OPTIMIZATION STRATEGIES FOR QUANTIZATION WATERMARKING WITH APPLICATION TO IMAGE AUTHENTICATION

Guixing Wu, En-hui Yang and Wei Sun

Department of Electrical and Computer Engineering,
University of Waterloo, 200 University Avenue West,
Waterloo, ON, CA, N2L 3G1
Email:{g2wu,ehyang,wsun}@bbcr.uwaterloo.ca

ABSTRACT

In this paper we present optimal quantization watermarking strategies with respect to the robustness of a watermarking system given the embedding rate and distortion constraint. Firstly, we investigate the optimal decoding for quantization watermarking and show that by making use of channel statistics, the maximum likelihood decoder is always better than the minimum distance decoder. Secondly, the optimal encoding is designed by exploiting the knowledge of the host signal and channel statistics. Algorithms for designing the optimal uniform quantization encoding scheme and optimal nonuniform quantization encoding scheme are proposed. Simulation results show that the optimal nonuniform quantization watermarking can achieve better performance. Finally, applications to image authentication which is robust to high quality JPEG compression are described.

I. INTRODUCTION

In the recent years digital watermarking has been widely accepted as a valid approach for copyright protection and content authentication. It has been viewed as communication with side information [1] and can be generally described by Figure 1. In this Figure,

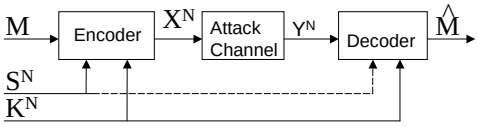

Fig. 1. General watermarking model

there is a host signal vector S^N into which we wish to embed a uniformly distributed watermark message M. The embedding rate is expressed as $R = \frac{1}{N}\log|\mathcal{M}|$, where $|\mathcal{M}|$ is the cardinality of the message set $\mathcal{M}$. The encoder is a function that maps S^N and M to a composite signal X^N subject to a distortion constraint D_1. The attacker, who is unable to access the side information S^N, produces a corrupted output signal Y^N in an attempt to remove the watermark with a distortion constraint D_2. The decoder extracts the embedded watermark and forms an estimate $\hat{M}$. The decoding error probability is defined as $P_e = P_r\{\hat{M} \neq M\}$ which can be used to characterize the robustness of a watermarking system. The secret key K^N is used to provide a source of randomness that is known to the decoder. In this paper we are primarily interested in the case where the host signal $S^N = (S_1, S_2 \cdots, S_N)$ is a sequence of i.i.d. random variables with distribution $p_S(s)$ and the attack channel is a memoryless channel.

Usually the original host signal is not available at the decoder. Indeed, many watermarking algorithms proposed so far have a general property that the host signal is treated as a source of the interference to the watermark message. Chen and Wornell[2] proposed a quantization watermarking (QW) method which can reject the host signal interference. In particular, they proposed a dither modulation approach as a low complexity QW method where the embedding can be described as

$$x = q(s + d(m)) - d(m) \stackrel{\Delta}{=} q^m(s) \qquad (1.1)$$

where $d(m)$ represents a dither vector and $q(\cdot)$ is a quantization operator. The watermark information is conveyed in the choice of quantizer. For an uncoded binary dither modulation with uniform scalar quantization, the output levels of quantizers can be specified as

$$x = \begin{cases} b_k^0 = \frac{\Delta}{4} + k\Delta, & \text{if } m = 0 \\ b_k^1 = -\frac{\Delta}{4} + k\Delta, & \text{if } m = 1 \end{cases}$$

where k is an integer.

