A PRACTICAL LATTICE QIM METHOD: TCQ-IS

Ersin Esen[1,2] and A. Aydın Alatan[1]

[1]Department of Electrical and Electronics Engineering, METU, Ankara Turkey
[2]Tübitak Bilten, Balgat 06531 Ankara Turkey
email: ersin.esen@bilten.metu.edu.tr, alatan@eee.metu.edu.tr
web: http://mmrg.eee.metu.edu.tr

ABSTRACT

Designing practical methods that target achieving the ideal data hiding capacity is one of the main foci of data hiding field. High dimensional quantization enables to narrow the gap between ideal and actual capacities. However, computational complexity becomes a prohibitive factor. Lattice based quantization appears to be a good candidate for practical solutions. In this paper, it is shown that TCQ-IS, a previously proposed data hiding method, constitutes a practical method for lattice quantization based data hiding.

1. INTRODUCTION

Oblivious/blind data hiding from communications perspective can be interpreted as in Figure 1, where *m* is the data to be hidden, *s* is the stego/host signal (side information), *x* is the stego signal, *y* is the stego signal after the channel, and finally $\underline{m}$ is the extracted data.

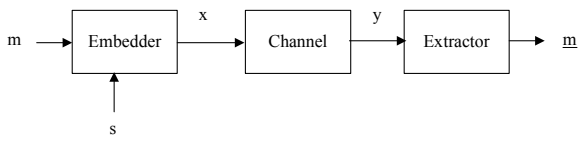

Figure 1. Data hiding as a communication problem.

The similarity of data hiding problem with communication with side information at the transmitter problem led to insightful observations. With the assumption of modelling the channel as an additive independent Gaussian noise term, the channel capacity for power limited stego signal and this channel can be given by [1]

$$C = \frac{1}{2}\log_2\left(1+\frac{P_x}{\sigma_n^{\,2}}\right). \qquad (1)$$

Eq.(1) indicates that channel capacity is independent of the side information power and it is equal to the case where side information is also available at the extractor. Hence, oblivious data hiding schemes that achieve the ideal capacity limit can be devised. In this respect Quantization Index Modulation [2] forms a theoretical basis for practical methods that try to achieve this ideal limit. QIM basically corresponds to a quantization process, in which the quantizers are modulated according to the message, while the extraction is performed by minimum distance decoding. Various QIM based methods are proposed [4] with the aim to find practical ways to get close to the ideal channel capacity.

2. LATTICE QIM

In QIM framework, N-dimensional Vector Quantization (VQ) can be employed as well as scalar quantization. However, the design and computational complexity of high dimensional quantization can be prohibitive. In that respect, structured schemes can be helpful and hence lattices can be employed for this purpose. First of all, the lattices will be described briefly (for a complete description, refer to [3]). Then, lattice QIM [4] concept will be summarized.

2.1 Lattice

An N-dimensional lattice, Λ, is a discrete subgroup of the Euclidean space R^N with addition operation. That is,

$$\lambda_1 \in \Lambda \text{ and } \lambda_2 \in \Lambda \rightarrow \lambda_1 \pm \lambda_2 \in \Lambda.$$

Λ can be defined using an NxN dimensional generator matrix G (which is non-unique):

$$\Lambda = \{\lambda = Gx: x \in Z^N\}.$$

A coset of Λ is defined as a translated version of it:

$$x \in R^N \rightarrow x + \Lambda \text{ is a coset.}$$

For quantization modulation, nested lattices are used. In order to obtain a nested-lattice pair, a sublattice, $\Lambda`$, of $\Lambda$ is formed. The generator matrix of $\Lambda`$, G`, is obtained by subsampling G:

$$G`=JG,$$

where J_{NxN} is the sampling matrix. There are det(J) number of cosets of $\Lambda`$, whose union form Λ:

$$\Lambda = U_{m=0}^{\det(J)-1} \Lambda`_m ,$$

where $\Lambda`_m$ is a coset of $\Lambda`$. A sample of nested lattices is shown in Figure 2, where nine cosets of $\Lambda`$ (represented by the big hexagonal) form Λ (represented by small hexagonals).

