JOINT WATERMARKING AND COMPRESSION FOR GAUSSIAN AND LAPLACIAN SOURCES USING UNIFORM VECTOR QUANTIZATION

Guixing Wu , En-hui Yang and Da-ke He * †‡

ABSTRACT

Using fixed rate uniform vector quantization, in this paper, we consider how to design a joint watermarking and compression (JWC) system for Gaussian and Laplacian sources to maximize the robustness in the presence of additive Gaussian attacks under constraints on the compression rate and quantization distortion. Firstly, we construct vector quantizers shaped to match the multidimensional distribution of source signals. Then we scale codebooks corresponding to the vector quantizers to maximize the robustness of the watermarks against the additive Gaussian attacks. Simulation results show that the proposed scheme can achieve up to 0.92 dB distortion-to-noise ratio (DNR) gain over JWC schemes using uniform scalar quantization while maintaining the simplicity of implementation with uniform quantization.

Index Terms— Joint watermarking and compression, uniform vector quantization, distortion-to-noise ratio, robustness

I. INTRODUCTION

As a widely accepted approach for copyright protection and content authentication, digital watermarking and information hiding has recently drawn intensive attention from both industrial and academic communities[1], [2], [3]. In most applications, watermarked signals will be likely stored and/or transmitted in compressed format. Instead of treating watermarking and compression separately, it is interesting and beneficial to look at joint design of watermarking and compression schemes [6], [7], [8]. In [6], using fixed-rate scalar quantization (SQ) for watermarking and compression, the authors investigated how to design optimal joint watermarking and compression (JWC) systems to maximize the robustness of the systems in the presence of addictive Gaussian attacks under constraints on the compression rate and quantization distortion.

*Guixing Wu is with SlipStream Subsidiary, Research In Motion, 295 Phillip Street, Waterloo, ON, CA, N2L 3W8. E-mail: guwu@rim.com.

†En-hui Yang is with Department of Electrical and Computer Engineering, University of Waterloo, 200 University Avenue West, Waterloo, ON, CA, N2L 3G1. E-mail: ehyang@bbcr.uwaterloo.ca.

‡Da-ke He is with SlipStream Subsidiary, Research In Motion, 295 Phillip Street, Waterloo, ON, CA, N2L 3W8. E-mail: dhe@rim.com.

Motivated by the performance gain of vector quantization(VQ) over SQ in source coding, in this paper, we extend JWC schemes using SQ to JWC schemes using uniform VQ for i.i.d. Gaussian and Laplacian sources by utilizing lattice VQ techniques in [4]. Experimental results show that the new proposed JWC scheme achieves better performance than binary JWCs using uniform SQ in [6] by up to 0.92 dB DNR gain. We also show that the proposed scheme outperforms JWCs using nonuniform SQ schemes in [6] with additional superiority on the simplicity of implementation.

The remainder of the paper is organized as follows. Section II briefly reviews uniform VQ, that is, integer lattice VQ. In Section III we describe the design of a joint watermarking and compression algorithm using uniform VQ. Simulation results are given in Section V.

II. LATTICE VQ FOR GAUSSIAN AND LAPLACIAN SOURCES

By imposing a structural constraint on the output, the implementation of lattice VQ has the advantage of design simplicity and reduced computation complexity over those of un-structural VQ's. Therefore, lattice VQ has been widely studied and used in the design of source coding [4]. Some of the most frequently used lattices in VQ include $A_n(n \geq 1), D_n(n \geq 3), E_n(n \geq 16)$, and their duals [4]. In this paper we focus on the Z^n lattice, also called cubic or integer lattice because of its exceptional simplicity.

An integer lattice, denoted by Λ, is a set of vectors defined by

$$\Lambda = \{\mathbf{x} : \mathbf{x} = c_1\mathbf{a_1} + c_2\mathbf{a_2} + \cdots + c_n\mathbf{a_n}\}$$

where the $\mathbf{a_i}$ is a vector with the ith component equal to one and all other components zeros, and the c_i are integers. Since all possible integer combinations are allowed, the size of the lattice is, in general, infinite. For a given dimension and a compression rate, the design of a cubic lattice codebook consists of two steps [4]. First, an infinite lattice is truncated to obtain an integer codebook with the number of output points which is determined by the compression rate and dimension. Second, scaling is performed on the finite integer lattice codebook to minimize the encoding distortion.

