DATA HIDING USING TRELLIS CODED QUANTIZATION[1]

Ersin Esen[2,3] and A. Aydın Alatan[2,3]
[2]Department of Electrical and Electronics Engineering, M.E.T.U.
[3]TÜBİTAK BİLTEN, Balgat 06531 Ankara TURKEY

ABSTRACT

Information theoretic tools lead to the design and analysis of new blind data hiding methods. A novel quantization-based blind method, which uses trellis coded quantization, is proposed in this manuscript. The redundancy in initial state selection during trellis coded quantization is exploited to hide information as the index of this initial state. This index is recovered at the receiver by Viterbi decoding after comparison with all initial states. The performance of the proposed method is compared against other well-known approaches via simulations and promising results are obtained. Based on these results, the proposed method can be preferred in certain applications with high distortion attacks.

1. INTRODUCTION

In the early stages of data hiding, mostly *informed detection (private watermarking)* has been examined, compared to *blind detection (public watermarking)*. Although, the former problem intuitively appears to be simpler than the latter, some recent developments based on information theoretic tools [1], caused blind detection problem to attract more attention. Costa's paper [2] is one of the most remarkable works, which results in the analysis and design of novel blind detection methods. Costa shows the equality between the capacity of a communication system with side information available only to encoder and that of the system with side information available to both encoder and decoder [2]. Hence, it is possible to devise public watermarking systems achieving the same capacity with private systems.

Inspired by the information theoretic tools, many public watermarking algorithms are developed and analyzed [3-6]. Chen et.al. [3,4] has introduced Quantization Index Modulation (QIM), as a generic class of data hiding methods. QIM embeds data into cover content using quantization. Different quantizers are used for different watermarks or data; i.e. quantizers are modulated according to the data. At the decoder, the hidden data is decoded using the knowledge of the QIM structure employed at the encoder; hence, the original content is not required. Other public data hiding method based on quantization are proposed in [5,6]. In a slightly different approach, Chou et.al. [7] use quantization after trellis coded modulation as a consequence of the observation of the duality between source coding and channel coding with side information.

In this paper, we propose yet another quantization-based public data hiding method. The method is mainly based on Trellis Coded Quantization (TCQ), which is described briefly in Section 2. The proposed method is presented in Section 3, as well as two other quantization based methods. An algorithm that utilizes the proposed method to embed hidden information into the images is also described in Section 4. Following the simulations in Section 5, the concluding remarks are given in Section 6.

2. TRELLIS CODED QUANTIZATION

TCQ [8] can be considered as a special case of trellis coding. The main ideas behind TCQ are due to trellis coded modulation (TCM) [9]. TCQ employs a set of trellises and set partitioning ideas of TCM in order to achieve better distortion performance with low complexity.

TCQ uses a trellis and an associated codebook. A sample trellis of 4 states is shown in Figure 1, in accordance with its finite state machine and the codebook. In this figure, u is the input bit of the finite state machine, s_1, s_0 are the states, and o_1, o_2 are the outputs of this machine. The smooth lines in the trellis correspond to $u=0$ and the dashed lines correspond to $u=1$. Each branch of the trellis is associated with a subset D_i of the codebook, whose index i is determined by the output of the finite state machine. In order to design the codebook of TCQ, a scalar codebook C of size $2^{R+\acute{R}}$ is taken. R is the encoding rate and $\acute{R}$ represents the number of bits that specify the particular codeword in the selected subset. For the sample system in Figure 1, R is 2 bits per sample (bps), whereas $\acute{R}$

[1] This work is partially supported by TÜBİTAK under project EEEAG 101E007

is equal to 1. For an encoding rate of 2 bps, C is twice larger than the corresponding scalar quantizer. After C is determined, it is partitioned into $2^{\acute{R}+1}$ subsets, each of which has 2^{R-1} codewords.

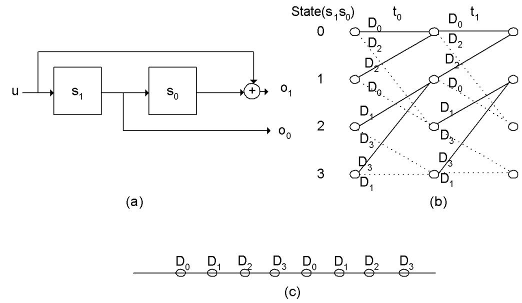

Fig. 1. A typical 4-state TCQ structure.

In order to quantize an input sequence s of length m, a trellis of m stages is used. Viterbi algorithm is used to find the closest path to s among all possible trellis paths. $m(R-\acute{R})$ bits specify the trellis path and $m\acute{R}$ bits specify the codeword in the selected subset. Although initial state selection is completely arbitrary, this state is generally selected as 0, since for long data sequences ($m>>log_2N$, where N is the number of states) the effect of the initial state on Mean Square Error (MSE) is negligible [8].