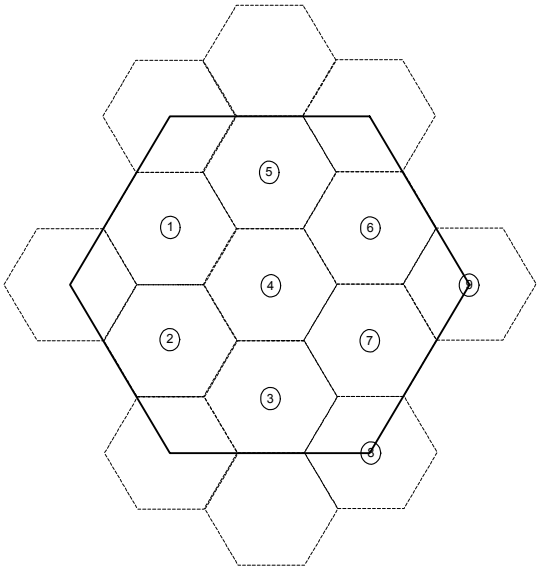

Figure 2. A sample of 2D Nested Lattices.

Quantization in a lattice can represented by a quantization function $Q_\Lambda(x)$, which maps each $x \in R^N$ to the nearest point in Λ. Using this quantization, the fundamental Voronoi cell of Λ can be defined as,

$$V = \{x \in R^N : Q_\Lambda(x)=0\}.$$

2.2 Lattice QIM [4]

A nested lattice pair is employed and QIM is performed over this pair. Embedder and extractor also use the same pair.

Each message $m \in \{0,..,det(J)-1\}$ is associated with a coset Λ_m of $\Lambda`$. Embedding is performed by quantizing the input s to the nearest point in Λ_m:

$$\underline{x}(m) = Q_{\Lambda_m}(s). \quad (2)$$

After the channel, the noisy stego data, y, is obtained and extraction is performed by minimum distance decoding:

$$m = \text{argmin}_m\, d(y, \Lambda_m), \quad (3)$$

where d(.,.) is any suitable distance metric.

Equations (2) and (3) represent the lattice QIM embedding and extraction, respectively.

The nested lattice pair should be designed so that the fundamental requirements of data hiding, imperceptibility and robustness, are met. In order to improve imperceptibility, Q_Λ should be a good VQ, that is V should be as spherical as possible [4]. On the other hand, for improving robustness, cosets should be as far as possible [4].

3. TCQ-IS

TCQ-IS [5], [6] is a Trellis Coded Quantization (TCQ) [7] based data hiding method. The redundancy in the selection of the initial state is exploited to hide the data. A sample embedding is shown in Figure 3 [6]. The initial state is selected according to the message (0,1) and input data of length three is quantized, for which the trellis path (shown in bold) is determined by Viterbi Algorithm. The number of hidden data bits depends on only the number of the states. Increasing the length of the input sequence is shown to improve the robustness [5].

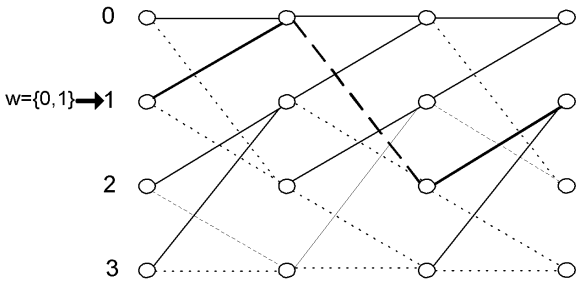

Figure 3. A TCQ-IS Embedding Sample.

The extraction is performed by trying each initial state and deciding on the one with minimum distance.

3.1 2D Case

Analyzing TCQ-IS in 2D discloses it as a lattice QIM method. For this purpose, 4-state Ungerboeck state machine and a uniform codebook for the TCQ structure, as in [6], will be used. Hence, the explored 2D case is composed of two input samples (and two stages of trellis), four subsets (each containing two codewords) in the codebook, and two message bits to identify the initial state.

