Random-Coding Lower Bounds for the Error Exponent of Joint Quantization and Watermarking Systems

Yangfan Zhong, Fady Alajaji, *Senior Member, IEEE*, and Tamás Linder, *Senior Member, IEEE*

***Abstract*—We establish random-coding lower bounds to the error exponent of discrete and Gaussian joint quantization and private watermarking systems. In the discrete system, both the covertext and the attack channel are memoryless and have finite alphabets. In the Gaussian system, the covertext is memoryless Gaussian and the attack channel has additive memoryless Gaussian noise. In both cases, our bounds on the error exponent are positive in the interior of the achievable quantization and watermarking rate region.**

***Index Terms*—Capacity region, error exponent, Gaussian-type class, information hiding, joint quantization and watermarking, private watermarking, random-coding lower bound.**

I. Introduction

WATERMARKING (or information hiding) is the process of embedding a secret source message (*watermark*) into a host-data message (*covertext*). In general, a good embedding system should produce a watermarked message that is perceptually indistinguishable from the original covertext. On the other hand, it is assumed that the watermarked message is subjected to manipulation by an attacker who attempts to render the hidden information undetectable, so the embedding process should also be resilient to such attacks. A large body of literature including theoretical studies as well as various practical applications has recently been devoted to this area (see, e.g., [2], [6], [13]–[19], [22] and the references therein). One of the most common applications is copyright protection, where the author embeds the copyright into the original multimedia data in order to preserve the ownership of intellectual property.

In the information-theoretical literature, watermarking is usually modeled as a constrained channel coding problem. The watermark, usually assumed to be uniformly selected from a given message set, is embedded into the covertext, resulting in a message called the *stegotext*. Since the hidden messages should not interfere perceptually with the covertext, a distortion constraint is placed between the stegotext and the original covertext. From an information-theoretic point of view, one important problem is to find the watermarking (embedding) capacity defined as the largest embedding rate for which, at the encoder, the distortion between the covertext and the stegotext does not exceed a preset threshold, and at the decoder, the watermark can be reproduced with an arbitrarily small probability of error. A watermarking scenario is called *private* if the covertext is available to both the encoder and the decoder [2], [13], [14], [18], and *public* if the covertext is available to the encoder only [2], [19].

In order to save storage or bandwidth resources, it is often desirable that the embedder produces a compressed version of the watermarked message. Systems that integrate watermarking and lossy compression into one common encoding procedure are called joint quantization–watermarking (JQW) systems. Several works have investigated the problem of joint quantization and watermarking under various assumptions; see, e.g., [10], [11], [20], and [22]. In this paper, we concentrate on the private watermarking model studied in [8] and [9] which is depicted in Fig. 1.

Here the information hider embeds a watermark w chosen from a set of e^{nR_W} messages into a covertext $\boldsymbol{u}$, and outputs a *quantized* stegotext $\boldsymbol{x}$, which is selected from a codebook of e^{nR_Q} codewords. The quantities R_W and R_Q are called the *watermarking rate* and the *quantization rate*, respectively. The stegotext is passed through a memoryless channel (the attack channel) that models the attacker's action to make the watermark undetectable. It is assumed that both the encoder and the decoder knows the statistics of the attack channel.

The achievable rate region, defined as the set of watermarking–quantization rate pairs such that the average distortion (with respect to some single-letter distortion measure) between the covertext and the compressed stegotext does not exceed a threshold Δ, and such that the watermark w can asymptotically be decoded with high probability has been determined for the following two private embedding systems.

1. A discrete memoryless system consisting of a discrete memoryless host source (covertext) and a discrete memoryless attack channel [8];
2. A Gaussian system consisting of a memoryless Gaussian host source (covertext) and an additive memoryless Gaussian attack channel [8], [9].

In this work, we refine the above results by investigating the error exponent (reliability function) of these JQW systems. Roughly speaking, the error exponent E is the positive number with the property that the probability of decoding error of a good JQW code is approximately e^{-nE} for codes of large

Manuscript received May 12, 2008; revised February 23, 2009. Current version published June 24, 2009. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC).

Y. Zhong is with the Bank of Montreal, Toronto, ON M5X 1A1, Canada (e-mail: zhongyangfan@hotmail.com).

F. Alajaji and T. Linder are with the Department of Mathematics and Statistics, Queen's University, Kingston, ON K7L 3N6, Canada (e-mail: fady@mast.queensu.ca; linder@mast.queensu.ca).

Communicated by E. Ordentlich, Associate Editor for Source Coding.

Digital Object Identifier 10.1109/TIT.2009.2021383

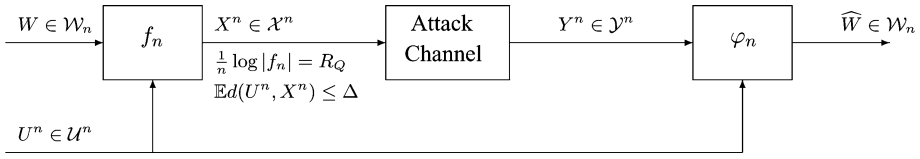

Fig. 1. A joint watermarking and quantization system.

block length n. Thus, the error exponent can be used to estimate the tradeoff between the probability of decoding error and the coding block length. Furthermore, one may use the error exponent or its bound as an information-theoretic criterion to design watermarking and quantization systems.

We note that error exponents for the watermarking problem without quantization have been studied, for example, in [13], [18], and [16] under various rather general assumptions on the strategies available to the embedder and the attacker. In [13], a Gallager-type lower bound on the error exponent was studied for private discrete watermarking systems. Regarding the lower bound as a target function of a game between the embedder and the attacker, a single-letter expression for the maximum lower bound was provided for certain distortion constraints. The study of the error exponent game was extended in [18] to the private system under large deviations distortion constraints. The authors established a random-coding lower bound and a sphere-packing upper bound for the error exponent, and a single-letter expression for the maximum error exponent was provided. In [16], the authors generalized the setup of the watermarking problem and derived a random-coding exponent for channel coding with side information at the encoder and the decoder. However, to our knowledge, the problem of error exponents for JQW systems has not yet been addressed in the literature, with the only exception of the recent work [21], where a Gallager-type random-coding lower bound on the error exponent is derived for the memoryless Gaussian system. However, this bound is somewhat loose in the sense that the resulting exponent is not positive over the entire region of achievable rate pairs.

In this work, we establish lower bounds to the coding error exponent (i.e., exponential upper bounds on the decoding error probability) for both the discrete system and the Gaussian system described above. To obtain the exponential bound for the discrete system, we employ a rate–distortion encoder that assigns a subcodebook to each watermark and encodes it by searching for the first codeword which is jointly typical with the covertext. At the decoder, a standard maximum-likelihood decoder is used. Here we point out that in the joint quantization–watermarking problem we consider one cannot simply apply Gallager's approach to the channel coding error exponent [5] since the encoder also incorporates a rate–distortion encoder. This makes the problem technically challenging, and in fact in deriving the lower bound on the error exponent we combine Gallager's random-coding bounding technique with a type-counting argument which is inspired by the proof of the type covering lemma [4]. To prove the error exponent bound for the Gaussian system, we borrow the notion of the Gaussian-type class introduced in [1] which facilitates the extension of the method of types to memoryless Gaussian sources. In both cases, the bounds will prove to be positive for all rate pairs in the interior of the achievable region.

The rest of the paper is organized as follows. In Section II, we formally describe the JQW problem and in Theorem 1 present the lower bound for the error exponent for discrete systems. The proof of the bound, which is the main result of this paper, is deferred to Section III. As a nontrivial extension, Theorem 2 in Section IV establishes an analogous lower bound to the coding error exponent of Gaussian quantization–watermarking systems. The proof of the bound for the Gaussian system is given in Section V. Section VI contains some concluding remarks and discussion.

II. Problem Formulation and Discrete Memoryless Systems

We first introduce some notational conventions used throughout the paper. Random variables (RVs) are denoted by capital letters, e.g., X, their specific values are denoted by lower case letters, e.g., x, and their alphabets are denoted by calligraphic letters, e.g., $\mathcal{X}$. Similarly, random vectors are denoted by capital letters superscripted by their lengths, e.g., X^n, their alphabets are denoted by calligraphic letters superscripted by their lengths, e.g., $\mathcal{X}^n$, and their realizations are denoted by boldface lower case letters, e.g., $\boldsymbol{x} \triangleq (x_1, x_2, \ldots, x_n) \in \mathcal{X}^n$.

For any finite alphabet $\mathcal{U}$, the set of all probability distributions on $\mathcal{U}$ is denoted by $\mathcal{P}(\mathcal{U})$, and for finite alphabets $\mathcal{U}, \mathcal{X}$, the set of all conditional distributions $P_{X|U}$ is denoted by $\mathcal{P}(\mathcal{X}\,|\,\mathcal{U})$. Given distributions $Q_U \in \mathcal{P}(\mathcal{U})$ and $A_{Y\,|\,X} \in \mathcal{P}(\mathcal{Y}\,|\,\mathcal{X})$, let $Q_U^{(n)}$ and $A_{Y\,|\,X}^{(n)}$ denote their n-fold product; i.e.,

$$Q_U^{(n)}(\boldsymbol{u}) = \prod_{i=1}^{n} Q_U(u_i)$$

and

$$A_{Y\,|\,X}^{(n)}(\boldsymbol{y}\,|\,\boldsymbol{x}) = \prod_{i=1}^{n} A_{Y\,|\,X}(y_i\,|\,x_i)$$

where $\boldsymbol{u} \triangleq (u_1, \cdots, u_n) \in \mathcal{U}^n$, $\boldsymbol{x} \in \mathcal{X}^n$, and $\boldsymbol{y} \triangleq (y_1, \cdots, y_n) \in \mathcal{Y}^n$. Note that $Q_U^{(n)}$ (resp., $A_{Y\,|\,X}^{(n)}$) is different from Q_{U^n} (resp., $W_{Y^n\,|\,X^n}$), where the latter denotes a generic probability distribution on $\mathcal{U}^n$ (resp., conditional distribution on $\mathcal{X}^n \times \mathcal{Y}^n$). For any finite set $\mathcal{X}$, the size of $\mathcal{X}$ is denoted by $|\mathcal{X}|$. If f is a function, $|f|$ is the size of its range, provided that it is finite. We denote the expectation of the RV X with respect to the distribution $P_X \in \mathcal{P}(\mathcal{X})$ by $\mathbb{E}_{P_X}(X)$; we also simply write $\mathbb{E}(X)$ if P_X is clear from the context. The joint entropy of RVs X and Y and the mutual information between RVs X and Y with respect to $P_{XY} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ are denoted by $H_{P_{XY}}(X,Y)$ and $I_{P_{XY}}(X;Y)$, respectively; we also simply write $H(X,Y)$ and $I(X;Y)$ whenever P_{XY} is clear from the context. All logarithms and exponentials are in the natural base.