3. QUANTIZATION-BASED DATA HIDING

In addition to the proposed method, two other well-known methods, Dither Modulation (DM) and TCQ-Path Selection (TCQ-PS), are also briefly described in this section.

3.1.Proposed Data Hiding Method : TCQ-IS

The proposed method makes use of TCQ while considering the effects of the initial state (IS) on MSE. Since initial state selection is arbitrary in TCQ, one can embed information into the content by enforcing the selection of the initial state, accordingly.

After enforcing the selection of the initial state according to the data to be hidden, the closest trellis path is found using Viterbi algorithm, as in conventional TCQ.

Figure 2 shows a sample embedding process for TCQ-IS. In this illustrated example, $N=4$, $m=3$, $R=2$, $\acute{R}=1$. Since N is 4, one can hide 2 bits into the m input samples. Assuming, the data to hide is arbitrarily selected as $w=\{0,1\}$, state 1 is chosen as the initial state. The corresponding closest path found by the Viterbi algorithm is shown with thicker branches.

The total number of bits that can be hidden by TCQ-IS is log_2N, which depends only on the number of states in the trellis. Embedding rate of TCQ-IS is log_2N/m bps. For a given m, one should use trellises with more states in order to hide more data.

In the decoding stage, all N states are considered as the candidate initial states. For each candidate initial state Viterbi algorithm is executed for the received input vector. The computed MSE values are stored and the initial state with minimum MSE gives the desired embedded data, as the index of the corresponding state.

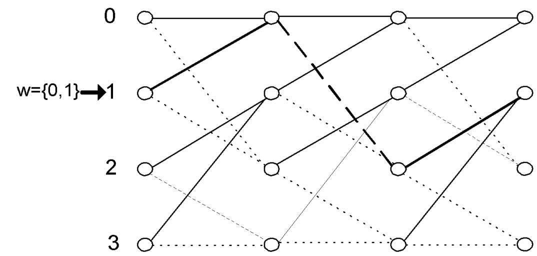

Fig. 2. A TCQ-IS sample.

It should be noted that the embedding distortion due to information hiding is mainly determined by the bin widths of the quantizer (Fig. 1), similar to other methods.

3.2. Dither Modulation (DM)

DM is a member of the QIM family. DM employs a quantizer set in which the quantization cells and the reconstruction points are the shifted versions of any other quantizer in the set [3]. The dither vector d is modulated with the watermark w. Then, using the corresponding dither vector for a given w, the embedding function is,

$$x(s,w) = q(x + d(w)) - d(w),$$

where q is the selected base quantizer. A uniform quantizer with step size Δ is used as the base quantizer. The dither vectors are $-\Delta/4$ and $+\Delta/4$ for $w=0$ and $w=1$, respectively. The hidden data is decoded by computing the distance between the reconstruction levels of each quantizer in the set. The index of the quantizer with the minimum distance gives the decoded data. According to the desired embedding rate, input data s can be used individually or sequentially in conjunction with majority voting in the decoding stage.

3.3.TCQ-PS

TCQ-PS is based on the TCM-TCQ scheme described in [5,6]. Using the same trellis structure in TCQ-IS, the coset selection in which the input signal s is to be quantized reduces to the trellis path determination according to the data w. Once the path is determined, s is quantized using the corresponding D_i. In that sense, TCQ-PS is also a member of QIM family. However, in this case, the quantizers are selected according to a trellis. Figure 3 shows a sample for TCQ-PS. The trellis path is determined with respect to the data $w=\{0,1,1\}$ starting always from the initial state 0. The data is quantized using the associated subsets of the branches in the order dictated by the trellis. In this scheme, embedding rate is 1 bps. At the decoding side, Viterbi algorithm is used to quantize the received signal using the trellis structure. Once the best path is found, the data is decoded starting from the initial state 0.

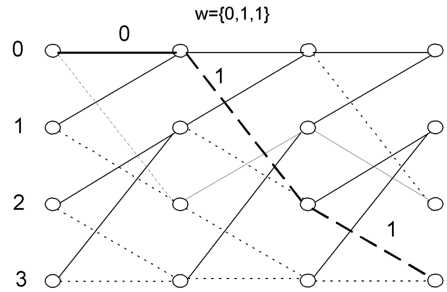

Fig. 3. A TCQ-PS sample.

4. IMAGE DATA HIDING BY TCQ-IS

TCQ-IS described in Section 3.1 is applied to images after transform domain conversion. For this purpose, the image is partitioned into blocks and for each block, Discrete Fourier Transform (DFT) is performed. The coefficients, for which TCQ-IS will be applied, are selected from the middle frequency band, as shown in Figure 4. The low frequency coefficients are not included, since modifications on these coefficients will be more visible. The high frequency band is also not considered, since the coefficients in this band are expected not to survive compression. The magnitudes of the selected mid-frequency DFT coefficients are fed into TCQ-IS. Resulting quantized values are replaced with the originals and finally, the cover image is obtained.