One can extend the above dither modulation approach to general quantizers $q^m(s),\ m \in \{0,1\}$, where each q^m is a mapping from the real line R to a codebook $B^m = \{b_1^m, b_2^m, b_3^m \cdots b_L^m\}$. Hence all codebooks $B^m(s),\ m \in \{0,1\}$, are assumed to be disjoint. The output values, $b_j^m, j = 1, 2, \cdots L$, are referred to as reconstruction points or output levels. L is the number of output levels or the size of codebook; it could be finite or infinite. Associated with the quantizer q^m is a partition of the real line R into L quantization cells C_j^m. The jth quantization cell

$$\begin{cases} C_j^m = \{s \in R : q^m(s) = b_j^m\} = (z_{j-1}^m, z_j^m) \\ \bigcup_{j=1}^L C_j^m = R \end{cases}$$

is an interval which has b_j^m as the reconstruction point and (z_{j-1}^m, z_j^m) as the input range, where $z_j^m = \frac{1}{2}(b_j^m + b_{j+1}^m)$ if $1 \leq j \leq L-1$, $z_0^m = -\infty$ and $z_L^m = +\infty$.

The squared error distortion corresponding to the quantizer q^m is $D^m = \sum_{j=1}^L \int_{z_{j-1}^m}^{z_j^m} (s - b_j^m)^2 p(s) ds$ where $p(s)$ is the probability density function of the host signal. The average embedded

This work was supported in part by the Natural Sciences and Engineering Research Council of Canada under Grants RGPIN203035-98 and RGPIN203035-02, by the Premier's Research Excellence Award, by the Canada Foundation for Information, by the Ontario Distinguished Researcher Award, and by the Canada Research Chairs Program.

distortion is expressed as

$$D = D(S,X) = \frac{1}{2}\sum_{m\in\{0,1\}} D^m \tag{1.2}$$

At the receiver, a minimum distance (MD) decoder, which chooses the reconstruction point closest to the channel output signal y, is applied to extract the watermark, i.e.,

$$\hat{m}(y) = \arg\min_m ||y - q^m(y)|| \tag{1.3}$$

The above watermarking scheme is very simple. However, it doesn't consider the statistics of the host signal and attack channel to improve the robustness of the watermarking system, and hence it's not optimal. In this paper we consider the optimization problem with respect to the robustness of QW given the embedding rate and distortion constraint. In Section 2, we will explore the optimal decoding strategy to maximize the robustness. Optimal encoding strategies are proposed in Section 3. Applications to image authentication are presented in Section 4.

II. OPTIMAL DECODING FOR QUANTIZATION WATERMARKING

Watermarking has been viewed as a form of communication. From communication theory we know that maximum a posteriori (MAP) detection forms the optimal decision rule when the costs for all possible errors are equal. When all codewords are sent with equal probability, MAP detection is equal to maximum likelihood (ML) detection. For a QW system, the ML rule can be expressed as

$$\hat{m}(y) = \arg\max_m \{P(y|m)\} \tag{2.4}$$

where $P(y|m)$ is the conditional probability distribution of y under the condition that m is sent and can be expressed as

$$P(y|m) = \sum_{j=1}^{L} P(s \in C_j^m) A(y|b_j^m) \tag{2.5}$$

In (2.5), $P(s \in C_j^m)$ is the probability that the signal s lies in the quantization cell C_j^m, and $A(y|x)$ is the transitional probability distribution of the attack channel.

The performance of the decoder can be characterized by the average error probability

$$P_e = 1 - \frac{1}{M}\sum_{m\in\mathcal{M}} \int_{\mathcal{Y}_m} p(y|M=m)dy \tag{2.6}$$

where $\mathcal{Y}_m$ denotes the region for which we decide that the message m was sent.

In general it's difficult to get a simple closed–form formula to compute the error probability P_e given in (2.6). Figures 2 and 3 give the experimental results of the ML decoder vs MD decoder for the uncoded binary dither modulation with uniform quantization when the host signal $S \sim \mathcal{N}(0,1)$, the embedded signal is a binary random sequence, the attack is an additive white Gaussian channel with zero mean and variance of σ_n^2 and the two levels of distortion are 0.21333 and 0.003338, which correspond to a large and small distortion respectively. In the graphs SNR denotes the ratio of the encoded distortion to the variance of noise, i.e, $SNR = 10\log_{10}\frac{D(S,X)}{D(X,Y)} = 10\log_{10}\frac{D(S,X)}{\sigma_n^2}$.

