

AN ANALYSIS OF QUANTIZATION BASED EMBEDDING-DETECTION TECHNIQUES

Husrev T. Sencar¹, Mahalingam Ramkumar², Ali N. Akansu¹

¹ New Jersey Institute of Technology
Department of Electrical and Computer Engineering
Newark, NJ 07102

e-mail: {*taha.sencar, ali*}@njit.edu

² Mississippi State University.
Department of Computer Science and Engineering
Mississippi State, MS 39762
e-mail: *ramkumar@cse.msstate.edu*

ABSTRACT

We analyze quantization based embedding and detection schemes in terms of the data hiding framework introduced in Refs. [1, 2]. This framework enables a better connection between analytical results and practical designs. We lay out the performance evaluation criteria and present comparison results for scalar quantization based data hiding techniques. Embedder-detector designs are evaluated based on three key issues. These are: 1) the type of post-processing employed at the embedder 2) the form of demodulation 3) the criteria used to optimize embedding-detection parameters. Data hiding methods are compared based on rate, correlation, and probability of error performance merits.

1. INTRODUCTION

The design principle that governs the operation of the embedder-detector pair is the most important characteristic of a data hiding method. Among a variety of research approaches the ones that draw a lot of attention are inspired from *communication with side information*. Costa in [3] assumed a communications scenario in which a side information about channel's state, that is in the form of a signal additive to the sent codeword, is made available at the encoder before the transmission of a message. Using the results of Ref. [4], Costa showed that for an additive white Gaussian noise (AWGN) channel with Gaussian input and side information, the channel capacity does not depend on the side information. When evaluated within the context of data hiding, these results encouraged researchers to devise practical oblivious data hiding methods that can achieve the hiding capacity. For this purpose, several implementations that utilize this approach are proposed [5, 6, 7, 8]. These techniques are characterized by the use of quantization procedures in order to design embedding-detection methods that

approximate the performance of Costa's optimal encoding-decoding.

Chen *et al.* in [5] provide a formal treatment of data hiding methods that use high dimensional quantization for embedding an information signal into a host (cover) signal, quantization index modulation (QIM). They also introduced distortion compensated version of QIM (DC-QIM), that can achieve the capacity under AWGN attacks. Similarly, Chou *et al.* in Refs. [9, 8], based on a duality with distributed source coding problem, implemented the exhaustive code-word generation of Costa's scheme by an optimization technique through the use of optimal quantizers.

In this research direction, the most popular embedding technique is a low complexity implementation of QIM which relies on uniform scalar quantization, dither modulation (DM) [5]. Ramkumar, *et al.* [6], considering scalar embedding, used a continuous triangular periodic function for extracting the embedded signal and also employed a thresholding type of processing at the embedder. In Ref. [7], Eggers, *et al.* optimized the performance of DC-DM by a more careful optimization of embedding parameters. They also combined multi-level signaling with binary coding techniques for low attack applications, and provided some performance results, [10]. Perez-Gonzalez, *et al.* [11] proposed a probability density function (pdf) transformation type of processing for embedding.

In this paper, we introduce performance evaluation criteria for quantization based data hiding methods in terms of the data hiding framework proposed in [1, 2]. The characteristics of a data hiding method is studied in three respects. These are the type of post-processing utilized at the embedder, the form of demodulation, and the criteria used to optimize the embedding-detection parameters. Various embedding-detection techniques are compared based on rate, correlation, and probability of error performance

results. In the next section, we revisit the proposed alternate framework based on channel adaptive encoding and channel independent decoding (CAE-CID). Section 3 investigates the performance evaluation issues for embedding-detection techniques. The performance results are provided in Section 4, and our conclusions are given in Section 5.