We assume that the watermark W is uniformly drawn from the message set $\mathcal{W}_n \triangleq \{1, 2, \ldots, W_n\}$. The covertext U^n is a length-n sequence generated from a discrete memoryless source (DMS) with finite alphabet $\mathcal{U}$ and distribution Q_U. The attack channel is a discrete memoryless channel (DMC) with finite input alphabet $\mathcal{X}$, finite output alphabet $\mathcal{Y}$, and a transition distribution $A_{Y|X}$.

Let $d : \mathcal{U} \times \mathcal{X} \to [0, \infty)$ be a single-letter distortion measure and define $d_m \triangleq \max_{u,x} d(u, x)$. We make the standard assumption that $\min_x d(u, x) = 0$ for all u. For $\boldsymbol{u} \in \mathcal{U}^n$ and $\boldsymbol{x} \in \mathcal{X}^n$, let

$$d(\boldsymbol{u}, \boldsymbol{x}) = \frac{1}{n} \sum_{j=1}^{n} d(u_j, x_j).$$

An (f_n, φ_n) JQW code for the watermark set $\mathcal{W}_n$, host source Q_U, and attack channel $A_{Y|X}$ consists of an encoding function $f_n : \mathcal{W}_n \times \mathcal{U}^n \to \mathcal{X}^n$ which maps a watermark w and a covertext $\boldsymbol{u}$ to a representation sequence $\boldsymbol{x} \in \mathcal{X}^n$, and a decoding function $\varphi_n : \mathcal{Y}^n \times \mathcal{U}^n \to \mathcal{W}_n$. The quantities $R_W = \frac{1}{n} \log W_n$ and $R_Q = \frac{1}{n} \log |f_n|$ are , respectively, referred to as the watermarking and quantization rates.

The system operates under a private watermarking scenario since the decoder has also access to the host source. The (average) probability of erroneously decoding the watermarks is defined by

$$P_e^{(n)}(f_n, \varphi_n) \triangleq \frac{1}{e^{nR_W}} \sum_{w=1}^{e^{nR_W}} P_{e,w}^{(n)}(f_n, \varphi_n)$$

where $P_{e,w}^{(n)}(f_n, \varphi_n) \triangleq \Pr(\varphi_n(Y^n, U^n) \neq w \,|\, W = w)$, and the distortion between the covertext and the stegotext is given by

$$D(f_n, \varphi_n) \triangleq \mathbb{E} d(U^n, f_n(W, U^n))$$

where U^n is the covertext, and Y^n is the output of the attack channel.

Definition 1: The rate pair (R_1, R_2) is said to be achievable with respect to the distortion level $\Delta > 0$ if there exists a sequence of encoder–decoder pairs (f_n, φ_n) with $\lim_{n\to\infty} \frac{1}{n} \log |\mathcal{W}_n| \geq R_1$ and $\lim_{n\to\infty} \frac{1}{n} \log |f_n| \leq R_2$ which satisfy

$$\lim_{n\to\infty} P_e^{(n)}(f_n, \varphi_n) = 0$$

and

$$\limsup_{n\to\infty} D(f_n, \varphi_n) \leq \Delta.$$

Definition 2: The achievable region $\mathcal{C}(\Delta)$ is the closure of the set of achievable rate pairs (R_1, R_2).

It has been shown in [8] that for a DMS Q_U, a DMC $A_{Y|X}$, and distortion level $\Delta > 0$, the private quantization/watermarking achievable region is given by (1) shown at the bottom of the page,[1] where the mutual informations are taken under the joint distribution $Q_U P_{X|U} A_{Y|X}$.

Remark 1: Define

$$R_2^* \triangleq \max_{P_{X|U} : \mathbb{E}d(U,X) \leq \Delta} I(X; U, Y).$$

Then since $I(X; U, Y) - I(U; X) = I(X; Y \,|\, U)$, we have for all $R_2 \geq R_2^*$

$$\begin{aligned} \mathcal{C}(\Delta) \bigcap \{(R_1, R_2) : R_2 \geq R_2^*\} &= \Big\{(R_1, R_2) : R_2 \geq R_2^*, 0 < R_1 \\ &\qquad \leq R_{1,\max} \triangleq \max_{P_{X|U} : \mathbb{E}d(U,X) \leq \Delta} I(X; Y \,|\, U)\Big\}. \quad (2) \end{aligned}$$

This means that for $R_2 \geq R_2^*$, the maximum watermarking rate is a constant and is equal to $R_{1,\max}$. Obviously, one always has $R_2^* \leq \log |\mathcal{X}|$, and in fact all rates $R_2 \geq \log |\mathcal{X}|$ are equivalent to $R_2 = \log |\mathcal{X}|$, the largest rate the quantizer can take if the stegotext alphabet is finite. The fact that we still formally allow $R_2 > \log |\mathcal{X}|$ (the definition of achievability does not exclude such rates) should cause no confusion.

In many cases, $R_2^* < \log |\mathcal{X}|$. For example, if $A_{Y|X}$ is noiseless ($Y = X$ almost surely), then

$$R_2^* = R_2^*(\Delta) = \max_{P_{X|U} : \mathbb{E}d(U,X) \leq \Delta} H(X).$$

If we furthermore assume that $\mathcal{U} = \mathcal{X}$, $d(u, x) = 0$ iff $u = x$, and $H(U) < \log |\mathcal{U}|$, then $R_2^*(0) = H(U)$ and since $R_2^*(\Delta)$ is continuous, we have $R_2^*(\Delta) < \log |\mathcal{X}|$ for $\Delta > 0$ sufficiently small. Similar arguments can be used to show that $R_2^* < \log |\mathcal{X}|$ under quite general conditions if Δ is small enough. In such cases, lossy compression of the covertext to rates between R_2^* and $\log |\mathcal{X}|$ does not result in a loss of optimality in terms of the embedding capacity with respect to the uncompressed system (i.e., $R_2 = \log |\mathcal{X}|$).

Definition 3: Given $R_1 > 0$ and $R_2 > 0$, the JQW error exponent $E_{\mathrm{QW}}(R_1, R_2)$ for a DMS Q_U and a DMC $A_{Y|X}$ is defined as the supremum of the set of all numbers E for which there exists a sequence of JQW codes (f_n, φ_n) such that $\lim_{n\to\infty} \frac{1}{n} \log |\mathcal{W}_n| \geq R_1, \lim_{n\to\infty} \frac{1}{n} \log |f_n| \leq R_2$

$$\limsup_{n\to\infty} D(f_n, \varphi_n) \leq \Delta$$

and

$$E \leq \liminf_{n\to\infty} -\frac{1}{n} \log P_e^{(n)}(f_n, \varphi_n).$$

We next define some quantities that are needed for stating our lower bound on the JQW error exponent. Given the DMS Q_U,

[1]We remark that in [8] and [9] the achievable region is defined with respect to the maximum error probability $\max_w P_{e,w}^{(n)}(f_n, \varphi_n)$. However, the converse theorems in [8] and [9] guarantee that the regions $\mathcal{C}(\Delta)$ and $\hat{\mathcal{C}}(\Delta)$ given in (1) and (38) remain the same if we define the achievable region with the average error probability $P_e^{(n)}(f_n, \varphi_n)$.

$$\mathcal{C}(\Delta) = \left\{ (R_1, R_2) : \begin{array}{l} R_2 \geq \min\limits_{P_{X|U} : \mathbb{E}d(U,X) \leq \Delta} I(U; X) \\ 0 < R_1 \leq \max\limits_{P_{X|U} : \mathbb{E}d(U,X) \leq \Delta} \min\{R_2 - I(U; X), I(X; Y \,|\, U)\} \end{array} \right\} \quad (1)$$

and a conditional distribution $P_{X|U} \in \mathcal{P}(\mathcal{X}\,|\,\mathcal{U})$, for any $\Delta > 0$ and $R > 0$, define

$$F(Q_U, P_{X|U}, \Delta, R) \triangleq \inf_{P_U \notin \Phi} D(P_U \| Q_U)$$

where

$$D(P_U \| Q_U) \triangleq \sum_{u \in \mathcal{U}} P_U(u) \log \frac{P_U(u)}{Q_U(u)}$$

is the Kullback–Leibler divergence between P_U and Q_U ([3], [4]), and

$$\Phi = \Phi(P_{X|U}) \triangleq \Big\{ P_U \in \mathcal{P}(\mathcal{U}) : I_{P_U P_{X|U}}(U;X) < R \text{ and } \mathbb{E}_{P_U P_{X|U}} d(U,X) < \Delta \Big\}.$$

Note that the function $F(Q_U, P_{X|U}, \Delta, R)$ and Marton's lossy source coding error exponent [12] are related, but not equal. In the definition of $F(Q_U, P_{X|U}, \Delta, R)$, we use the convention that the infimum of the empty set is $+\infty$. By definition, $F(Q_U, P_{X|U}, \Delta, R)$ is positive if $Q_U \in \Phi$ and it is nondecreasing in R. If $\mathbb{E}_{Q_U P_{X|U}} d(U,X) < \Delta$, then we clearly have

$$F(Q_U, P_{X|U}, \Delta, R) = 0, \quad \text{if } 0 \le R \le I_{Q_U P_{X|U}}(U;X)$$

and

$$F(Q_U, P_{X|U}, \Delta, R) > 0, \quad \text{if } R > I_{Q_U P_{X|U}}(U;X).$$

Note that

$$F(Q_U, P_{X|U}, \Delta, R) < +\infty \text{ if } 0 \le R \le C(P_{X|U})$$

where

$$C(P_{X|U}) \triangleq \max_{P_U \in \mathcal{P}(\mathcal{U})} I_{P_U P_{X|U}}(U;X).$$

If the set $\{P_U : \mathbb{E}_{P_U P_{X|U}} d(U,X) \ge \Delta\}$ is not empty, then $F(Q_U, P_{X|U}, \Delta, R)$ is finite for all $0 \le R \le \log|\mathcal{X}|$.