In the first step, the way of truncation is determined by the distribution of source signal and it is performed in such a way that the higher probability region of the source signal is emphasized [4]. Consider an n-dimensional vector $\mathbf{S} = (S_1, S_2, \cdots, S_n)$, where the S_i are i.i.d. Gaussian or Laplacian random variables with zero mean and unit variance. The joint probability density function (pdf) of $\mathbf{S}$ is given by

$$p(\mathbf{s}) = A_1 exp(-A_2 \sum_{i=1}^{n} |s_i|^v) \tag{2.1}$$

where $A_1 = \frac{v\Gamma(3/v)^{1/2}}{2\Gamma(1/v)^{3/2}}$, $A_2 = [\frac{\Gamma(3/v)}{\Gamma(1/v)}]^{v/2}$, $\Gamma(.)$ is the Gamma function defined as $\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}dt$ for $x > 0$, v is the shape parameter with $v = 1$ for a Laplacian source and $v = 2$ for a Gaussian source. Since each s_i is i.i.d., the multidimensional pdf has contours of constant probability defined by $n-1$–dimensional surfaces

$$\sum_{i=1}^{n} |s_i|^v = constant. \tag{2.2}$$

From (2.1) and (2.2) we can see, the region close to the origin is more important than a region far from it. Furthermore, the pdf is symmetric with respect to the coordinate axes. Therefore, the shape of the constant pdf contours should be taken into account in the codebbok design and the codebook should be symmetric with respect to the coordinate axes. For the Gaussian source, the infinite integer lattice should be truncated in a spherical form so as to include the high pdf region. A so called theta function of the cubic lattice is used to compute the number of lattice vectors in a sphere with a certain radius[4]. In the Laplacian case, a finite pyramidal codebook is obtained. To determine the number of integer lattice vectors within a pyramid, Fisher's recursive algorithm in [5] can be used.

By constructing a vector quantizer which is shaped to match the multidimensional distribution of the source signal, lattice VQ can achieve smaller distortion than SQ [4].

III. AN ALGORITHM FOR JWC USING UNIFORM VECTOR QUANTIZATION

Having reviewed integer lattice VQ in the last section, in this section, we present an JWC algorithm by utilizing the above lattice VQ techniques.

Consider embedding an n-dimensional binary watermark message vector $\mathbf{m} = (m_1, m_2, \cdots, m_n)$, $m_i \in \{0, 1\}$ within an n-dimensional host signal vector. We construct 2^n different quantizers with each quantizer representing a watermark vector. Each quantizer $\mathbf{vq}^j(\mathbf{s})$, $j \in \{1, \cdots, 2^n\}$ is a mapping from the $\mathbf{R}^n$ to a codebook $VB^j = \{\mathbf{vb}_1^j, \mathbf{vb}_2^j, \cdots, \mathbf{vb}_L^j\}$. All codebooks VB^j are assumed to be disjoint. The output values, $\mathbf{vb}_l^j, l = 1, \cdots, L$ are referred to as reconstruction points. The component of the reconstruction point $\mathbf{vb}_l^j = (vb_{l1}^j, vb_{l2}^j, \cdots, vb_{ln}^j)$ can be specified as

$$vb_{li}^j = \begin{cases} (k_i - \frac{1}{4} - \lceil r_m \rceil)\Delta, & \text{if } m_i = 0 \\ (k_i - \frac{3}{4} - \lceil r_m \rceil)\Delta, & \text{if } m_i = 1 \end{cases}$$

where Δ is the quantization step size, k_i, $i = 1, \cdots, n$, is an integer chosen from the set $\{k_i : \ 1 \le k_i \le 2\lceil r_m \rceil\}$, and k_i should be chosen such that the following formula is satisfied

$$(\sum_{i=1}^{n} |vb_{li}^j|^v)^{1/v} \le r_m\Delta$$

where v is the shape parameter mentioned in the last section and r_m is a certain radius of cubic lattice codebook in lattice VQ [4] which determines the number of reconstruction points in a codebook, that is L, in the quantizer $\mathbf{vq}^j(\mathbf{s})$.