With respect to the initial state, the set of output codewords differ. For initial state 0, the possible output codewords are $\{D_0, D_0\}$, $\{D_0, D2\}$, $\{D_2, D1\}$, $\{D_2, D_3\}$. The constellation diagram for all initial states is depicted in Figure 4. The horizontal axis denotes the first input sample and the vertical axis denotes the second input sample. The possible outputs for each initial state are shown using the corresponding index {0,1,2,3}.

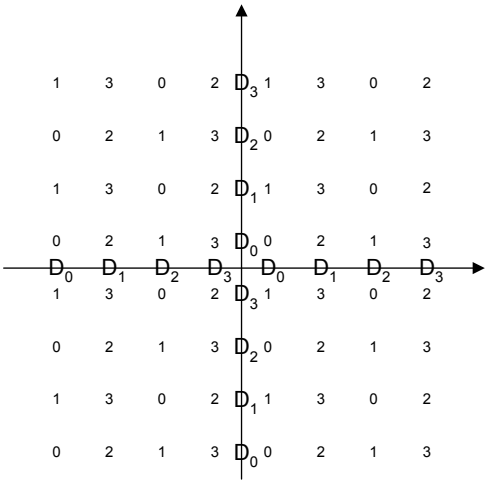

Figure 4. 2D Constellation of TCQ-IS.

Figure 4 illustrates that for 2D case, TCQ-IS is a lattice QIM with an alternating cubic lattice. The generator matrices can be determined as (neglecting the axis offsets):

$$G = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \& \; G' = \begin{bmatrix} 2 & 0 \\ 1 & 2 \end{bmatrix}.$$

G is equal to the identity matrix, since Λ is equal to Z^2. The subsampling matrix J is equal to G` and det(J) is four. Hence, the union of four cosets form Λ. As a different observation, the constellation in Figure 4 is a typical coset code [8].

The performance of TCQ-IS should be analyzed from two perspectives: embedding distortion (i.e. imperceptibiliy) and probability of error (i.e. robustness).

3.1.1Embedding Distortion

The quantization cells in Figure 4 are hexagonal. This way V is closer to spherical with respect to 2D uniform quantizer. By a simple error analysis, for uniform source and a fixed quantization cell with, Δ, the ratio of quantization MSE for uniform quantizer and TCQ is found out to be constant, being equal to

$$\mathrm{MSE}_{\mathrm{TCQ}}(\Delta) / \mathrm{MSE}_{\mathrm{uniform}}(\Delta) = 0.969 \qquad (4).$$

Eq. (4) states that quantization error is independent from Δ and 2D TCQ-IS has a lower embedding distortion with respect to a 2D Dither Modulation (DM) with scalar uniform base quantizer [2]. This fact is empirically verified and shown in Figures 5 and 6, for uniform (between –10 and 10) and Gaussian (zero mean and 10 variance) sources, respectively. The codebooks are enlarged to cover all of the input range, since we are not restricted with the bit allocation. The solid lines in Figures 5 and 6 represent 2D TCQ-IS embedding distortion and the dots represent 2D DM embedding distortion. The figures 5 and 6 verify the validity of Eq. (4).

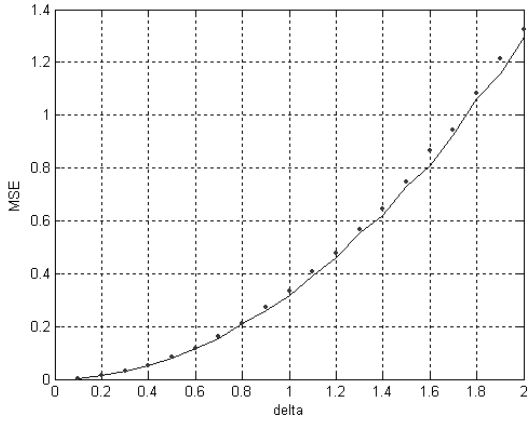

Figure 5. Embedding Distortion For Uniform Source (-10,10).