The decoder uses the same set of coefficients and extracts the hidden bits after the Viterbi decoding. Figure 4 shows a typical cover image (gray level *Lena* of size 512x512) with embedding distortion (PSNR between original and cover image) of 43dB.

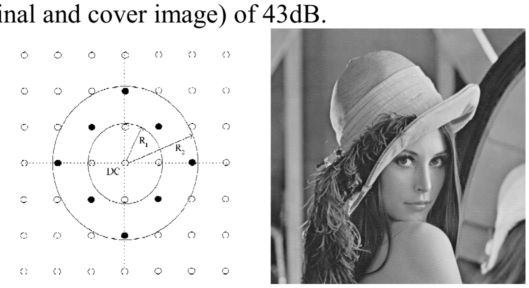

Fig. 4. Coefficient Selection and a typical example.

5. SIMULATIONS

5.1. Effect of the Sequence Length on TCQ-IS

The robustness performance of TCQ-IS against data sequence length is shown in Figure 5. The robustness is measured by the relation between the probabilities of erroneous bit decoding versus the watermark-to-noise ratio (WNR). Figure 5 displays the robustness of TCQ-IS with different lengths for Gaussian input source with zero mean, unit variance against a Gaussian channel noise of zero mean, 0.5 variance. As apparent from Figure 5, increasing data length improves the performance. However, beyond a limit, the improvement becomes indistinguishable. The reason for such a performance should be due to the fundamental problem (i.e. $m>>log_2N$) for detecting the initial state, as the length increases.

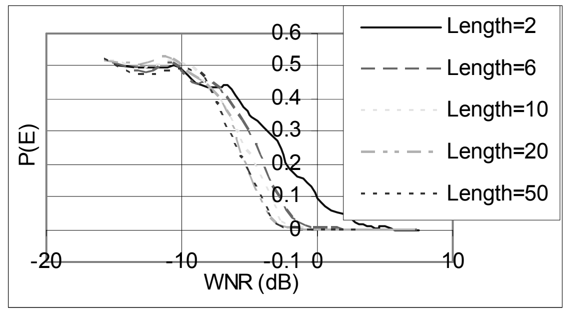

Fig. 5. TCQ-IS for different sequence lengths.

5.2. Comparison between TCQ-IS, DM, and TCQ-PS

The robustness performances of the 3 methods described in Section 3 are examined in terms of WNR and the probability of error, P(E). The channel noise power is kept constant, while the watermark power is varied. The probability of error is computed as the ratio of erroneously decoded data bits to the number of total data bits. The final values are computed by averaging the results for 500 random experiments. Two sources are used to embed data: a uniform source in the range (-1,1) and a Gaussian source with zero mean and unit variance. The TCQ structure in Figure 1 is utilized for both TCQ-IS and TCQ-PS during these simulations. The codebook is chosen so that it covers all input data range for the uniform source. For Gaussian source, the selected range contains most of the signal energy. Input data length is selected as 10. In order to equate the data embedding rate, DM uses 1 sample to hide 1 bit and TCQ-IS operates on input samples in lengths of 2. The robustness of the methods is plotted with respect to various Gaussian channel noises in Figures 6-9 .

The results indicate that, for all low-noise cases, TCQ-IS and DM performs similar, which is better than TCQ-PS. On the other hand, for high noise case, TCQ-IS has the best performance among the three methods.

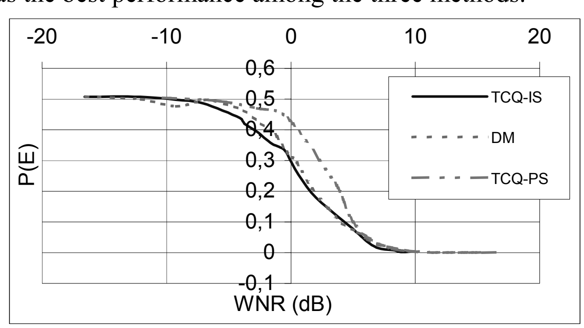

Fig.6. Uniform Source (-1,1) and Gaussian (0,0.5) Channel

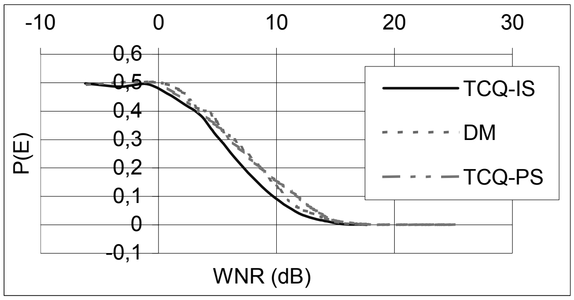

Fig.7. Uniform Source (-1,1) and Gaussian (0,1) Channel.