The quantization procedure corresponding to $\mathbf{vq}^j(\mathbf{s})$ is illustrated as follows. The norm and radius in the following denote the l_1 and l_2 norm and radius for a Laplacian and Gaussian source respectively.

Step 1 Given a dimension and a compression rate, determine the l_1 or l_2 radius r_m of an integer lattice codebook by using the methods mentioned in [4] or [5].

Step 2 Compute the norm of the host vector and compare it to $r_m\Delta$. If it is greater than $r_m\Delta$, go to Step 3. Otherwise, quantize each component of the host vector using a scalar quantizer as follows:

$$q^{m_i}(s_i) = \begin{cases} b_{k_i}^0 = (k_i - \frac{1}{4} - \lceil r_m \rceil)\Delta, & \text{if } m_i = 0 \\ b_{k_i}^1 = (k_i - \frac{3}{4} - \lceil r_m \rceil)\Delta, & \text{if } m_i = 1 \end{cases} \tag{3.3}$$

where $\lceil \ \rceil$ is a ceiling function, k_i is an integer chosen from the set $\{k_i : \ 1 \le k_i \le 2\lceil r_m \rceil\}$ such that the mean square error between s_i and $q^{m_i}(s_i)$ is minimized. If the norm of the new quantized vector is not greater than $r_m\Delta$, then this new vector is the watermarked signal and stop the process. Otherwise, go to Step 4.

Step 3 Project the host signal vector orthogonally onto the surface of a sphere or pyramid with a radius $r_m\Delta$. Use (3.3) to quantize each component of the projected vector. If the norm of the new quantized vector is not greater than $r_m\Delta$, then the new vector is the watermarked signal and stop the process. Otherwise, go to Step 4.

Step 4 Given the new vector from Step 2 or Step 3, find all vectors in $\mathbf{R}^n$ such that each of those vectors differs from it in only one component but with the same distance Δ. If one or more of those vectors lie in the jth codebook, choose the one closest to the original host vector or projected vector in Euclidian distance to be the watermarked signal and stop the process. Otherwise, find the one with the smallest norm, and repeat Step 4 until an acceptable point is found.

Associated with the quantizer $\mathbf{vq}^j$ is a partition of the $\mathbf{R}^n$ into L quantization or Voronoi cells. The lth Voronoi cell C_l^j is defined by

$$\begin{cases} C_l^j = \{\mathbf{s} \in \mathbf{R}^n : \mathbf{vq}^j(\mathbf{s}) = \mathbf{vb}_l^j\} \\ \bigcup_{l=1}^{L} C_l^j = \mathbf{R}^n \end{cases}$$

The average squared error distortion per dimension corresponding to C_l^j is

$$D_l^j = \frac{1}{n}\int_{C_l^j}\sum_{i=1}^{n}(s_i - vb_{li}^j)^2\, p(\mathbf{s})ds_1\cdots ds_n \qquad (3.4)$$

The total average squared error distortion D^j for the quantizer $\mathbf{vq}^j$ should sum up all the D_l^j's for all Voronoi cells in the quantizer $\mathbf{vq}^j$. Since the host vector has a symmetric distribution with respect to the coordinate axes, we have

$$D(\mathbf{S}, \mathbf{X}) = D^1 = D^2 = \cdots = D^{2^n}$$

where $D(\mathbf{S}, \mathbf{X})$ denotes the average distortion per dimension between the host signal and the watermarked signal.

At the decoder, a minimum distance decision rule is employed to extract the watermark. For the simplicity of computation, we decode the watermark bit by bit, that is,

$$\hat{m}(y) = \arg\min_{m\in\{0,1\}} ||\, y - q^m(y)|| \qquad (3.5)$$

where y is the received signal and $q^m(.)$ was defined in (3.3).

Denote by P_e the average bit error probability

$$P_e = \frac{1}{2}\sum_{m\in\{0,1\}}\sum_{k=1}^{2\lceil r_m\rceil}[\int p(s)p(b_k^m|s)\;ds\;]P_{k,\;e}^m \qquad (3.6)$$

where $p(b_k^m|s)$ is the transitional probability when quantizing the host signal and $P_{k,\;e}^m$ is the conditional decoding error probability given m and given the fact that b_k^m is the watermarked signal. Intuitively the decoding error probability P_e decreases with the increase of the quantization step size Δ. In the following we analyze P_e in the assumption of high compression rates.