From the graphs, we can see that the ML decoder is always better than the MD decoder. For instance, when $D(S,X) = 0.21333$ and $P_e = 0.375$, the SNR difference (ΔSNR) between the MD and ML decoder is $\Delta SNR = SNR_{MD} - SNR_{ML} = 0.5$ dB. The ML decoder achieves a 0.5 dB SNR gain. We also notice from Figure 3 that in the small distortion scenario, i.e, $D(S,X) << \sigma_s^2$, the performance of the MD decoder approaches that of the ML decoder, which suggests that in the small distortion scenario we can use the MD decoder instead of the ML decoder as the MD decoder has low implementation complexity.

III. OPTIMAL ENCODING FOR QUANTIZATION WATERMARKING

In [2], QW has been viewed as a combination of source coding (quantizers) and channel coding (signal constellations). In this section we will examine how source coding and channel coding theory can be utilized in watermark encoding to minimize the transmission error probability. In source coding, a quantizer can be optimized if we know the statistics of the host signal. LLoyd[3] and MAX[4] have proposed a method called Lloyd-Max algorithm to get an optimum quantizer which can minimize the distortion if the number of quantization levels L is fixed. Based on the LLoyd-Max algorithm, we will develop encoding schemes which can increase the robustness of the watermarking system while keeping the distortion within a prescribed limit. We begin with the design of optimal uniform QW schemes. As the usual embedded distortion is small, we employ the MD decoder below in our watermarking design.

III-A. Optimal Uniform Quantization Encoding

For a fixed L level uniform binary scalar quantizers, the output levels b_k^0 and b_k^1 are distributed symmetrically around the origin, which can be specified as

$$\begin{cases} b_k^0 = \frac{\Delta}{4} + (k - 1 - \lfloor\frac{L}{2}\rfloor)\Delta \\ b_k^1 = -\frac{\Delta}{4} - (L - k - \lfloor\frac{L}{2}\rfloor)\Delta \end{cases}$$

where $k = 1, 2, \cdots, L$.

The decoding error probability of the corresponding watermarking system can be expressed as

$$P_e = \frac{1}{2}\sum_{m\in\{0,1\}}\sum_{j=1}^{L} P(s \in C_j^m) P_{j,e}^m \tag{3.7}$$

where $P_{j,e}^m$ is the decoding error probability when the signal s is in the quantization cell C_j^m. In the case of an additive white Gaussian noise (AWGN) channel with a noise variance of σ_n^2, it can be shown that the error probability of the MD decoder is expressed as

$$\begin{cases} P_{j,e}^0 = Q(|\frac{((4L-j)+1)\Delta}{4\sigma_n}|\,) \\ \quad + \sum_{i=1}^{L-1} |\, Q(|\frac{(4(i+1-j)-3)\Delta}{4\sigma_n}|) - Q(|\frac{(4(i+1-j)-1)\Delta}{4\sigma_n}|\,)| \\ P_{j,e}^1 = Q(|\frac{(4(j-1)+1)\Delta}{4\sigma_n}|) \\ \quad + \sum_{i=2}^{L} |\, Q(|\frac{(4(i-j)-3)\Delta}{4\sigma_n}|\,) - Q(|\frac{(4(i-j)-1)\Delta}{4\sigma_n}|\,)| \end{cases} \tag{3.8}$$

when L is even. In (3.8), $Q(\cdot)$ is the Gaussian Q-function and $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-t^2/2}dt$. A similar formula can be obtained when L is odd.