Proposition 1: $F(Q_U, P_{X|U}, \Delta, R)$ is a continuous function of R in the interval $[0, C(P_{X|U})]$.

Proof: The proof is given in Appendix A. □

Given the DMS Q_U, the DMC $A_{Y\,|\,X}$, and a conditional distribution $P_{X|U} \in \mathcal{P}(\mathcal{X}\,|\,\mathcal{U})$, for any $R > 0$ define

$$E_r(Q_U, A_{Y\,|\,X}, P_{X|U}, R) \triangleq \max_{0 \le \rho \le 1} [E_o(Q_U, A_{Y\,|\,X}, P_{X|U}, \rho) - \rho R] \quad (3)$$

where

$$E_o(Q_U, A_{Y\,|\,X}, P_{X|U}, \rho) = -\log \sum_{\mathcal{U}} Q_U(u) \sum_{\mathcal{Y}} \left[\sum_{\mathcal{X}} P_{X|U}(x\,|\,u) A_{Y\,|\,X}^{\frac{1}{1+\rho}}(y\,|\,x) \right]^{1+\rho}.$$

We note that $E_r(Q_U, A_{Y\,|\,X}, P_{X|U}, R)$ is analogous to Gallager's random-coding lower bound for the DMC error exponent ([5, Theorem 5.6.1]). Also, it was shown in [13] that

$$E_{W,r}(R) = \sup_{P_{X|U}: \mathbb{E}_{Q_U P_{X|U}} d(U,X) < \Delta} E_r(Q_U, A_{Y\,|\,X}, P_{X|U}, R) \quad (4)$$

is a lower bound for the error exponent for watermarking *without* quantization.

The following is one of the two main results of the paper.

Theorem 1: For a DMS covertext Q_U and an attack DMC $A_{Y\,|\,X}$, the JWQ error exponent $E_{\mathrm{QW}}(R_1, R_2)$ is lower-bounded for all $R_1 > 0$ and $R_2 > 0$ as

$$E_{\mathrm{QW}}(R_1, R_2) \ge E_{QW,r}(R_1, R_2) \triangleq \sup_{P_{X|U}: \mathbb{E}_{Q_U P_{X|U}} d(U,X) < \Delta} \min \Big\{ F(Q_U, P_{X|U}, \Delta, \tilde{R}_2 - R_1), E_r(Q_U, A_{Y\,|\,X}, P_{X|U}, R_1) \Big\} \quad (5)$$

where $\tilde{R}_2 = \min(R_2, \log|\mathcal{X}|)$.

Remark 2: Although we only consider memoryless attack channels, it is relatively straightforward to extend the lower bound to an arbitrary discrete attack channel $\mathbf{A}_{Y\,|\,X}$ defined by the finite input and output alphabets $\mathcal{X}$ and $\mathcal{Y}$, and a sequence of transition distributions $\{W_{Y^n\,|\,X^n}\}_{n=1}^{\infty}$. In this general case (of attack channels with memory), $E_r(Q_U, A_{Y\,|\,X}, P_{X|U}, R_1)$ in (5) is replaced by

$$E_r(Q_U, \mathbf{A}_{Y\,|\,X}, P_{X|U}, R_1) \triangleq \max_{0 \le \rho \le 1} [E_o(Q_U, \mathbf{A}_{Y\,|\,X}, P_{X|U}, \rho) - \rho R_1] \quad (6)$$

where

$$E_o(Q_U, \mathbf{A}_{Y\,|\,X}, P_{X|U}, \rho) \triangleq \liminf_{n \to \infty} -\frac{1}{n} \log \sum_{\mathcal{U}^n} Q_U^{(n)}(\boldsymbol{u}) \sum_{\mathcal{Y}^n} \left[\sum_{\mathcal{X}^n} P_{X|U}^{(n)}(\boldsymbol{x}\,|\,\boldsymbol{u}) A_{Y^n\,|\,X^n}^{\frac{1}{1+\rho}}(\boldsymbol{y}\,|\,\boldsymbol{x}) \right]^{1+\rho}.$$

Remark 3: Note that for quantization rates $R_2 \ge \log|\mathcal{X}|$ the problem reduces to the watermarking problem without quantization. For this case, Merhav in [13] derived the lower bound $E_{W,r}$ given in (4). Clearly

$$E_{\mathrm{QW}}(R_1, R_2) \ge E_{W,r}(R_1) \ge E_{QW,r}(R_1, R_2)$$

for all $R_2 \ge \log|\mathcal{X}|$. We have not been able to show that our bound $E_{\mathrm{QW},r}(R_1, R_2)$ reduces to $E_{W,r}(R_1)$ for $R_2 \ge \log|\mathcal{X}|$. However, our numerical results (see Example 1 below) indicate that this is the case. Furthermore, the numerical results demonstrate that there exists a rate $R_2' = R_2'(R_1)$ which is *less* than $\log|\mathcal{X}|$ such that $E_{\mathrm{QW},r}(R_1, R_2) = E_{\mathrm{QW},r}(R_1, R_2')$ for all $R_2 \ge R_2'$.

The following property of $E_{\mathrm{QW},r}(R_1, R_2)$ is straightforward.

Lemma 1: $E_{\mathrm{QW},r}(R_1, R_2)$ is nondecreasing in R_2 and nonincreasing in R_1.

It is easy to verify that

$$E_o(Q_U, A_{Y\,|\,X}, P_{X|U}, 0) = 0,$$

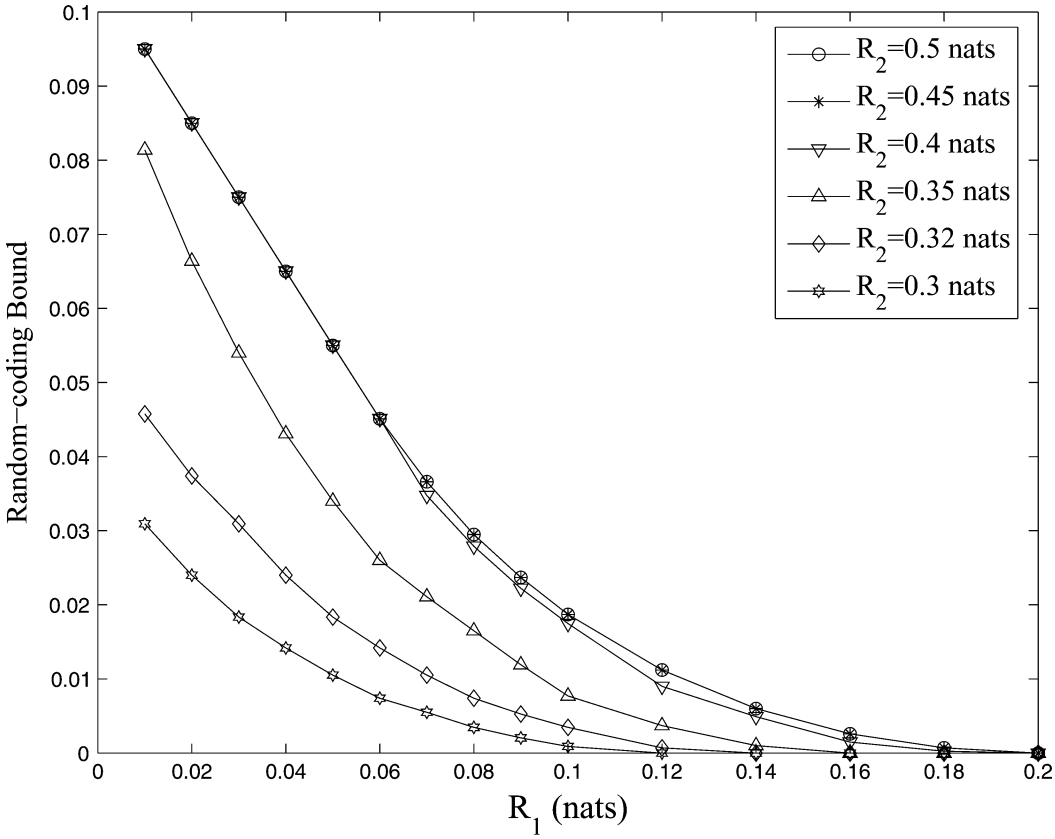

Fig. 2. The random-coding lower bound $E_{\mathrm{QW},r}(R_1, R_2)$ versus R_1 for the JQW system of Example 1.

$$\left.\frac{\partial E_o(Q_U, A_{Y\,|\,X}, P_{X|U}, \rho)}{\partial \rho}\right|_{\rho=0} = I(X;Y\,|\,U),$$
$$\frac{\partial^2 E_o(Q_U, A_{Y\,|\,X}, P_{X|U}, \rho)}{\partial \rho^2} \le 0, \quad \rho \ge 0. \tag{7}$$

These properties of $E_o(Q_U, A_{Y\,|\,X}, P_{X|U}, \rho)$ imply that $E_r(Q_U, A_{Y\,|\,X}, P_{X|U}, R)$ is positive if and only if $R < I(X;Y\,|\,U)$. We obtain the following corollary.