2. CAE-CID FRAMEWORK

Costa, [3], considered an AWGN channel with power constrained input \mathbf{X} and side information \mathbf{C} . A message index m is transmitted to the receiver by properly selecting the channel input \mathbf{X} that is additive to \mathbf{C} . Correspondingly, the channel output is defined as $\mathbf{Y} = \mathbf{X} + \mathbf{C} + \mathbf{Z}$ where \mathbf{Z} is the additive channel noise. Assuming \mathbf{X} , \mathbf{C} , \mathbf{Z} are independent, identically distributed (*iid*) length N sequences of random variables with zero covariance matrices and Gaussian marginal distributions (*i.e.* $X \sim \mathcal{N}(0, P)$, $C \sim \mathcal{N}(0, \sigma_C^2)$, $Z \sim \mathcal{N}(0, \sigma_Z^2)$), and considering an auxiliary variable \mathbf{U} with the design $\mathbf{U} = \mathbf{X} + \alpha\mathbf{C}$, $0 < \alpha < 1$, Costa showed that communication rate achieves $\frac{1}{2} \log_2(1 + \frac{P}{\sigma_Z^2})$ bits per transmission for $\alpha = \frac{P}{P + \sigma_Z^2}$. This is the capacity of an AWGN channel with no side information.

Consider the same communications scenario by modifying the channel input as $\mathbf{X}_n = \mathbf{X} - \mathbf{X}_t$ and the design for the auxiliary variable as $\mathbf{U} = \mathbf{X} + \mathbf{C}$ ($\alpha = 1$ for all the cases). \mathbf{X}_t is called the processing distortion and obtained as function of \mathbf{X} . The channel output, in this case, is defined as $\mathbf{Y} = \mathbf{C} + \mathbf{X} - \mathbf{X}_t + \mathbf{Z}$. Assuming, \mathbf{X}_t is an *iid* vector with the marginal $X_t \sim \mathcal{N}(0, \sigma_{X_t}^2)$ (\mathbf{X}_t is a linear function of \mathbf{X}), it can be shown that both scenarios yield the same channel capacity. Therefore, the two frameworks are equivalent and can be translated into each other by $\sigma_X = \frac{\sqrt{P}}{\sigma_Z}$.

An obvious difference between Costa's framework and CAE-CID framework is in how channel dependent nature reflects in the encoding-decoding operations. The channel dependency of \mathbf{U} , through α , in the former is shifted to the generation of codeword \mathbf{X}_n , through \mathbf{X}_t , in the latter. (It will next be shown that in practical data hiding methods \mathbf{X}_t actually represents the processing that follows the embedding quantization.) The encoding and decoding that delivers the channel capacity for both frameworks relies on random coding techniques. Simply, the encoder finds the \mathbf{U} sequence, out of a huge collection of \mathbf{U} sequences shared by both encoder and decoder, that yields the codeword orthogonal to \mathbf{C} and satisfying the power constraint P . At the decoder, on the other hand, the same \mathbf{U} sequence is searched based on joint typicality with the received \mathbf{Y} .

These results can be extended to data hiding by setting up dualities between the communications and data hiding frameworks. Within the context of data hiding, \mathbf{W} is an information signal corresponding to message index m ,

\mathbf{C} is the host signal, \mathbf{X} is the embedding distortion introduced to \mathbf{C} , \mathbf{X}_t is the distortion induced on \mathbf{C} due to some processing \mathcal{P} , $\mathbf{X}_t = \mathcal{P}(\mathbf{X})$, \mathbf{Z} is the attack on the stego signal $\mathbf{S} = \mathbf{C} + \mathbf{X} - \mathbf{X}_t$, and \mathbf{Y} is the distorted stego signal. The encoder-decoder pair is functionally equivalent to embedder-detector pair. However, the corresponding encoder-decoder structures cannot be applied to practical embedder-detector designs due to complexity issues, since the former is simply a brute search over a huge collection of \mathbf{U} sequences. Finally, the power constraint on the codeword is dual to the Euclidean distance between \mathbf{S} and \mathbf{C} .