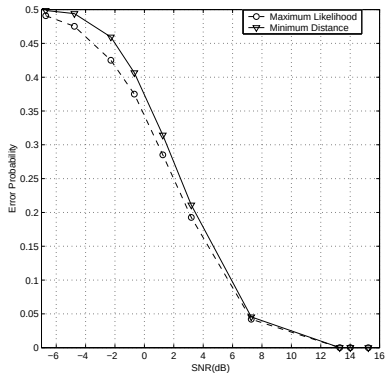

Fig. 2. Decoding error prob. for dither modulation when $D(S,X) = 0.21333$

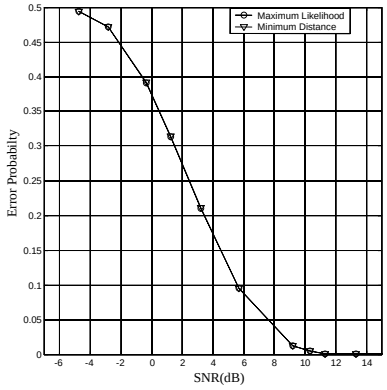

Fig. 3. Decoding error prob. for dither modulation when $D(S,X) = 0.003338$

The increase of quantization step size Δ will decrease the error probability $P_{j,e}^m$ and P_e. This can be showed by the following lemma.

Lemma 1 *When $t > \sqrt{4\ln 3}$ and $a > \frac{1}{2}$, function $f(t) = Q((a+\frac{1}{4})t) - Q((a-\frac{1}{4})t)$ is a decreasing function of the variable t.*

Therefore the optimization problem for the uniform QW is to find the largest allowable quantization step size Δ_{opt} with the distortion constraint D_1. One method to find Δ_{opt} is to set the distortion function (1.2) to the distortion constraint D_1 and then find the largest root of the equation $D = D_1$. In general it's difficult to determine the roots mathematically. In the following, we will use a numerical method to find Δ_{opt}.

Assume the equation $\frac{dD}{d\Delta} = 0$ has only one root $\Delta_{\min}$. Then we can show that $\frac{dD}{d\Delta} > 0$ if $\Delta > \Delta_{\min}$. The average distortion D is minimized with $D_{\min}$ at the point $\Delta_{\min}$. When $\Delta > \Delta_{\min}$, the distortion D is a increasing function of Δ. To determine Δ_{opt} with a distortion constraint D_1 which is greater than $D_{\min}$, we can first determine the quantization step size $\Delta_{\min}$ and then scale the quantization step size with one coefficient a $(a > 1)$ such that $D = D_1$. The optimal quantization step size is $\Delta_{\text{opt}} = a\Delta_{\min}$.

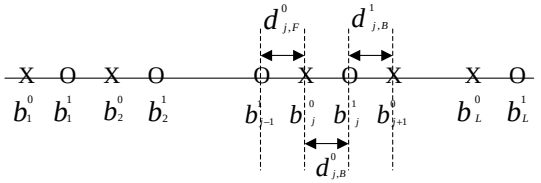

Fig. 4. Binary quantization watermarking with an even L

The root of the equation $\frac{dD}{d\Delta} = 0$, i.e, $\Delta_{\min}$, could be obtained by using the bisection method or Newton method. To find the optimal quantization step size Δ_{opt} is equal to determining one of the roots of the equation $D - D_1 = 0$, which is greater than $\Delta_{\min}$. By applying the same bisection method as in determining $\Delta_{\min}$, Δ_{opt} can be located easily.

It can be verified that $\frac{dD}{d\Delta}$ is an increasing function of the variable Δ and has only one root for the equation $\frac{dD}{d\Delta} = 0$ when the host signal is Gaussian or Laplacian for a fixed codebook size L.

Denote the optimal quantization step size for a fixed codebook size L as Δ_{opt}^L. When L is a variable we have the following theorem.