In the case of high compression rates, the probability of the host vector outside the sphere (or pyramid) can be assumed to be negligible. Base on this assumption, the total encoding process can be approximated by Step 2. Since each component of the host vector in Step 2 is quantized independently, Step 2 in the encoding process is actually an n-dimensional product of binary uniform scalar quantization. Assume that the attack channel is i.i.d. AWGN with zero mean and a noise variance of σ_n^2, P_e can then be approximated by the decoding error probability of the JWC system using fixed-rate uniform SQ in [6].

For the host signal vector lying within a sphere or pyramid, we have the following lemma.

Lemma 1 *The marginal pdf of a Gaussian or Laplacian host vector which lies in a sphere or pyramid with any radius , $f(s)$, is symmetric with respect to the origin, continuous and nonincreasing when $s \geq 0$.*

In view of Lemmas 1 and 2 in [6], the decoding error probability is then a decreasing function of the quantization step size Δ over the range where $\frac{\Delta}{\sigma_n} > 4.0941$. Therefore, under the condition that $\frac{\Delta}{\sigma_n} > 4.0941$, we can increase the quantization step size to decrease the decoding error probability. With an encoding constraint D_1, the optimization problem is to find the largest allowable quantization step size Δ_{opt} . To determine Δ_{opt}, one can set the distortion function to D_1 and find the largest root of the equation $D = D_1$. In general it is difficult to determine the roots mathematically. Therefore, we determine the optimum root numerically.

It can be verified by the experiment that the distortion function is a convex function of the quantization step size. To find Δ_{opt}, we can first find the quantization step size Δ_{min} that minimizes the encoding distortion by numerical methods such as the bisection method or Newton method, and then scale the quantization step size with one coefficient $a(a > 1)$ such that $\Delta = a\Delta_{min}$ and $D(\Delta) = D_1$, the resulting quantization step size being the optimum quantization step size.

IV. SIMULATION AND COMPARISON

Having described algorithms for designing JWCs using uniform VQs, in this section, we evaluate the performance of the JWC schemes using uniform VQ by simulation and compare it to the JWC schemes using SQ in [6].

Consider an i.i.d. Gaussian and Laplacian host signal with zero mean and unit variance. Assume that the squared error distortion measure is used and the attack channel is AWGN. The algorithm for designing the JWC using uniform VQ scheme is carried out. Since it's difficult to compute D and P_e mathematically, we perform Monte Carlo simulation to approximate the true average encoding distortion and decoding error probability. In the Monte Carlo simulation, 50 sample sequences of length 10^7 were processed.

Figure 1 plots curves for Gaussian sources in terms of the bit error probabilities P_e versus DNR for the optimum JWC schemes using 16–dimensional uniform VQ, and optimum uniform SQ in [6] respectively. The composite compression rate of watermarked signal is 5 bits per host sample in which we embed 1 watermark bit of information per watermarked sample. The encoding distortion is 0.011624. From the figure, we can see that the optimum JWC using 16–dimensional uniform VQ achieves better performance than JWCs using optimum uniform SQ in [6]. At $P_e = 5 \times 10^{-4}$, the JWC using optimum uniform VQ provides 0.92 dB DNR gain over the JWC using optimum uniform SQ.

Table 1. gives a comparison of the decoding error probabilities between JWCs using uniform VQ and JWCs using nonuniform SQ [6]. As we can see, the JWC using optimum uniform VQ achieves better performance than the JWC using optimum nonuniform SQ. In addition, given a distortion constraint JWC using uniform VQ only requires a single quantization step size for any channel statistics while JWC using nonuniform SQ should produce different quantization codebooks for different channel statistics. Therefore, the imple-

mentation of the JWC using uniform VQ is simpler than that using nonuniform SQ.