Corollary 1: $E_{\mathrm{QW},r}(R_1, R_2) > 0$ for any $(R_1, R_2) \in \mathrm{int}(\mathcal{C}(\Delta))$, where $\mathrm{int}(\mathcal{C}(\Delta))$ denotes the interior of the rate region $\mathcal{C}(\Delta)$ given in (1).

Proof: By definition

$$E_{\mathrm{QW},r}(R_1, R_2) = E_{\mathrm{QW},r}(R_1, \log|\mathcal{X}|)$$

for any $R_2 > \log|\mathcal{X}|$, so we have to show that $E_{\mathrm{QW},r}(R_1, R_2) > 0$ for $(R_1, R_2) \in \mathrm{int}(\mathcal{C}(\Delta))$ such that $R_2 \le \log|\mathcal{X}|$.

Note that by the definition of $\mathcal{C}(\Delta)$, if $(R_1, R_2) \in \mathrm{int}(\mathcal{C}(\Delta))$ and $R_2 \le \log|\mathcal{X}|$, then there exists a $P_{X|U}$ such that

$$\mathbb{E}_{Q_U P_{X|U}} d(U, X) \le \Delta, \quad 0 < R_1 < R_2 - I_{Q_U P_{X|U}}(U;X),$$
$$R_1 < I_{Q_U P_{X|U} A_{Y\,|\,X}}(X;Y\,|\,U). \tag{8}$$

Assume (Case 1) that the first inequality is strict in (8). Then we clearly have $E_{\mathrm{QW},r}(R_1, R_2) > 0$ since

$$F(Q_U, P_{X|U}, \Delta, R_2 - R_1) > 0$$

for $R_2 - R_1 > I(U;X)$; on the other hand, $R_1 < I(X;Y\,|\,U)$ implies

$$E_r(Q_U, A_{Y\,|\,X}, P_{X|U}, R_1) > 0.$$

If (Case 2) the first inequality in (8) holds with equality, then because the quantities $\mathbb{E}_{Q_U P_{X|U}} d(U, X)$, $I_{Q_U P_{X|U}}(U;X)$, and $I_{Q_U P_{X|U} A_{Y\,|\,X}}(X;Y\,|\,U)$ are continuous functions of $P_{X|U}$, we can find a $P'_{X|U}$ such that $\mathbb{E}_{Q_U P'_{X|U}} d(U, X) < \Delta$, $0 < R_1 < R_2 - I_{Q_U P'_{X|U}}(U;X)$, and $R_1 < I_{Q_U P'_{X|U} A_{Y\,|\,X}}(X;Y\,|\,U)$. (Finding such a $P'_{X|U}$ is possible because the condition $\min_x d(u, x) = 0$ implies that for all $\Delta > 0$, $\{P_{X|U} : \mathbb{E}_{Q_U P_{X|U}} d(U, X) \le \Delta\}$ is the closure of $\{P_{X|U} : \mathbb{E}_{Q_U P_{X|U}} d(U, X) < \Delta\}$.) According to Case 1, we must have $E_{\mathrm{QW},r}(R_1, R_2) > 0$. □

Example 1: Let the covertext be a DMS with alphabet $\{0, 1\}$ and distribution $Q_U(0) = 0.2$. Let the attack channel $A_{Y\,|\,X}$ be a binary-symmetric channel with alphabets $\mathcal{X} = \mathcal{Y} = \{0, 1\}$ and crossover probability $\epsilon = 0.05$ and consider the Hamming distortion measure.

Set $\Delta = 0.1$. In Fig. 2, we plot the random-coding lower bound $E_{\mathrm{QW},r}(R_1, R_2)$ against R_1 for different values of R_2, both measured in nats. It is seen that $E_{\mathrm{QW},r}(R_1, 0.5) = E_{\mathrm{QW},r}(R_1, 0.45)$ for all R_1, and $E_{\mathrm{QW},r}(R_1, 0.4)$ coincides with $E_{\mathrm{QW},r}(R_1, 0.45)$ for small R_1. The plots also show that $E_{\mathrm{QW},r}(R_1, R_2)$ does not depend on R_2 if R_2 is sufficiently large and it numerically coincides with $E_{W,r}(R_1, R_2)$. For example, if we fix $R_1 = 0.1$, then $E_{\mathrm{QW},r}(0.1, R_2) = E_{\mathrm{QW},r}(0.1, 0.405) = E_{W,r}(0.1, R_2)$ for all $R_2 \ge 0.405$. Note that $\log|\mathcal{X}| = 0.69$ nats.

In Fig. 3, we plot the quantization–watermarking rate region. In regions $\mathbf{A}$ and $\mathbf{B}$ our lower bound $E_{\mathrm{QW},r}(R_1, R_2)$ is positive, and it is zero in $\mathbf{C}$. The region $\mathbf{A} \cup \mathbf{B}$ coincides with $\mathcal{C}(\Delta)$ given in (1). Note that for $R_2 \ge R_2^* =$

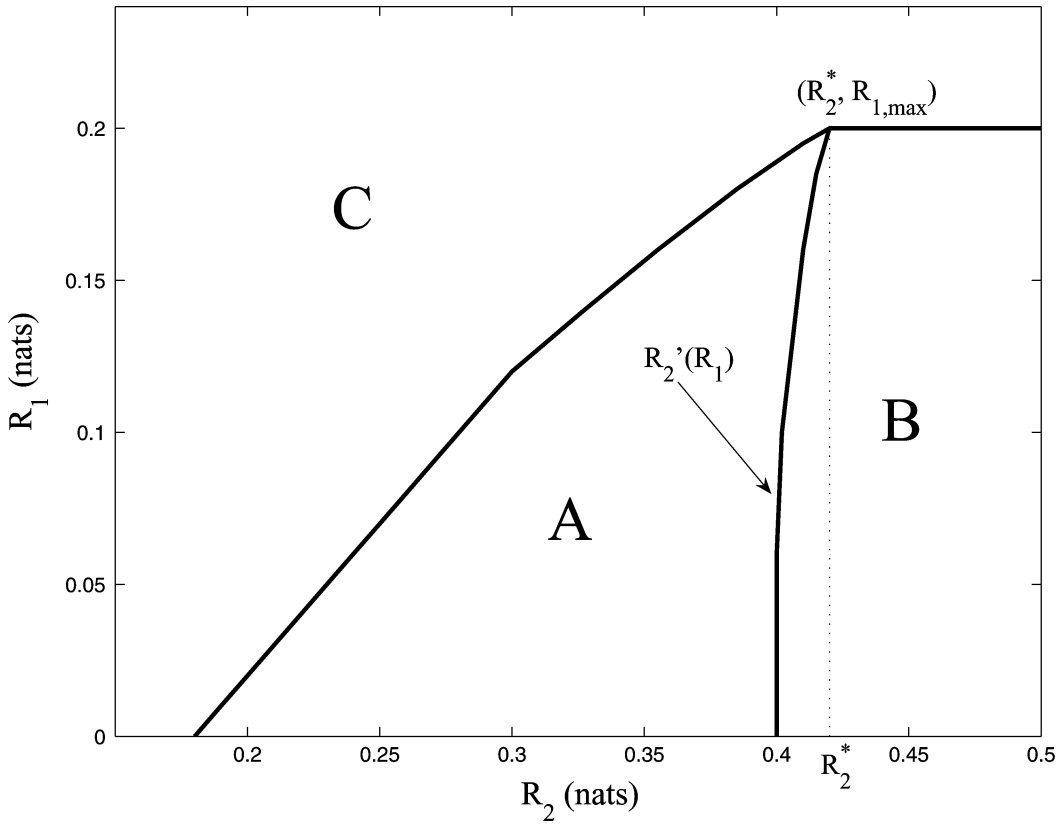

Fig. 3. The quantization–watermarking rate region of Example 1: $E_{\mathrm{QW},r}(R_1, R_2) > 0$ in $\mathbf{A}$ and $\mathbf{B}$; $E_{\mathrm{QW},r}(R_1, R_2) = 0$ in $\mathbf{C}$ (including its boundary). Note that $\log |\mathcal{X}| = 0.69$ nats.

0.42 nats the maximum watermarking rate is a constant and is equal to $R_{1,\max} = 0.2$ nats (see also Remark 1). The boundary between $\mathbf{A}$ and $\mathbf{B}$ determines the rate $R_2' = R_2'(R_1)$ such that $E_{\mathrm{QW},r}(R_1, R_2) = E_{\mathrm{QW},r}(R_1, R_2')$ for all $R_2 \geq R_2'$; i.e., for R_2 rates larger than R_2', our lower bound is constant in R_2 and only depends on R_1. For example, when $R_1 = 0.02$ nats, $R_2' = 0.4$ nats, which means that $E_{\mathrm{QW},r}(0.02, R_2) = E_{\mathrm{QW},r}(0.02, 0.4)$ for all $R_2 \geq 0.4$ nats, and when $R_1 = 0.16$ nats, $R_2' = 0.41$ nats, which means that $E_{\mathrm{QW},r}(0.16, R_2) = E_{\mathrm{QW},r}(0.16, 0.41)$ for all $R_2 \geq 0.41$ nats.