Theorem 1 *When the number of quantization levels is not fixed for a binary uniform quantization watermarking scheme, the optimal quantization step size is $\Delta_{\text{opt}}^\infty = \lim_{L\to\infty} \Delta_{\text{opt}}^L$.*

By relaxing the constraint that the quantizers in the watermarking scheme be uniform, we can get a more robust watermarking encoding scheme by utilizing the statistics of the host signal.

III-B. Optimal Nonuniform Quantization Encoding

Optimal nonuniform quantization in source coding includes the nearest neighbor rule and centroid rue with respect to the squared error distortion measure. Applying the above two rules can decrease the distortion, but it doesn't guarantee the decrease of the decoding error probability P_e. Thus a compromise is needed. The detailed algorithm is stated as follows:

Step 1 First use the algorithm in subsection III-A to get an optimal binary uniform quantization codebook set. Denote this initial quantization codebook set as $B^{(1)} = \{B^{0^{(1)}}, B^{1^{(1)}}\}$, and compute the average distortion as $D_{B^{(1)}}$ using the formula (1.2). Set $t = 1$ and $i = 1$. Compute the decoding error probability $P_e^{(1)}$ for this initial codebook set and set $s = 1$. At high signal to noise ratios, P_e can be approximated as

$$P_e \sim \frac{1}{2} \sum_{m\in\{0,1\}} \sum_{j=1}^{L} P(s \in C_j^m)[\, Q(\frac{d_{j,F}^m}{2\sigma_n}) + Q(\frac{d_{j,B}^m}{2\sigma_n})\,] \tag{3.9}$$

where

$$\begin{cases} d_{j,F}^0 = |b_j^0 - b_{j-1}^1|, & j = 2,\cdots,L \\ d_{j,B}^0 = d_{j,F}^1 = |b_j^1 - b_j^0|, & j = 1,\cdots,L-1 \\ d_{j,B}^1 = |b_{j+1}^0 - b_j^1|, & j = 1,\cdots,L-1 \\ d_{1,F}^0 = d_{L,B}^1 = \infty \end{cases}$$

are illustrated in Figure 4 when L is even.

Step 2 Given the codebook set $B^{(t)}$, find the centroid of the quantization cell C_i^0 and denote it as $b_i^{0'} = E[S|S \in C_i^0]$. Construct a temporary codebook set $B^{'} = \{B_0^{'}, B_1^{'}\}$ such that $B_0^{'} = \{b_1^0, b_2^0, \cdots, b_i^{0'} \cdots b_L^0\}$, $B_1^{'} = B_1$ and $z_i^{0'} = \frac{1}{2}(b_i^{0'} + b_{i+1}^{0\ '})$. Compute the decoding error probability $P_e^{'}$ for $B^{'}$. If $P_e^{'} < P_e$, let $B = B^{'}$, $P_e = P_e^{'}$; otherwise leave the old codebook set intact. Update the quantization cell C_i^1 and the codebook set likewise to a new codebook set.

Step 3 Repeat the above operation until $i = L$, and we get a codebook set $B^{(t+1)}$. Compute the corresponding distortion $D_{B^{(t+1)}}$. If $D_{B^{(t)}} - D_{B^{(t+1)}} < \epsilon_1$ for some t, where ϵ_1 is a prescribed threshold, then go to Step 4; otherwise increase t by 1, set i=1 and go to Step 2.

Step 4 Scale the codebooks in the codebook set with a coefficient $a(a > 1)$ using the bisection method such that we get a new codebook set with the distortion $D = D_1$. As the distance between signal constellations increases, the decoding error probability will decrease. Compute the decoding error probability for this new codebook set and denote it as $P_e^{(s+1)}$. If $P_e^{(s)} - P_e^{(s+1)} < \epsilon_2$ for some s, where ϵ_2 is a prescribed threshold, stop; otherwise increase s by 1, set $t = 1$ and $i = 1$, denote the newly obtained codebook set by $B^{(1)}$ and go to Step 2.