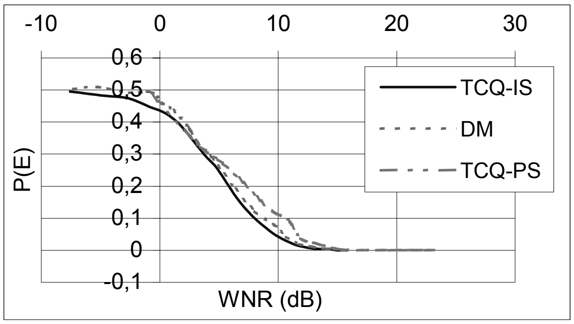

Fig 8. Gaussian Source (0,1) and Gaussian (0,1) Channel.

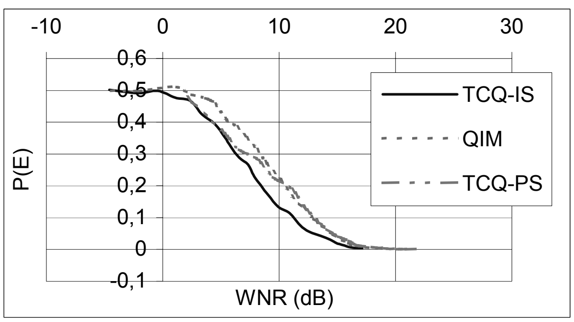

Fig.9. Gaussian Source (0,1) and Gaussian (0,2) Channel.

5.2. TCQ-IS for Images

The robustness of TCQ-IS for image data hiding is computed against JPEG compression attack using different trellises and codebooks. The block size is taken as 16. The first 6 coefficients between the circles of radii 3 and 2 are selected in raster scan. In addition to 4-state trellis shown in Figure 1, 8-PSK trellises with 8 and 16 states [9] are also employed. The results are shown in Figure 10, as the embedding distortion versus probability of error against JPEG-80 compression attack. It is apparent that as the trellis structure becomes dense, the robustness increases. It is also observed that even if the state numbers differ two PSK schemes behave similarly, since they share the same codebook.

6. CONCLUSIONS

A novel quantization-based data hiding method is proposed. The simulation results show that TCQ-IS method has better performance with respect to other well-known quantization based data hiding methods for certain input sources and channel noises, especially when distortion noise is high. Furthermore, embedding data using the magnitude of Discrete Fourier Transform coefficients of natural images by TCQ-IS is also implemented and it is observed that dense TCQ structures yield better results. As a future research optimal structures for certain attacks should be investigated.

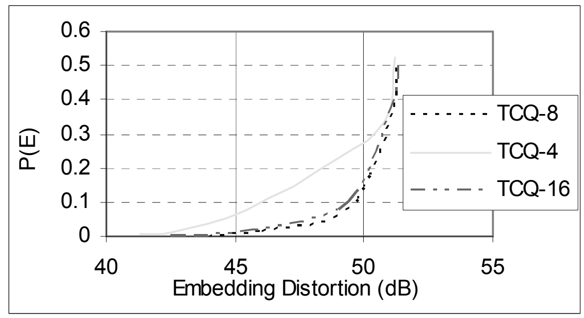

Fig.10. JPEG-80 Compression Attack Performance.

7. REFERENCES

[1] P. Moulin, "The role of information theory in watermarking and its application to image watermarking," invited paper, *Signal Processing.*, vol. 81, no. 6, pp. 1121-1139, June 2001.

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

[3] B. Chen, *Design and Analysis of Digital Watermarking, Information Embedding, and Data Hiding Systems*, Phd. Dissertation, MIT, 2000.

[4] 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.

[5] J. Chou, S. S. Pradhan, and K. Ramchandran, "On the duality between data hiding and distributed source coding," *Invited Paper, Proc. 33rd Annual Asilomar conference on Signals, Systems, and Computers,* Pacific Grove, CA, Nov. 1999.

[6] J. Chou, S. S. Pradhan, L. El Ghaoui, and K. Ramchandran, "A robust optimization solution to the data hiding problem using distributed source coding principles," *Proc. SPIE conference, San Jose, CA, Jan. 2000.*

[7] S. S. Pradhan, J. Chou, and K. Ramchandran, "Duality between source coding and channel coding and its extension to the side information case," *IEEE Trans. Inform. Theory*, vol. 49, no.5, May2003.

[8] 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.

[9] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. Inform. Theory*, vol.28, pp.55-67, Jan. 1982.