III. Proof of Theorem 1

Note that if $R_1 \geq R_2$, then the lower bound is trivially equal to 0. Thus we will assume throughout the proof that $R_2 > R_1 > 0$.

A. Preliminaries

The following notation and conventions are adopted from [4]. The type of an n-length sequence $\boldsymbol{u} \in \mathcal{U}^n$ is the empirical probability distribution $P_{\boldsymbol{u}} \in \mathcal{P}(\mathcal{U})$ defined by

$$P_{\boldsymbol{u}}(a) \triangleq \frac{1}{n} N(a \,|\, \boldsymbol{u}), \quad a \in \mathcal{U}$$

where $N(a \,|\, \boldsymbol{u})$ is the number of occurrences of a in $\boldsymbol{u}$. Let $\mathcal{P}_n(\mathcal{U}) \subseteq \mathcal{P}(\mathcal{U})$ be the collection of all types of sequences in $\mathcal{U}^n$. For any $P_U \in \mathcal{P}_n(\mathcal{U})$, the set of all $\boldsymbol{u} \in \mathcal{U}^n$ with type P_U is called the P_U-type class and is denoted by $\mathcal{T}_{P_U}^{(n)}$, or simply by $\mathcal{T}_U^{(n)}$ if P_U is clear from the context.

For any distribution $P_X \in \mathcal{P}(\mathcal{X})$, a sequence $\boldsymbol{x} \in \mathcal{X}^n$ is called ϵ-typical with respect to P_X if for all $a \in \mathcal{X}$ with $P_X(a) > 0$, we have

$$\left| \frac{N(a \,|\, \boldsymbol{x})}{n} - P_X(a) \right| \leq \epsilon,$$

and for all $a \in \mathcal{X}$ with $P_X(a) = 0, N(a \,|\, \boldsymbol{x}) = 0$. The set of such sequences will be denoted by $\mathcal{T}_{[P_X]_\epsilon}^{(n)}$ or simply by $\mathcal{T}_{[X]_\epsilon}^{(n)}$ if P_X is clear from the context. Note that $\mathcal{T}_{[P_X]_\epsilon}^{(n)} = \mathcal{T}_{P_X}^{(n)}$ if $\epsilon = 0$. The typical set $\mathcal{T}_{[U,X]_\epsilon}^{(n)}$ with respect to a joint distribution is defined similarly (see [4]).

For a conditional distribution $P_{X|U}$ defined on $\mathcal{U} \times \mathcal{X}$, a sequence $\boldsymbol{x} \in \mathcal{X}^n$ is called ϵ-typical with respect to $P_{X|U}$ conditional on $\boldsymbol{u} \in \mathcal{U}^n$ if for all $a \in \mathcal{X}$ and $b \in \mathcal{U}$ with $P_{X|U}(a \,|\, b) > 0$, we have

$$\left| \frac{N(b, a \,|\, \boldsymbol{u}, \boldsymbol{x})}{n} - \frac{N(b \,|\, \boldsymbol{u}) P_{X|U}(a \,|\, b)}{n} \right| \leq \epsilon$$

and for all $a \in \mathcal{X}$ and $b \in \mathcal{U}$ with $P_{X|U}(a \,|\, b) = 0, N(b, a \,|\, \boldsymbol{u}, \boldsymbol{x}) = 0$, where $N(b, a \,|\, \boldsymbol{u}, \boldsymbol{x})$ is the number of occurrences of the pair (b, a) in $(\boldsymbol{u}, \boldsymbol{x})$. The set of such sequences will be denoted by $\mathcal{T}_{[P_{X|U}]_\epsilon}^{(n)}(\boldsymbol{u})$ or simply by $\mathcal{T}_{[X\,|\,U]_\epsilon}^{(n)}(\boldsymbol{u})$ if $P_{X|U}$ is clear from the context. The following facts will be used in the proof of Theorem 1.

Lemma 2: [4] In what follows $\gamma = \gamma(\epsilon, n)$ is a generic positive term such that $\lim_{\epsilon\to 0}\lim_{n\to\infty}\gamma(\epsilon, n) = 0$.

a) $|\mathcal{P}_n(\mathcal{U})| \le (n+1)^{|\mathcal{U}|}$.
b) $Q_U^{(n)}(\mathcal{T}_{P_U}^{(n)}) \le \exp\{-nD(P_U\|Q_U)\}$ for all $P_U, Q_U \in \mathcal{P}_n(\mathcal{U})$.
c) $\exp\{n(H_{P_UP_{X|U}}(X\,|\,U) - \gamma)\} \le |\mathcal{T}_{[P_{X|U}]_\epsilon}^{(n)}(\boldsymbol{u})| \le \exp\{n(H_{P_UP_{X|U}}(X\,|\,U) + \gamma)\}$ for all $\boldsymbol{u} \in \mathcal{T}_{[P_U]_\epsilon}^{(n)}$.
d) If $\boldsymbol{u} \in \mathcal{T}_{[U]_\epsilon}^{(n)}$ and $\boldsymbol{x} \in \mathcal{T}_{[X\,|\,U]_\epsilon}^{(n)}(\boldsymbol{u})$, then $(\boldsymbol{u}, \boldsymbol{x}) \in \mathcal{T}_{[U,X]_\epsilon}^{(n)}$ and, consequently, $\boldsymbol{x} \in \mathcal{T}_{[X]_\epsilon}^{(n)}$.
e) If $\boldsymbol{u} \in \mathcal{T}_{[U]_\epsilon}^{(n)}$ and $\boldsymbol{x} \in \mathcal{T}_{[X\,|\,U]_\epsilon}^{(n)}(\boldsymbol{u})$, then $P_{X|U}^{(n)}(\boldsymbol{x}\,|\,\boldsymbol{u}) \ge \exp\{-n(H_{P_UP_{X|U}}(X\,|\,U) + \gamma)\}$.
f) If $(\boldsymbol{u}, \boldsymbol{x}) \in \mathcal{T}_{[U,X]_\epsilon}^{(n)}$, then $d(\boldsymbol{u}, \boldsymbol{x}) \le \mathbb{E}d(U, X) + \delta(\epsilon)$ if n sufficiently large, where $\delta(\epsilon) \to 0$ as $\epsilon \to 0$.

Remark: We note that Property d) is meant in the following sense: For any $\epsilon_1 > 0$ and $\epsilon_2 > 0$, if $\boldsymbol{u} \in \mathcal{T}_{[U]_{\epsilon_1}}^{(n)}$ and $\boldsymbol{x} \in \mathcal{T}_{[X\,|\,U]_{\epsilon_2}}^{(n)}(\boldsymbol{u})$, then $(\boldsymbol{u}, \boldsymbol{x}) \in \mathcal{T}_{[U,X]_{\epsilon_1+\epsilon_2}}^{(n)}$, and consequently $\boldsymbol{x} \in \mathcal{T}_{[X]_{\epsilon_3}}^{(n)}$ for $\epsilon_3 = (\epsilon_1+\epsilon_2)|\mathcal{U}|$. For the sake of convenience, and with a slight abuse of notation, instead of $\mathcal{T}_{[U]_{\epsilon_1}}^{(n)}, \mathcal{T}_{[X\,|\,U]_{\epsilon_2}}^{(n)}(\boldsymbol{u})$ and $\mathcal{T}_{[X]_{\epsilon_3}}^{(n)}$, we write $\mathcal{T}_{[U]_\epsilon}^{(n)}, \mathcal{T}_{[X\,|\,U]_\epsilon}^{(n)}(\boldsymbol{u})$ and $\mathcal{T}_{[X]_\epsilon}^{(n)}$ (cf. the delta convention in [4, p. 34]).

B. Proof Outline

We shall prove that for any $\delta > 0$, there exists a sequence of JQW codes (f_n, φ_n) with watermarking rate converging to R_1 and quantization rate converging to R_2 such that for n sufficiently large, the distortion satisfies

$$D(f_n, \varphi_n) \le \Delta + \delta$$

and the probability of error is bounded as

$$P_e^{(n)}(f_n, \varphi_n) \le e^{-nE_{\mathrm{QW},r}(R_1,R_2)+o(n)}$$

where $o(n)$ satisfies $\lim_{n\to\infty}\frac{o(n)}{n} = 0$. The existence of such code sequences for all $\delta > 0$ then implies the bound of Theorem 1 through a standard subsequence diagonalization procedure.

We next outline our proof. In Section III-C, we construct the code $C = (f_n, \varphi_n)$ in a random manner. In particular, the encoder f_n is randomly chosen from an ensemble of encoders, and the decoder φ_n is a maximum-likelihood decoder. In Section III-D, we show that the probability of error, when averaged over the random choice of the encoder, is upper-bounded by $e^{-nE_{\mathrm{QW},r}(R_1,R_2)+o(n)}$. In Section III-E, we show that the distortion, when averaged over the random encoder, is upper-bounded by $\Delta + \delta$ for n sufficiently large and any $\delta > 0$. Finally, in Section III-F, we complete the proof by showing that there exists at least one sequence of codes $\{C = (f_n, \varphi_n)\}$ which simultaneously satisfies the distortion constraint $\Delta + \delta$ and achieves the exponent $E_{\mathrm{QW},r}(R_1, R_2)$.

C. Code Construction

Fix $\Delta > 0$ and a conditional distribution $P_{X|U}$ such that

$$\mathbb{E}_{Q_UP_{X|U}}d(U, X) < \Delta.$$

For *each type* $P_U \in \mathcal{P}_n(\mathcal{U})$, we generate a codebook and define the encoding and decoding function as follows.