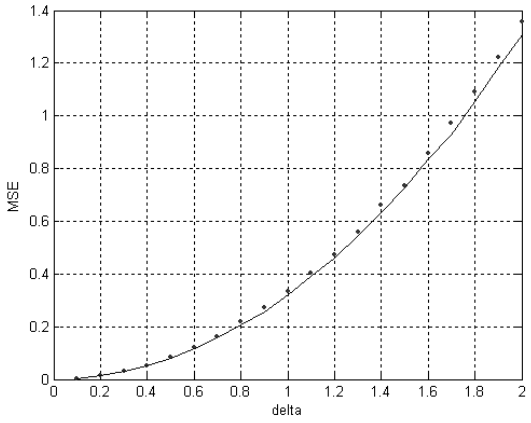

Figure 6. Embedding Distortion For Gaussian Source (0,10).

3.1.2Probability of Error P(E)

The channel codewords (the points of Λ) are distributed regularly, which is identical to 2D uniform DM. Hence, the same level of channel noise results in the same probability of error performance.

As a result, watermark-to-noise-ratio (WNR) versus P(E) analysis, that encapsulates both imperceptibility and robustness, indicates that TCQ-IS has a better performance than 2D DM. Figures 7 and 8 display P(E) vs. Watermark-to-Noise-Ratio(WNR) characteristics for uniform (between –10 and 10) and Gaussian (zero mean and 10 variance) sources, respectively. The solid lines represent TCQ-IS and dashed lines represent DM. The codebooks are enlarged to cover all of the input range. The channel noise (Gaussian with zero mean and 0.5 variance) is kept constant and embedding distortion (i.e. the watermark power) is varied. P(E) is computed as the average of 5000 random experiments. The results indicate that TCQ-IS and DM have similar performances. Although in the transition region DM is slightly better than TCQ-IS, the latter reaches zero error earlier (i.e. with a lower embedding distortion) than the former.

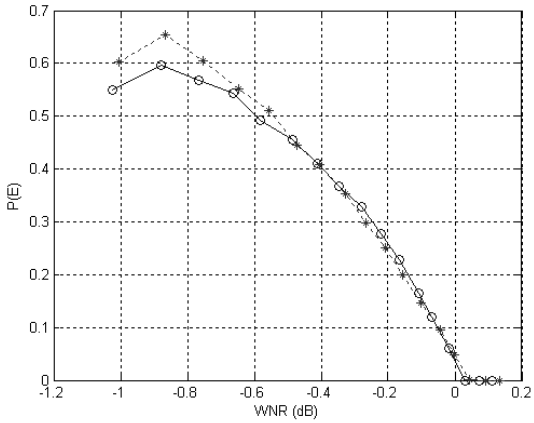

Figure 7. P(E) vs. WNR for Uniform Source (-10,10).

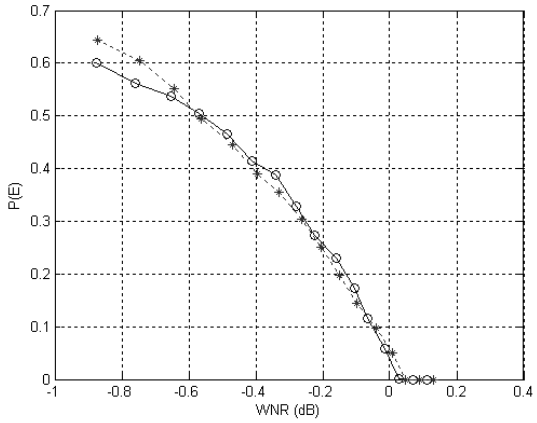

Figure 8. P(E) vs. WNR for Gaussian Source (0,10).

3.2 3D Case

The same TCQ structure in Section 3.1 is used. In this case, three input samples (i.e. a trellis with three stages) are employed. The 3D constellation is shown in Figure 9. Square, star, diamond, and circle represent the four sublattices, Λ_m.