It's easy to see that the algorithm will necessarily produce a sequence of codebook sets with monotone nonincreasing values of the decoding error probability. Hence the algorithm will converge to a final codebook set. Figure 5 is a comparison of the performance of the optimal nonuniform QW vs the optimal uniform QW when $\mathcal{S} \sim \mathcal{N}(0, 1)$, the codebook size is 12 and the distortion $D(S, X) = 0.019089$. From the graphs, we can see the optimal nonuniform QW can achieve better performance. The difference of SNR between the two methods is 0.25 dB at $P_e = 10^{-5}$. At $P_e = 10^{-1}$, the difference increases to approximately 0.55 dB.

The above optimal QW scheme can be directly applied to image authentication when the watermark is required to be robust to high quality JPEG compression as JPEG compression can be modelled as one kind of Gaussian noise.

IV. APPLICATION IN IMAGE AUTHENTICATION

In this section we compare the robustness of our image authentication watermarking scheme incorporating the optimal nonuniform quantization with the watermarking method developed by Kundur and Hatzinakos[5] to high quality JPEG compression. Our watermarking technique is developed in the S–transform domain, one type of integer wavelet transforms, which can avoid the noise issue caused by round operations of the pixel value when saving the watermarked image using the transform domain watermarking[5].

Consider embedding a random sequence, one bit per coefficient, at each resolution level of the wavelet decomposition of 256×256 Lena image respectively with a mean square error (mse) constraint of 6 such that $PSNR \approx 40$ dB, which is a tolerated perturbation level for an image. We employ the optimal nonuniform QW in each subband and a Laplacian pdf is used to model the distribution of the wavelet coefficients in each subband. In Kundur and Hatzinakos's scheme the quantization step size is set to 2.2^{l_w} such that $mse \approx 6$ where l_w is the resolution level.

We tested the decoding error probabilities with Kundur and Hatzinakos's(KH) scheme and our optimal nonuniform QW scheme when the quality of JPEG compression ranges from 70 to 97. Table 1 illustrates the experimental result when the quality of JPEG compression is 92. We can see that the optimal nonuniform QW achieves better performance, which is useful for lossy communications. Similar performance gains were also obtained for other quality values.

V. CONCLUSIONS

In this paper we study how to improve the robustness of the quantization watermarking. The optimal decoding and encoding strategies are presented. Our technique can be applied to image authentication where robustness to JPEG compression is required.

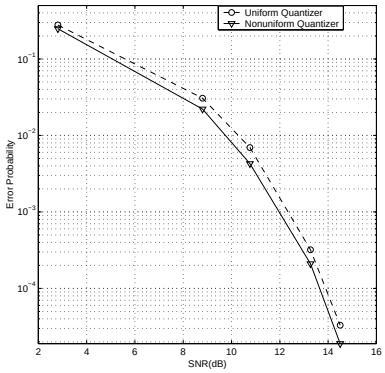

Fig. 5. Decoding error probability for optimal binary quantization watermarking

P_e	$l_w = 1$	$l_w = 2$	$l_w = 3$	$l_w = 4$	$l_w = 5$
KH	0.4252	0.1414	0.0436	0.0208	0.0052
QW	0.3972	0.0699	0.0111	0.0000	0.0000

Table 1. Decoding error prob. for KH's scheme and optimal QW scheme with a JPEG compression quality of 92

VI. REFERENCES

[1] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding." Preprint, avail-able at http: //www.ifp.uiuc.edu / moulin /paper.html, 2001.

[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] S. P. Lloyd. "Least Squares Quantization in PCM." IEEE Transactions on Information Theory. Vol IT-28, pp.129-137, March 1982 .

[4] J. Max. "Quantizing for Minimum Distortion." IRE Transactions on Information Theory. Vol. IT-6, pp.7-12, March 1960.

[5] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," in Proc. IEEE, vol. 87, pp. 1167-1180, July 1999.