Relationship between Quantization and Distribution Rates of Digitally Watermarked Data

Damianos Karakos
Department of Electrical and
Computer Engineering
University of Maryland
College Park, MD 20742, USA
e-mail: karakos@eng.umd.edu

Adrian Papamarcou
Department of Electrical and
Computer Engineering
University of Maryland
College Park, MD 20742, USA
e-mail: adrian@eng.umd.edu

Abstract — We consider a watermarking system where $2^{nR_W}$ distinct Gaussian watermarks are embedded in respective copies of an $n$-dimensional i.i.d. Gaussian image. Copies are distributed to customers in digital form, using $R_Q$ bits per image dimension. We establish the rate region for the pair $(R_Q, R_W)$ such that (i) the average quadratic distortion between the original image and each distributed copy is no more than a specified level; and (ii) the error probability in decoding the embedded watermark in the distributed copy approaches zero asymptotically in $n$.

I. PROBLEM FORMULATION

Recently, there have been some information-theoretic approaches to the analysis of watermarking systems. Of particular interest is [1], which gives a general expression for the maximum rate of the set of messages that can be hidden within a host data set subject to a distortion constraint, as well as the requirement that the message withstand a deliberate attack aimed to destroy it.

In this paper, we study a related problem that combines source and channel coding in a watermarking framework. This problem is motivated by the following scenario. A data distributor (e.g., a news agency) has to deliver an information sequence $\Gamma^n$ (e.g., a digital image) to $M_n = 2^{nR_W}$ customers, such that each customer receives a different watermarked version of $\Gamma^n$. To that end, the agent creates $M_n$ watermarks $X^n(1), \ldots, X^n(M_n)$ independently of $\Gamma^n$, and uses them to generate the watermarked copies $Y^n(k) = \Gamma^n + X^n(k)$, $k = 1, \ldots, M_n$. Due to bandwidth limitations, the agent compresses the watermarked data at a rate of $R_Q$ bits per image dimension subject to a fidelity criterion prior to distribution.

For security purposes as well as for maximum usability, we assume that both the quantization and the reconstruction of the image are independent of the choice of the watermark set. In addition, the agent who generated the image should be able to discern which watermark is present in a digital image with a low probability of error $P_e$ (e.g., in case an authenticator needs to track the initial owner of an illegally distributed image). Therefore, watermarks and source codewords have to be designed in such a way that knowledge of the watermark set and the original data is enough for detecting reliably the watermark in a compressed, watermarked image.

The main result of this paper is the determination of the allowable rates $R_Q$ and $R_W$ for the above system, under the following assumptions: (i) $\Gamma^n$ is i.i.d. $\mathcal{N}(0, P_1)$, (ii) the watermarks $X^n(1), \ldots, X^n(M_n)$ are generated i.i.d. $\mathcal{N}(0, P_X)$ with $P_X < P_1$, and (iii) the distortion constraint $n^{-1} \mathbb{E}[(\Gamma^n - Y^n)^2] \leq D$ is met (the quantized version of $Y^n$). Unlike the case in [1], here we consider a single fidelity criterion, namely the resultant distortion between the original data sequence and the watermarked/quantized data. Also, while quantization degrades the original image, it cannot be construed as a malicious attack of the type modeled in [1]. In our case, data compression and watermarking are cooperative (not competing) schemes, and must be optimized jointly.

II. RESULTS

The coding theorem that establishes the bounds on $R_Q$ and $R_W$ consists of two parts. The forward theorem demonstrates the existence of a source code for $\hat{Y}^n$ and an i.i.d. Gaussian random code for the watermark set such that the distortion constraint is satisfied and the probability of error $P_e$ is arbitrarily small, as long as $(R_Q, R_W)$ belong to some region $\mathcal{R}_D$. The converse theorem shows that if an arbitrary source code and an i.i.d. Gaussian watermark code jointly satisfy the distortion constraint and yield an asymptotically vanishing $P_e$, then $(R_Q, R_W)$ must lie in $\mathcal{R}_D$. We proved that $\mathcal{R}_D$ is characterized as follows:

$$R_Q \geq r_q(D) \triangleq \frac{1}{2} \log \left( \frac{P_1^2}{(P_1 + P_X)D - P_1P_X} \right)$$

$$R_W \leq r_w(R_Q, D) \triangleq R_Q - \frac{1}{2} \log \left( \frac{P_1}{D} \right)$$

where $\frac{P_1}{P_1 + P_X} < D \leq P_1$ (all distortion values of interest). The graphical representation of these results is given in Figure 1.

Fig. 1: For any distortion constraint $D$, the shaded area represents the region $\mathcal{R}_D$ of achievable pairs $(R_Q, R_W)$. As $D$ varies, the minimum source coding rate $r_q(D)$ and the maximum corresponding watermarking rate $r_w(R_Q(D), D)$ parametrically define curve $C$.

REFERENCES