In 3D, Λ is a subgroup of Z^3 and hence G is different than the identity matrix. The order of Z^3/Λ partition is given in Eq. (5).

$$|Z^3/\Lambda| = 4^3/(4x2^3) = 2 \qquad (5).$$

In the denominator of Eq.(5), the term 2 is due to the number of trellis branches that are leaving a state and the multiplier 4 in front of it is due the number of initial states. Eq. (5) states that Λ fills Z^3 with a density ½. In order to obtain a density of 1 with four codewords, one should use an eight state trellis.

Similarly, the order of $Z^3/\Lambda`$ partition is $|Z^3/\Lambda`|=4^3/(2^3)=8$. Hence, $|\Lambda/\Lambda`|=4$ which is equal to det(J). As dictated by the TCQ structure, the union of four cosets of $\Lambda`$ form Λ.

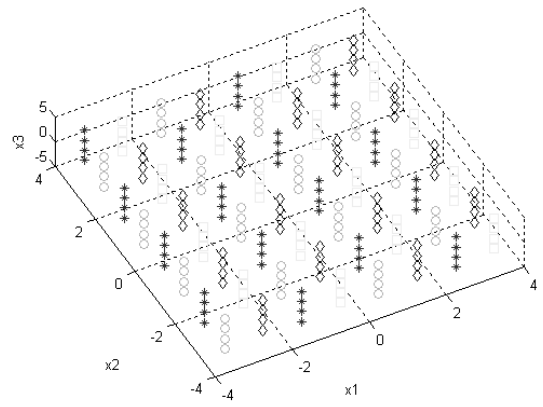

Figure 9. 3D Constellation of TCQ-IS.

3.3 Multi-D Case

$Z^N/\Lambda/\Lambda`$ is a partition chain. The partition orders are $|Z^N/\Lambda|=4^N/(4x2^N)=2^{N-2}$ and $|Z^N/\Lambda`|=4^N/2^N=2^N$. The order $|\Lambda/\Lambda`|$ is always four for all N due to the same TCQ structure used in all dimensions. In other words, for any dimension N, the selection of the initial state in TCQ yields a coarse lattice, whose cosets form the fine lattice. This nested lattice pair can be used for data hiding by only selecting the initial state in TCQ. The coarse lattice $\Lambda`$ determines the embedding distortion. The fine lattice Λ, whose members can be interpreted as the channel codewords, is related to the P(E) performance of the data hiding system.

4. CONCLUSION

It is shown that TCQ-IS constitutes a practical lattice QIM method. Since, it does not introduce any additional complexity to TCQ, it is practically feasible and can be extended easily to higher dimensions. The additional burden is only in the extraction stage; in which all initial states should be tried.

Although, it is shown here that TCQ-IS is a practical lattice QIM method, more rigorous theoretical analysis is needed in order to obtain guidelines to design the TCQ structure. The TCQ structure should be designed to fulfil the trade-off between the robustness and imperceptibility. The guidelines for this purpose still remains as an open issue.

REFERENCES

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

[2] B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," *IEEE Trans. Inform. Theory*, vol. 47, no.4, May 2001.

[3] J. H. Conway and N. J. A. Sloane, Sphere Packings, Lattices, and Groups. New York: Springer-Verlag, 1988.

[4] P. Moulin and R. Koetter, "Data-Hiding Codes," to be published, Oct. 2004.

[5] E. Esen, A. A. Alatan, and M. Askar, "Trellis Coded Quantization for Data Hiding," *EUROCON 2003*, Ljubljana, Slovenia, September 22-24 2003.

[6] E. Esen and A. A. Alatan, "Data Hiding Using Trellis Coded Quantization", *IEEE ICIP 2004*, Singapore, 24-27 October 2004.

[7] M.W. Marcellin and T.R. Fischer, "Trellis coded quantization of memoryless and Gauss-Markov sources," *IEEE Transactions on Communications*, vol. 38, pp. 82–93, January 1990.

[8] G. D. Forney, "Coset Codes – Part I: Introduction and Geometrical Classification," *IEEE Trans. Inform. Theory*, vol.34, no.5, pp.1123-1151, September 1988.