In quantization based methods, the optimal encoding-decoding procedure is effectively simplified by generating \mathbf{U} sequences, as sequences of reconstruction points selected from a set of quantizers each of which is uniquely described by a set reconstruction points that are non-overlapping with other sets. The number of quantizers in the set corresponds to number of message (code) letters. Accordingly, the embedding operation is the quantization of \mathbf{C} vector with the quantizer(s) pointed by the message signal \mathbf{W} to be embedded, and then processing the resulting quantized signal by a choice of (post-processing) function. Hence, input \mathbf{X} in the CAE-CID framework is the distortion introduced to \mathbf{C} due to embedding quantization, and the processing distortion \mathbf{X}_t is the result of processing \mathcal{P} . The detection of the sent message, on the other hand, is by determining the nearest reconstruction point(s) to the received signal \mathbf{Y} , and generating the message by mapping the corresponding quantizer(s) to the message letters they are associated with.

3. PERFORMANCE EVALUATION

A quantization based embedding-detection technique can be evaluated based on three key characteristics.

3.1. Type of post-processing

Three forms of post-processing have been proposed. These are:

- distortion compensation, [12, 7]
- thresholding, [6]
- Gaussian mapping [11].

In Ref. [12], Chen *et al.* introduced distortion compensation type of processing, DC-QIM, by subtracting $(1 - \alpha)$ scaled version of embedding distortion \mathbf{X} from quantization index modulated signal. Hence, for distortion compensation processing $\mathbf{X}_t = (1 - \alpha)\mathbf{X}$ and $\mathbf{X}_n = \alpha\mathbf{X}$. Ramkumar *et al.* [6] proposed thresholding type of post-processing by thresholding the maximum amount of distortion to $\pm \frac{\beta}{2}$. Therefore, $\mathbf{X}_t = \max(0, |\mathbf{X}| - \frac{\beta}{2})\text{sign}(\mathbf{X})$ and $\mathbf{X}_n = \min(|\mathbf{X}|, \frac{\beta}{2})\text{sign}(\mathbf{X})$. Similarly, Perez-Gonzalez *et*

al. in Ref. [11] proposed Gaussian mapping as the post-processing. They generated \mathbf{X}_t by transforming \mathbf{X} into a zero mean Gaussian random variable with variance σ_V^2 .

It's shown in [1] that when \mathbf{X} is Gaussian distributed, distortion compensation is the optimal processing. However, for other distributions of \mathbf{X} , the optimal processing is a function of dependency between \mathbf{X} and \mathbf{X}_t and noise level σ_Z^2 . Therefore, for high-dimensional quantization where \mathbf{X} approaches Gaussian distribution, distortion compensation will perform better. For scalar quantized case, like DM, where \mathbf{X} is uniformly distributed the optimum processing varies with channel noise level.

3.2. Form of demodulation

A message is hidden into a host signal by embedding the signal \mathbf{W} pointed by the message index. Correspondingly, detection of the sent message is either by sample-wise hard decisions or soft decisions depending on the availability of collection of \mathbf{W} messages at the detector side. Two forms of detectors are employed by practical methods. These are the minimum distance detector and the maximum correlation detector.

When the message set is present, an improved detection is possible as the sent message is restricted to be a member of the set. In this case, detector determines the sent message by the minimum distance of the received signal to the set of message signals. The message yielding the smallest distance is deemed the sent message [5]. Alternately, decoder can extract $\hat{\mathbf{W}}$ (distorted version of \mathbf{W}) and compute the correlations with the set of message signals [6]. The message signal \mathbf{W} that has the highest correlation with the extracted signal is declared the sent message.

If the detector has no access to the message set, then each component of \mathbf{W} is decoded by minimum distance decoding [7, 11]. Then the decoded set of values are combined to generate the sent message.

3.3. Optimization Criteria for Parameters

In quantization based methods, embedding and detection operations are parameterized by two variables. One is the quantization step size Δ which sets the distance between the reconstruction points of the quantizers. The other parameter is the one that controls the amount of post-processing applied on the quantized signal in order to generate the stego signal. This latter may take the form of scaling factor α for distortion compensation processing, β for thresholding processing, and σ_V for the Gaussian mapping processing. Both parameter values are interdependent and are functions of the embedding distortion, P , and the channel noise level, σ_Z^2 .