Random Code Generation: Let $R_W = \frac{1}{n}\log\lceil e^{nR_1}\rceil$ and $R_Q = \min(\frac{1}{n}\log\lfloor e^{nR_2}\rfloor, \log|\mathcal{X}|)$, where $\lceil\cdot\rceil$ and $\lfloor\cdot\rfloor$ denote the floor and ceiling functions, respectively. For type P_U satisfying

$$I_{P_UP_{X|U}}(U; X) \le \hat{R} - \eta \quad \text{and} \quad \mathbb{E}_{P_UP_{X|U}}d(U, X) < \Delta \tag{9}$$

where $\hat{R} = R_Q - R_W - |\mathcal{U}|\frac{1}{n}\log(n+1) > 0$ and $\eta \in (0, \hat{R})$ is arbitrary, generate a codebook consisting of $W_n = e^{nR_W}$ "subcodebooks" $C(P_U) = \{C_1(P_U), C_2(P_U), \ldots, C_{W_n}(P_U)\}$ where each subcodebook $C_w(P_U)$ consists of $M = \lfloor e^{n\hat{R}}\rfloor$ codewords for each $w \in \mathcal{W}_n = \{1, 2, \ldots, W_n\}$; i.e.,

$$C_w(P_U) = \{\boldsymbol{x}(w, 1, P_U), \boldsymbol{x}(w, 2, P_U), \ldots, \boldsymbol{x}(w, M, P_U)\},$$

such that each codeword $\boldsymbol{x}(w, t, P_U)$ is independently and uniformly drawn from the typical set $\mathcal{T}_{[X]_\epsilon}^{(n)}$ with respect to the distribution $P_X(x) = \sum_{\mathcal{U}} P_U(u)P_{X|U}(x\,|\,u)$. If the type P_U does not satisfy (9), then generate codebook $C_w(P_U) = \{\boldsymbol{x}_0\}$ for all $w \in \mathcal{W}_n$, where $\boldsymbol{x}_0$ is an arbitrary sequence in $\mathcal{X}^n$. Since there are at most $(n+1)^{|\mathcal{U}|}$ types in $\mathcal{P}_n(\mathcal{U})$, we have $\lim_{n\to\infty}\frac{1}{n}\log|\mathcal{W}_n| \ge R_1$ and $\lim_{n\to\infty}\frac{1}{n}\log|f_n| \le R_2$.

Watermark Embedding: Given a watermark w and a covertext $\boldsymbol{u} \in \mathcal{T}_U^{(n)} = \mathcal{T}_{P_U}^{(n)}$ (so that $P_U = P_{\boldsymbol{u}}$), the encoder chooses the first codeword $\boldsymbol{x}(w, t, P_U)$ in the codebook $C_w(P_U)$ such that $\boldsymbol{x}(w, t, P_U)$ lies in the conditional typical set $\mathcal{T}_{[X\,|\,U]_\epsilon}^{(n)}(\boldsymbol{u})$ with respect to the conditional distribution $P_{X|U}$. The output of the encoder is denoted by $\boldsymbol{x}(C_w(\boldsymbol{u}))$. If none of the codewords are in the set $\mathcal{T}_{[X\,|\,U]_\epsilon}^{(n)}(\boldsymbol{u})$, then the encoder outputs the first codeword $\boldsymbol{x}(C_1(\boldsymbol{u}))$.

Decoding: The decoder has full knowledge of $\boldsymbol{u}$, and thus generates all possible watermarked versions of $\boldsymbol{u}$, $\{\boldsymbol{x}(C_w(\boldsymbol{u}))\}_{w=1}^{W_n}$. Upon receiving $\boldsymbol{y}$, a maximum-likelihood decoder is employed; i.e., the output of the decoder satisfies

$$\hat{w} = \arg\max_{w\in\mathcal{W}_n} A_{Y\,|\,X}^{(n)}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\boldsymbol{u}))).$$

D. Average Probability of Error Analysis

Denote

$$\Phi(\eta) \triangleq \Big\{P_U \in \mathcal{P}_n(\mathcal{U}) : I_{P_UP_{X|U}}(U; X) \le \hat{R} - \eta, \text{ and } \mathbb{E}_{P_UP_{X|U}}d(U, X) < \Delta\Big\}. \tag{10}$$

For a given randomly generated codebook $C = \bigcup_{P_U\in\mathcal{P}(\mathcal{U})} C(P_U)$ with rate parameters R_W and R_Q, we write

$$P_e^{(n)}(C) = P_e^{(n)}(f_n, \varphi_n) = \frac{1}{W_n}\sum_{w=1}^{W_n} P_{e,w}^{(n)}(C)$$

where $P_{e,w}^{(n)}(C) = \Pr(\varphi_n(Y^n, U^n) \ne w\,|\,W = w)$ is the probability of error given that w is transmitted and can be expressed as

$$P_{e,w}^{(n)}(C) = \sum_{P_U\in\mathcal{P}_n(\mathcal{U})}\sum_{\boldsymbol{u}\in\mathcal{T}_U^{(n)}} Q_U^{(n)}(\boldsymbol{u}) \times \sum_{\boldsymbol{y}\in\mathcal{Y}^n} A_{Y\,|\,X}^{(n)}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\boldsymbol{u})))\mathbb{I}\{\varphi_n(\boldsymbol{y}) \ne w\}$$

$$\le \sum_{P_U \notin \Phi(\eta)} \sum_{\boldsymbol{u} \in \mathcal{T}_U^{(n)}} Q_U^{(n)}(\boldsymbol{u}) + \sum_{P_U \in \Phi(\eta)} \sum_{\boldsymbol{u} \in \mathcal{T}_U^{(n)}} Q_U^{(n)}(\boldsymbol{u}) \times \sum_{\boldsymbol{y} \in \mathcal{Y}^n} A_{Y\,|\,X}^{(n)}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\boldsymbol{u})))\mathbb{I}\{\varphi_n(\boldsymbol{y}) \neq w\} \quad (11)$$

where $\mathbb{I}A$ is the indicator of the event A. It immediately follows from Lemma 2 that

$$\sum_{P_U \notin \Phi(\eta)} \sum_{\boldsymbol{u} \in \mathcal{T}_U^{(n)}} Q_U^{(n)}(\boldsymbol{u}) \le (n+1)^{|\mathcal{U}|} e^{-n \min_{P_U \notin \Phi(\eta)} D(P_U \| Q_U)}. \quad (12)$$

Taking expectation on both sides of (11) with respect to the random choice of the codebooks we have

$$\bar{P}_{e,w}^{(n)} \triangleq \mathbb{E}\left[P_{e,w}^{(n)}(C)\right] \le (n+1)^{|\mathcal{U}|} e^{-n \min_{P_U \notin \Phi(\eta)} D(P_U \| Q_U)} + \sum_{P_U \in \Phi(\eta)} \sum_{C(P_U) \in \mathcal{C}(P_U)} \Pr(C(P_U)) \sum_{\boldsymbol{u} \in \mathcal{T}_U^{(n)}} Q_U^{(n)}(\boldsymbol{u}) \times \sum_{\boldsymbol{y} \in \mathcal{Y}^n} A_{Y\,|\,X}^{(n)}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\boldsymbol{u})))\mathbb{I}\{\varphi_n(\boldsymbol{y}) \neq w\} \quad (13)$$

where $C(P_U) = \{C_1(P_U), C_2(P_U), \ldots, C_{W_n}(P_U)\}$ and $\mathcal{C}(P_U)$ is the set of all possible codes for type P_U. For $P_U \in \Phi(\eta)$, each code $C(P_U)$ is generated according to the distribution

$$\Pr(C(P_U)) \triangleq \prod_{w' \in \mathcal{W}_n} q(C_{w'}(P_U)). \quad (14)$$

We recall that each subcode $C_{w'}(P_U)$ is generated according to distribution $q(C_{w'}) = \prod_{t=1}^{M} q(\boldsymbol{x}(w', t))$, where $q(\boldsymbol{x}(w', t)) \triangleq \frac{1}{|\mathcal{T}_{[X]_\epsilon}|}$ and $P_X(x) = \sum_{\mathcal{U}} P_U(u) P_{X|U}(x\,|\,u)$.

Define

$$\mathcal{D}_i \triangleq \left\{C_i(P_U) : \boldsymbol{x}(C_i(\boldsymbol{u})) \notin \mathcal{T}_{[X\,|\,U]_\epsilon}^{(n)}(\boldsymbol{u})\right\}$$

for $1 \le i \le W_n$. Using the union bound on the indicator function

$$\mathbb{I}\{\varphi_n(\boldsymbol{y}) \neq w\} \le \mathbb{I}\left\{\bigcap_{i=1}^{W_n} \mathcal{D}_i^c \bigcap \{\varphi_n(\boldsymbol{y}) \neq w\}\right\} + \sum_{i=1}^{W_n} \mathbb{I}\{\mathcal{D}_i\} \quad (15)$$

and substituting (14) for $\Pr(C(P_U))$, we can upper-bound the sum over $C(P_U)$ in (13) as

