employed for hiding. A code symbol is erased at the encoder if the local perceptual criterion for the block or coefficient is not met. Since we code over entire space, long codewords can be constructed to achieve very good correction ability. A minimum distance separable (MDS) code, like Reed Solomon

(RS) code, does not incur any penalty for erasures at the encoder. Turbo-like codes, which operate very close to capacity, incur only a minor overhead due to erasures at the encoder. It should be noted that a deletion, which causes an erasure, is half as costly as an insertion, which causes an error. Hence, it is desirable that the data-hiding scheme be adjusted in such a manner that there are very few (or no) insertions.

Thus, using a good erasure correcting code, one can deal with insertions/deletions without significant decline in original embedding rate. Reed Solomon codes [8] have been used for ET scheme and Repeat Accumulate codes [9] have been used for the SEC scheme as described in following sections.

B. Reed-Solomon (RS) coding for ET scheme

Reed Solomon codes [8] are MDS codes, such that any k coordinates of an (n, k) RS code can be treated as message positions. In other words, the k message symbols can be decoded even if any k symbols out of total n symbols sent are received at the decoder. The code can correct $(n-k)$ erasures, or half as many errors. The block length n of a Reed-Solomon code must be smaller than the symbol alphabet. Thus, the Reed-Solomon code operates over large nonbinary alphabets (each symbol can be interpreted as a block of bits), which matches the block-based ET scheme, where an entire block gets inserted or deleted. The code symbols should be interleaved in such a way that at least k of the n code symbols of a codeword are received at the decoder with high probability, under the erasures-only assumption. For example, if one whole codeword were placed in a smooth area of the image, all or most of the symbols would be erased, and it would be impossible to decode this particular codeword at the receiver.

Reed-Solomon codes are not well matched to AWGN channels (where they might more typically serve as an outer code for cleaning up after an inner code matched to the channel), but are ideal for the purpose of illustrating how to deal with the erasures caused by application of local criteria at the encoder and decoder. We now turn to the SEC scheme, where we consider powerful binary codes that are well-matched to AWGN channels, as well as close to optimal for dealing with erasures.

C. Repeat-accumulate (RA) coding for SEC scheme

Many turbolike codes such as low-density parity check (LDPC) codes by Gallager, repeat-accumulate (RA) codes and irregular repeat-accumulate codes (IRA) by Divsalar et. al. [9], [10], and certain others operate close to Shannon limit and can be used with SEC scheme. We used RA codes in our experiments because of their simplicity of decoding and near-capacity performance for erasure channels [10].

A rate $1/q$ RA encoder, as the name suggests, involves q -fold repetition, pseudorandom interleaving and accumulation of the resultant bit-stream. Decoding is performed iteratively using sum-product algorithm, as given in [11].

The unity-threshold SEC embedding was used which allows one to change the decoding method so as to favor

deletions compared to insertions. Moreover, the perceptual quality of the composite image is greatly improved, with a reduction in rate. The set of candidate coefficients, which governs the length of the RA code, lies within a designated low frequency band.

V. RESULTS

The use of perceptual criterion enables us to hide large volume of data without significant perceptual degradation. Due to the poor reproduction of images on paper, the reader is referred to our home page [7] for various examples of images with hidden data.

A. JPEG attacks

The decoder estimates the location of the embedded data, and uses hard decisions on the embedded bits in these locations. The bits in the remaining locations (out of the set of candidate frequencies) are set to erasures. Since the embedding procedure of both ET and SEC scheme is tuned to JPEG, the decoding of embedded data is perfect for all the attacks lesser than or equal to the design quality factor (QF). Table I shows the number of bits embedded (with perfect recovery) in uncoded and coded ET and SEC schemes at various design QFs, under JPEG attacks for 512×512 Lena image. It should be noted that, coded and uncoded SEC rates cannot be compared directly because zero-threshold SEC scheme is used when uncoded, and a unity-threshold SEC scheme is used when coded. The perceptual quality of the composite image is extremely good in the latter case.