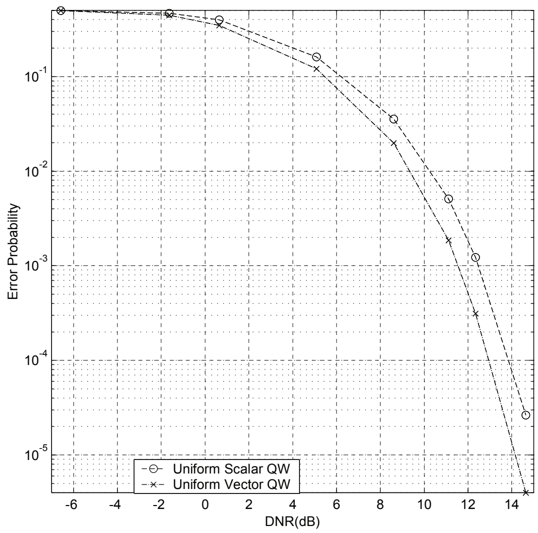

Fig. 1. Decoding error prob. for Gaussian host signal

DNR (dB)	-1.625	5.09	8.612	12.35	14.633
Nonuniform SQ	0.4461	0.1279	0.02294	4.87e-4	5.99e-6
Uniform VQ	0.445	0.1205	1.98e-2	3.13e-4	4.0e-6

Table 1. A comparison of error prob. between JWC using uniform VQ and JWCs using nonuniform SQ

Fig. 2 gives a comparison of decoding error probabilities for Laplacian sources between JWC using uniform VQ and JWCs using nouniform SQ. The encoding distortion is 0.02518. Likewise JWC using uniform VQ achieves better performance. For other compression rates and distortion constraints, similar results have been obtained.

V. CONCLUSION

In this paper, a JWC scheme using uniform VQ was proposed. We showed that it could achieve better performance than JWCs using SQ. In the future research, we will extend the current research to JWC schemes using other lattices. To further improve the robustness, channel coding techniques will also be applied.

VI. REFERENCES

[1] P. Moulin and R. Koetter, "Data-hiding codes," *Proceedings IEEE*, vol. 93, no. 12, pp. 2083-2127, Dec. 2005.

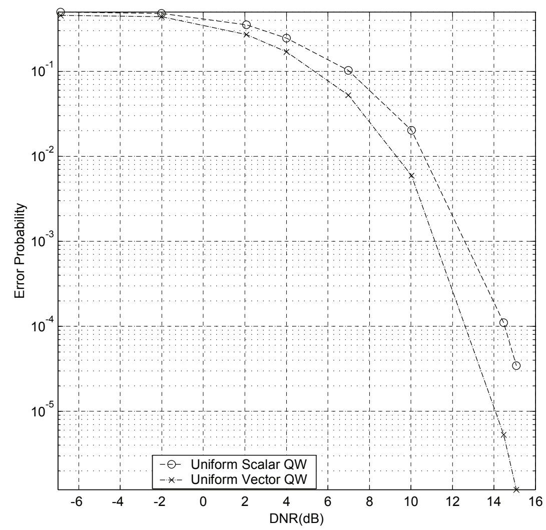

Fig. 2. Decoding error prob. for Laplacian host signal

[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, pp. 1423-1443, May 2001.

[3] L. Prez-Freire and F. Prez-Gonzlez, "Security of lattice-based data hiding against the watermarked only attack," *IEEE Trans. on Inform. Forens. and Security*, vol. 3, pp. 593-610, Dec. 2008

[4] D. G. Jeong and J. D. Gibson, "Uniform and piecewise uniform lattice vector quantization for memoryless Gaussian and Laplacian sources ," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 786-804, May 1993.

[5] T. R. Fisher, "A pyramidal vector quantizer ," *IEEE Trans. Inform. Theory*, vol. 32, pp. 568-583, July 1986.

[6] G. Wu and E.-H. Yang, "Joint watermarking and compression using scalar quantization for maximizing robustness in the presence of additive gaussian attacks," *IEEE Trans. Signal Processing*, vol. 53, no. 2, pp. 834-844, Feb. 2005.

[7] L. Guillemot and G.-M. Moureaux, "Indexing lattice vectors in a joint watermarking and compresison scheme," in *Proc. of ICASSP*, pp. 672-675, 2003.

[8] A. Maor and N. Merhav, "On joint information embedding and lossy compression," *IEEE Trans. Inform. Theory*, vol. 51, no. 8, pp. 2998-3008, Aug. 2005.