$$\begin{aligned}
&\sum_{C(P_U) \in \mathcal{C}(P_U)} \Pr(C(P_U)) \sum_{\boldsymbol{u} \in \mathcal{T}_U^{(n)}} Q_U^{(n)}(\boldsymbol{u}) \times \sum_{\boldsymbol{y} \in \mathcal{Y}^n} A_{Y\,|\,X}^{(n)}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\boldsymbol{u})))\mathbb{I}\{\varphi_n(\boldsymbol{y}) \neq w\} \\
&= \sum_{\boldsymbol{u} \in \mathcal{T}_U^{(n)}} Q_U^{(n)}(\boldsymbol{u}) \sum_{C_1(P_U)} \cdots \sum_{C_{W_n}(P_U)} \prod_{w' \in \mathcal{W}_n} q(C_{w'}(P_U)) \times \sum_{\boldsymbol{y} \in \mathcal{Y}^n} A_{Y\,|\,X}^{(n)}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\boldsymbol{u})))\mathbb{I}\{\varphi_n(\boldsymbol{y}) \neq w\} \\
&\le \sum_{\boldsymbol{u} \in \mathcal{T}_U^{(n)}} Q_U^{(n)}(\boldsymbol{u}) \sum_{i=1}^{W_n} \sum_{\mathcal{D}_i} q(C_1(P_U)) + \sum_{\boldsymbol{u} \in \mathcal{T}_U^{(n)}} Q_U^{(n)}(\boldsymbol{u}) \sum_{\mathcal{D}_w^c} q(C_w(P_U)) \quad (16) \\
&\times \sum_{\mathcal{D}_1^c} \cdots \sum_{\mathcal{D}_{w-1}^c} \sum_{\mathcal{D}_{w+1}^c} \cdots \sum_{\mathcal{D}_{W_n}^c} \prod_{w' \in \mathcal{W}_n : w' \neq w} q(C_{w'}(P_U)) \\
&\times \sum_{\boldsymbol{y} \in \mathcal{Y}^n} A_{Y\,|\,X}^{(n)}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\boldsymbol{u})))I\{\varphi_n(\boldsymbol{y}) \neq w\} \\
&= \sum_{\boldsymbol{u} \in \mathcal{T}_U^{(n)}} Q_U^{(n)}(\boldsymbol{u}) e^{nR_W} \sum_{\mathcal{D}_1} q(C_1(P_U)) + \sum_{\boldsymbol{u} \in \mathcal{T}_U^{(n)}} Q_U^{(n)}(\boldsymbol{u}) \sum_{\mathcal{D}_w^c} q(C_w(P_U)) \\
&\times \sum_{\boldsymbol{y} \in \mathcal{Y}^n} A_{Y\,|\,X}^{(n)}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\boldsymbol{u}))) \times \Pr\left(\{\varphi_n(\boldsymbol{y}) \neq w\} \bigcap \bigcap_{i=1, i \neq w}^{W_n} \mathcal{D}_i^c \,\middle|\, w, \boldsymbol{x}(C_w(\boldsymbol{u})), \boldsymbol{y}\right) \quad (17)
\end{aligned}$$

where in (16) we used the inequality in (15) and where (17) holds since the random codebooks $C_w(P_U)(w = 1, 2, \ldots, W_n)$ are independent and identically distributed (i.i.d.) and

$$\begin{aligned}
&\Pr\left(\{\varphi_n(\boldsymbol{y}) \neq w\} \bigcap \bigcap_{i=1, i \neq w}^{W_n} \mathcal{D}_i^c \,\middle|\, w, \boldsymbol{x}(C_w(\boldsymbol{u})), \boldsymbol{y}\right) \\
&= \sum_{\mathcal{D}_1^c} \cdots \sum_{\mathcal{D}_{w-1}^c} \sum_{\mathcal{D}_{w+1}^c} \cdots \sum_{\mathcal{D}_{W_n}^c} \prod_{w' \in \mathcal{W}_n : w' \neq w} q(C_{w'}(P_U)) \times \mathbb{I}\{\varphi_n(\boldsymbol{y}) \neq w\}. \quad (18)
\end{aligned}$$

Bounding the Conditional Probability in (17): Fix $P_U \in \Phi(\eta)$. Let w and $\boldsymbol{u} \in \mathcal{T}_{P_U}^{(n)} = \mathcal{T}_U^{(n)}$ be the encoder inputs and $\boldsymbol{y}$ be the received sequence. Assume that the subcodebook associated with w is $C_w(P_U)$, and $C_w(P_U)$ satisfies $\boldsymbol{x}(C_w(\boldsymbol{u})) \in \mathcal{T}_{[X\,|\,U]_\epsilon}^{(n)}(\boldsymbol{u})$. Define the event $E_{w'}$ for a $w' \neq w$ by

$$E_{w'} : A_{Y\,|\,X}^{(n)}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_{w'}(\boldsymbol{u}))) \ge A_{Y\,|\,X}^{(n)}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\boldsymbol{u}))) \quad \text{and} \quad \boldsymbol{x}(C_{w'}(\boldsymbol{u})) \in \mathcal{T}_{[X\,|\,U]_\epsilon}^{(n)}(\boldsymbol{u}).$$

Since the subcode $C_{w'}(P_U)$ is generated according to the distribution $q(C_{w'}(P_U)) \triangleq \prod_{t=1}^{M} q(\boldsymbol{x}(w', t, P_U))$ where $q(\boldsymbol{x}(w', t, P_U)) \triangleq \frac{1}{|\mathcal{T}_{[X]_\epsilon}|}$, we have, given $w, \boldsymbol{u}, \boldsymbol{x}(C_w(\boldsymbol{u}))$ and $\boldsymbol{y}$, that

$$\Pr(E_{w'}) = \sum_{C_{w'}(P_U) : \boldsymbol{x}(C_{w'}(\boldsymbol{u})) \in \mathcal{T}_{[X\,|\,U]_\epsilon}^{(n)}(\boldsymbol{u})} q(C_{w'}(P_U)) \times \mathbb{I}\left\{A_{Y\,|\,X}^{(n)}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_{w'}(\boldsymbol{u}))) \ge A_{Y\,|\,X}^{(n)}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\boldsymbol{u})))\right\}.$$

Thus, since the decoder uses maximum-likelihood decoding

$$\Pr\left(\{\varphi_n(\boldsymbol{y}) \neq w\} \bigcap \bigcap_{i=1, i \neq w}^{W_n} \mathcal{D}_i^c \,\middle|\, w, \boldsymbol{x}(C_w(\boldsymbol{u})), \boldsymbol{y}\right)$$

$$\leq \Pr\left(\bigcup_{w' \neq w} E_{w'}\right) \leq \sum_{w' \neq w} \Pr(E_{w'}). \quad (19)$$

Applying the bounding technique due to Gallager ([5, p. 136]), we can upper-bound the above probability for any $\rho \in [0,1]$

$$\Pr\left(\{\varphi_n(\boldsymbol{y}) \neq w\} \bigcap \bigcap_{i=1, i\neq w}^{W_n} \mathcal{D}_i^c \,\middle|\, w, \boldsymbol{x}(C_w(\boldsymbol{u})), \boldsymbol{y}\right)$$
$$\leq e^{n\rho R_W} \left[\sum_{C_{w'}(P_U):\boldsymbol{x}(C_{w'}(\boldsymbol{u}))\in\mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})} q(C_{w'}(P_U)) \times \left(\frac{A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_{w'}(\boldsymbol{u})))}{A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\boldsymbol{u})))}\right)^{\frac{1}{1+\rho}}\right]^{\rho}. \quad (20)$$

It then follows from (17) that for $P_U \in \Phi(\eta)$

$$\sum_{C(P_U)\in\mathcal{C}(P_U)} \Pr(C(P_U)) \sum_{\boldsymbol{u}\in\mathcal{T}^{(n)}_U} Q^{(n)}_U(\boldsymbol{u}) \times \sum_{\boldsymbol{y}\in\mathcal{Y}^n} A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\boldsymbol{u})))\mathbb{I}\{\varphi_n(\boldsymbol{y}) \neq w\}$$
$$\leq \sum_{\boldsymbol{u}\in\mathcal{T}^{(n)}_U} Q^{(n)}_U(\boldsymbol{u}) e^{nR_W} \Pr\left(X^n(C_w(\boldsymbol{u})) \notin \mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right) \quad (21)$$
$$+ e^{n\rho R_W} \sum_{\boldsymbol{u}\in\mathcal{T}^{(n)}_U} Q^{(n)}_U(\boldsymbol{u}) \times \sum_{\boldsymbol{y}\in\mathcal{Y}^n} \left(\sum_{C_w(P_U):\boldsymbol{x}(C_w(\boldsymbol{u}))\in\mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})} q(C_w(P_U)) \times A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\boldsymbol{u})))^{\frac{1}{1+\rho}}\right)^{1+\rho} \quad (22)$$

where (22) follows from (20) and the random vector $X^n(C_w(\boldsymbol{u}))$ denotes the output of the encoder.

Bounding the Probability in (21): Since each codeword $X^n(w,t,P_U)$ in $C_w(P_U)$ is selected i.i.d. according to the uniform distribution $q(\boldsymbol{x}) = |\mathcal{T}^{(n)}_{[X]_\epsilon}|^{-1}$ on $\mathcal{T}^{(n)}_{[X]_\epsilon}$, by Lemma 2 d), we have

$$\Pr\left(X^n(w,t,P_U) \notin \mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right) \leq 1 - \frac{\left|\mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right|}{\left|\mathcal{T}^{(n)}_{[X]_\epsilon}\right|}$$

and thus by Lemma 2

$$\Pr\left(X^n(C_w(\boldsymbol{u})) \notin \mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right) \leq \prod_{t=1}^{M} \Pr\left(X^n(w,t,P_U) \notin \mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right) \leq \left[1 - \frac{\exp\left[n\left(H(X\,|\,U) - \frac{\eta}{2}\right)\right]}{\exp\left[n\left(H(X) + \frac{\eta}{4}\right)\right]}\right]^{e^{n\hat{R}}} = \left[1 - e^{-n(I(U;X)+\frac{\eta}{4})}\right]^{e^{n\hat{R}}}$$

for ϵ sufficiently small and n sufficiently large. Applying the inequality $(1-s)^m \leq e^{-sm}$ for $0 \leq s \leq 1$ and recalling that $\hat{R} - I(U;X) \geq \eta$ for $P_U \in \Phi(\eta)$ we have

$$e^{nR_W} \Pr\left(X^n(C_w(\boldsymbol{u})) \notin \mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right) \leq e^{nR_W} e^{-e^{n\left[\hat{R} - I(U;X) - \frac{\eta}{4}\right]}} \leq \exp\left(-\exp\left(\frac{n\eta}{4}\right) + nR_W\right) \quad (23)$$

which vanishes double-exponentially.