QF	attack compr. (bpp)	ET scheme # of bits		SEC scheme # of bits	
		uncoded	coded	uncoded	coded
25	0.42	6,240	4,608	11,117	5,734
50	0.66	15,652	12,096	19,346	9,577
75	1.04	34,880	30,560	32,117	14,336

TABLE I
PERFORMANCE WITH JPEG ATTACK

B. AWGN attacks

The results for the ET scheme with RS coding against AWGN attacks are summarized in Table II. The number of bits embedded is listed for the 512×512 Lena image. Although the RS code is not the best choice for AWGN, it is adequate for mild attacks.

Results for the RA-coded SEC scheme with soft decisions using the statistics of the AWGN (as in the capacity computation in Section II-B) will be included in the final paper.

VI. CONCLUSIONS

The information theoretic analysis of scalar quantization based hiding reveals only a 2dB penalty from the optimal embedding scheme. Furthermore, Figure 1 indicates that

Attack DNR	# of bits	bits/pixel
1/3	4,352	0.0166
1/5	3,328	0.0127
1/6	1,536	0.0059

TABLE II
PERFORMANCE OF ET SCHEME UNDER AWGN ATTACK, QF=25

binary signaling is sufficient to achieve capacity in the low DNR region our embedding schemes operate in. A by-product of the information-theoretic analysis is the log likelihood ratio for AWGN attacks, which can be employed to generate (a table look-up for) soft information to be passed to the outer decoder. In previous work on iterative decoding for data hiding in a Gaussian host, the soft decisions were generated in ad hoc fashion [12].

A significant practical contribution of the paper is a powerful coding framework that allows flexibility in terms of the application of local criteria for determining where to embed data. The use of powerful errors and erasures codes enables an elegant solution to the synchronization problem between the encoder and decoder which arises due to locally adaptive embedding. We are able to hide large volumes of data, of the same order as the capacity estimates in [4]. However, a careful comparison with such information-theoretic estimates is not the focus of the present paper, and will be undertaken in future work after further refinement of the encoding and decoding strategies.

REFERENCES

- [1] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Transaction on Information Theory*, vol. 47, no. 4, pp. 1423–1443, May 2001.
- [2] M. C. Davey and D. J. C. Mackay, "Reliable communication over channels with insertions, deletions, and substitutions," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 687–698, Feb. 2001.
- [3] K. Solanki, N. Jacobsen, S. Chandrasekaran, U. Madhow, and B. S. Manjunath, "High-volume data hiding in images: Introducing perceptual criteria into quantization based embedding," To appear *Proceedings ICASSP*, May 2002.
- [4] P. Moulin and M. K. Mihcak, "The data-hiding capacity of image sources," Preprint, June 2001.
- [5] M. H. M. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. 29, no. 3, pp. 439–441, May 1983.
- [6] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding," Preprint, Jan. 2001.
- [7] "<http://vision.ece.ucsb.edu>," UCSB Vision Research Laboratory Web Page.
- [8] S. B. Wicker and V. K. Bhargava, *Reed-Solomon Codes and Their Applications*, IEEE Press, 1994.
- [9] H. Jin, D. Divsalar, and R. J. McEliece, "Coding theorems for turbo-like codes," in *36th Allerton Conference on Communications, Control, and Computing*, Sept. 1998, pp. 201–210.
- [10] H. Jin, A. Khandekar, and R. J. McEliece, "Irregular repeat-accumulate codes," in *Proceedings 2nd International Symposium on Turbo codes and Related Topics*, 2000, pp. 1–8.
- [11] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 498–519, Feb. 2001.
- [12] M. Kesal, M. K. Mihcak, R. Koetter, and P. Moulin, "Iteratively decodable codes for watermarking applications," in *Proc. 2nd Int. Symp. on Turbo Codes and Related Topics*, Sept. 2000.