The problem now reduces to computation of the parameter values for a given P and σ_Z^2 . Since embedder-detector operations are known, and the attack statistics are given (*i.e.*

AWGN), the effective noise at the detector that distorts the embedded \mathbf{W} can be derived [1]. In other words, \mathbf{W} and $\hat{\mathbf{W}}$ can be probabilistically related to each other by modeling the noise $\hat{\mathbf{W}} - \mathbf{W}$ for the given channel noise statistics. Consequently, the optimization for the parameters can be based on different performance criteria.

- *SNR* – $\sigma_X^2 / (\sigma_{X_t}^2 + \sigma_Z^2)$ [5]: The parameter values can be selected to maximize the ratio of embedding distortion to sum of processing distortion and channel distortion. This can be interpreted as the maximization of signal-to-noise ratio at the detector where signal is the quantization noise and the noise is the deviation signal from the quantized values.
- *Correlation* [6]: As the noise that distorts the embedded message signal can be modeled, the parameter values can be selected to maximize the correlation between \mathbf{W} and $\hat{\mathbf{W}}$, $\frac{\mathbf{W}\hat{\mathbf{W}}}{|\mathbf{W}||\hat{\mathbf{W}}|}$.
- *Probability of error* [11]: The fact that each message letter is assigned to a different quantizer, or equivalently to reconstruction points associated with a quantizer, can also be considered as a signaling scheme that uses a periodic signal constellation. Using the statistics of the effective noise at the detector, the parameter values can be chosen to minimize the error probability at the given channel noise level.
- *Mutual information* [7]: Similarly, if the conditional probability $p(\mathbf{Y}|\mathbf{W})$ can be calculated, then the hiding rate can be obtained by computing the mutual information between \mathbf{Y} and \mathbf{W} for a given distribution of \mathbf{W} . Correspondingly, the embedding and detection parameters can be selected to maximize the hiding rate.

4. PERFORMANCE RESULTS

Fig. 1 displays the capacity and the hiding rates for various methods. Additive embedding and quantization based DM with no processing performs poorly on the two extremes, respectively for very high and very low embedding power to channel noise power ratios, WNRs. On the other hand for midrange WNR values, DM with post-processing is able to compensate for the inferior performance offered by additive scheme and DM. Thresholding and distortion compensation processings perform closely in the whole WNR range, and Gaussian mapping processing has a comparable performance only for WNRs higher than -8 dB. The normalized correlation, ρ , and probability of error, P_e , performances for quantization based methods are respectively given in Figs. 2 and 3.

The relative performances of the three post-processing functions obtained for the rate, normalized correlation, and

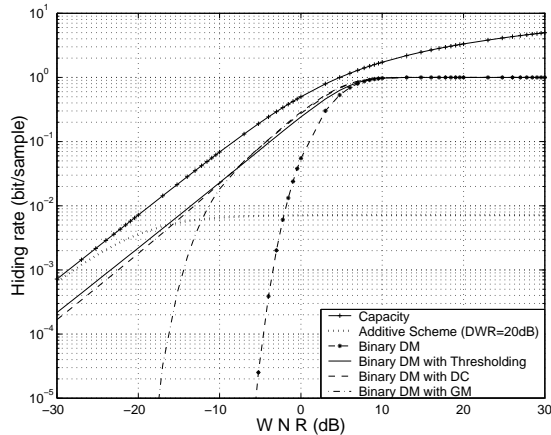


Fig. 1. Comparison of the hiding rates corresponding to various hiding methods considering binary signaling obtained for $P = 10$ where DWR is the $\frac{P}{\sigma_c^2}$ ratio in dB.

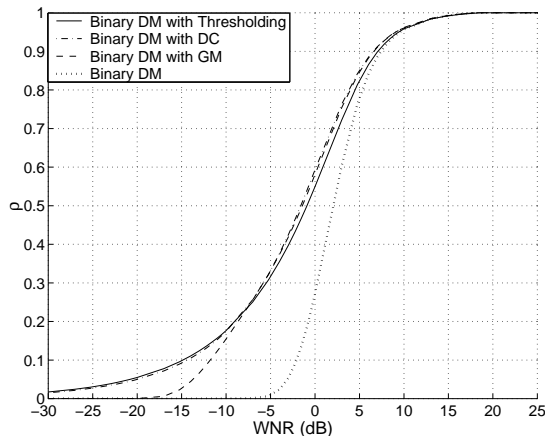


Fig. 2. The normalized correlation between \mathbf{W} and $\hat{\mathbf{W}}$ for the considered hiding methods when $P = 10$.

probability of error criteria are in accordance with each other. Thus, thresholding performs better when WNR is below approximately -9 dB, and at higher WNRs distortion compensation and Gaussian mapping have better performances.

5. CONCLUSIONS

In this paper, we have shown how CAE-CID framework links the practical embedder-detector designs. From this unified point of view, we identified the characteristics of quantization based methods that enable a better evaluation of a given method. We also compared performances of various methods using different metrics over a range of -30 dB to 30 dB, and shown how the use of post-processing functions improves the performance in the midrange WNRs.

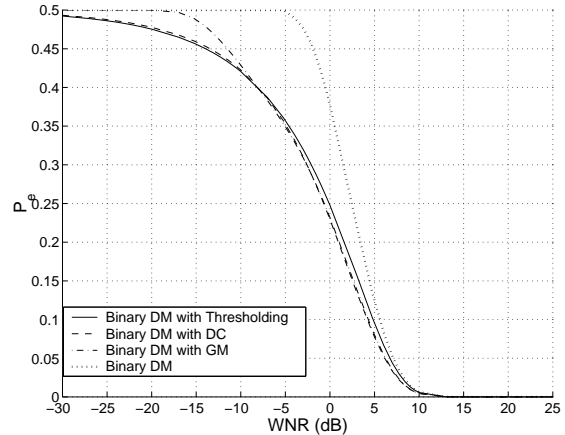


Fig. 3. The probability of error in detecting W for the considered hiding methods when $P = 10$.

6. REFERENCES

- [1] H. T. Sencar, M. Ramkumar, and A. N. Akansu, "An overview of scalar quantization based data hiding methods," *submitted to IEEE Transactions on Signal Processing*.
- [2] H. T. Sencar, M. Ramkumar, and A. N. Akansu, "A new perspective for embedding-detection methods with distortion compensation and thresholding processing techniques," in *Proc. of IEEE-ICIP Conference*, 2003.
- [3] M. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. 29, pp. 439–441, 1983.
- [4] S. I. Gelfand and M. S. Pinsker, "Coding for channel with random parameters," *Problems of Control and Information Theory*, vol. 9, no. 1, pp. 19–31, 1980.
- [5] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423–1443, May 2001.
- [6] M. Ramkumar and A. N. Akansu, "Self-noise suppression schemes for blind image steganography," in *Proc SPIE International Workshop on Voice, Video and Data Communication, Multimedia Applications*, Sept. 1999, vol. 3845.
- [7] J. J. Eggers, J. K. Su, and B. Girod, "A blind watermarking scheme based on structured codebooks," *IEE Colloq. Secure Images and Image Authentication*, vol. 4, pp. 1–6, Apr. 2000.
- [8] J. Chou, S. S. Pradhan, L. E. Ghaoui, and K. Ramchandran, "A robust optimization solution to the data hiding problem using distributed source coding principles," in *Proc SPIE: Image and Video Communications and Processing*, 2000, vol. 3974.
- [9] J. Chou, S. S. Pradhan, L. E. Ghaoui, and K. Ramchandran, "On the duality between data hiding and distributed source coding," in *Proc. of 33rd Annual Asilomar conference on Signals, Systems, and Computers*, 1999.
- [10] J. J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, "Scalar costea scheme for information embedding," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 1003–1019, 2003.
- [11] F. Perez-Gonzalez, F. Balado, and J. R. Hernandez Martin, "Performance analysis of existing and new methods for data hiding with known-host information in additive channels," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 960–980, 2003.
- [12] B. Chen and G. Wornell, "Preprocessed and postprocessed quantization index modulation methods for digital watermarking," in *Proc SPIE: Security and Watermarking of Multimedia Contents II*, 2000, vol. 3971, pp. 48–59.