Bounding (22): Note that

$$\sum_{C_w(P_U):\boldsymbol{x}(C_w(\boldsymbol{u}))\in\mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})} q(C_w(P_U)) A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\boldsymbol{u})))^{\frac{1}{1+\rho}}$$
$$= \sum_{\boldsymbol{x}(w,1,P_U)\in\mathcal{T}^{(n)}_{[X]_\epsilon}} \cdots \sum_{\boldsymbol{x}(w,M,P_U)\in\mathcal{T}^{(n)}_{[X]_\epsilon}} \prod_{t=1}^{M} q(\boldsymbol{x}(w,t,P_U)) \times A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\boldsymbol{u})))^{\frac{1}{1+\rho}} \mathbb{I}\left\{\boldsymbol{x}(C_w(\boldsymbol{u})) \in \mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right\}$$
$$= \sum_{i=1}^{M} \sum_{\boldsymbol{x}(w,1,P_U)\in\mathcal{T}^{(n)}_{[X]_\epsilon}} \cdots \sum_{\boldsymbol{x}(w,M,P_U)\in\mathcal{T}^{(n)}_{[X]_\epsilon}} \prod_{t=1}^{M} q(\boldsymbol{x}(w,t,P_U)) \times A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x}(w,i,P_U)))^{\frac{1}{1+\rho}} \mathbb{I}\left\{\boldsymbol{x}(w,i,P_U) \in \mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right\} \prod_{j=1}^{i-1} \mathbb{I}\left\{\boldsymbol{x}(w,j,P_U) \notin \mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right\}$$
$$= \sum_{i=1}^{M} \left(\sum_{\boldsymbol{x}\in\mathcal{T}^{(n)}_{[X]_\epsilon}} q(\boldsymbol{x}) \mathbb{I}\left\{\boldsymbol{x} \notin \mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right\}\right)^{i-1} \sum_{\boldsymbol{x}\in\mathcal{T}^{(n)}_{[X]_\epsilon}} q(\boldsymbol{x}) A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x})^{\frac{1}{1+\rho}} \mathbb{I}\left\{\boldsymbol{x} \in \mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right\} \quad (24)$$
$$\leq \frac{1}{1 - \Pr\left(X^n \notin \mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right)} \sum_{\boldsymbol{x}\in\mathcal{T}^{(n)}_{[X]_\epsilon}} \frac{1}{\left|\mathcal{T}^{(n)}_{[X]_\epsilon}\right|} \times A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x})^{\frac{1}{1+\rho}} \mathbb{I}\left\{\boldsymbol{x} \in \mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right\} \quad (25)$$
$$\leq \sum_{\boldsymbol{x}\in\mathcal{T}^{(n)}_{[X]_\epsilon}} \frac{1}{\left|\mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right|} A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x})^{\frac{1}{1+\rho}} \mathbb{I}\left\{\boldsymbol{x} \in \mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right\} \quad (26)$$

where in (24) we use the fact that the codewords $\boldsymbol{x}(w,1),\ldots,\boldsymbol{x}(w,M)$ are generated i.i.d. according to $q(\cdot), X^n$ in (25) denotes an RV drawn i.i.d. according to $q(\boldsymbol{x}) = \frac{1}{|\mathcal{T}^{(n)}_{[X]_\epsilon}|}$ on $\mathcal{T}^{(n)}_{[X]_\epsilon}$, and the inequality follows from

$$\sum_{i=1}^{M} q^{i-1} \leq 1/(1-q), \quad \text{for all } q \in (0,1).$$

Also, (26) follows from the inequality

$$\Pr\left(X^n \notin \mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right) \leq 1 - \frac{\left|\mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right|}{\left|\mathcal{T}^{(n)}_{[X]_\epsilon}\right|}$$

which holds since $\mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon} \subset \mathcal{T}^{(n)}_{[X]_\epsilon}$ by Lemma 2. Also from Lemma 2 we know that $\boldsymbol{u} \in \mathcal{T}^{(n)}_U$ and $\boldsymbol{x} \in \mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})$ imply that for any $\eta > 0$

$$P^{(n)}_{X|U}(\boldsymbol{x}\,|\,\boldsymbol{u}) \geq e^{-n(H(X\,|\,U)+\frac{\eta}{2})} = e^{-n\eta}e^{-n(H(X\,|\,U)-\frac{\eta}{2})} \geq e^{-n\eta}\frac{1}{\left|\mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right|} \quad (27)$$

if ϵ is sufficiently small and n is sufficiently large. It then follows from (26) and (27) that

$$\begin{aligned}&\sum_{C_w(P_U):\boldsymbol{x}(C_{w'}(\boldsymbol{u}))\in\mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})} q(C_w(P_U))A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\boldsymbol{u})))^{\frac{1}{1+\rho}}\\ &\quad\leq e^{n\eta}\sum_{\boldsymbol{x}\in\mathcal{T}^{(n)}_{[X]_\epsilon}} P^{(n)}_{X|U}(\boldsymbol{x}\,|\,\boldsymbol{u})A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x})^{\frac{1}{1+\rho}}\\ &\quad\leq e^{n\eta}\sum_{\boldsymbol{x}\in\mathcal{X}^n} P^{(n)}_{X|U}(\boldsymbol{x}\,|\,\boldsymbol{u})A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x})^{\frac{1}{1+\rho}}\end{aligned}$$

for ϵ sufficiently small and n sufficiently large. Since $0 \leq \rho \leq 1$ we can bound the term in (22), which we now denote by P_0, as

$$P_0 \leq \min_{0\leq\rho\leq 1}\left[e^{n(\rho R_W+\eta)}\sum_{\boldsymbol{u}\in\mathcal{T}^{(n)}_U} Q^{(n)}_U(\boldsymbol{u}) \times\sum_{\mathcal{Y}^n}\left(\sum_{\mathcal{X}^n} P^{(n)}_{X|U}(\boldsymbol{x}\,|\,\boldsymbol{u})A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x})^{\frac{1}{1+\rho}}\right)^{1+\rho}\right] \quad (28)$$

for ϵ sufficiently small and n sufficiently large. Therefore, on account of (10), (11), and (22), the probability of error (averaged over all codes) is upper-bounded by

$$\begin{aligned}\bar{P}^{(n)}_e &= \frac{1}{W}\sum_{w=1}^{W}\bar{P}^{(n)}_{e,w}\\ &\leq \min_{0\leq\rho\leq 1}\left[e^{n(\rho R_W+\eta)}\sum_{\mathcal{U}^n} Q^{(n)}_U(\boldsymbol{u})\sum_{\mathcal{Y}^n}\left(\sum_{\mathcal{X}^n} P^{(n)}_{X|U}(\boldsymbol{x}\,|\,\boldsymbol{u})A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x})^{\frac{1}{1+\rho}}\right)^{1+\rho}\right]\\ &\quad+(n+1)^{|\mathcal{U}|}e^{-n\min_{P_U\notin\Phi(\eta)}D(P_U\|Q_U)}\\ &\quad+\exp\left(-\exp\left(\frac{n\eta}{2}\right)+nR_W\right)\end{aligned}$$

for ϵ sufficiently small and n sufficiently large. Recall that $P_{X|U}$ is chosen arbitrarily from $\{P_{X|U} : \mathbb{E}_{Q_U P_{X|U}}(U,X) \leq \Delta\}$ and $\eta > 0$ is arbitrarily chosen. It is easy to show that $\min_{P_U\notin\Phi(\eta)} D(P_U\|Q_U)$ converges to $F(Q_U, P_{X|U}, \Delta, \hat{R}-\eta)$ as $n \to \infty$, since for any distribution $P_U \in \mathcal{P}(\mathcal{U})$, for large enough n we can find an appropriate type $\tilde{P}_U \in \mathcal{P}_n(\mathcal{U})$ to approximate it. Thus, by taking the minimum of the averaged probability of error over all possible $P_{X|U}$'s, and by letting $\eta \to 0$, on account of Proposition 1, we obtain that

$$\bar{P}^{(n)}_e \leq e^{-nE_{\mathrm{QW},r}(R_1,R_2)+o(n)}. \quad (29)$$

E. Average Distortion Analysis

Define

$$\mathcal{E}(C_w(P_U), P_U) \triangleq \left\{\boldsymbol{u}\in\mathcal{T}^{(n)}_{P_U} = \mathcal{T}^{(n)}_U : \boldsymbol{x}(C_w(\boldsymbol{u}))\notin\mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right\}. \quad (30)$$

By Lemma 2, for $P_U \in \Phi(\eta), \boldsymbol{u}\in\mathcal{T}^{(n)}_U$ and $\boldsymbol{x}\in\mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})$, the distortion is upper-bounded by

$$d(\boldsymbol{u},\boldsymbol{x}) \leq \mathbb{E}_{P_U P_{X|U}} d(U,X) + \frac{\delta}{2} \leq \Delta + \frac{\delta}{2} \quad (31)$$

for n sufficiently large. The distortion for a fixed code C with rate parameters R_W and R_Q is given by

$$\begin{aligned}D^{(n)}(C) &= D(f_n,\varphi_n)\\ &= \sum_{w=1}^{W}\frac{1}{W}\sum_{P_U\in\mathcal{P}_n(\mathcal{U})}\sum_{\boldsymbol{u}\in\mathcal{T}^{(n)}_U} Q^{(n)}_U(\boldsymbol{u})d(\boldsymbol{u},\boldsymbol{x}(C_w(\boldsymbol{u})))\\ &\leq \sum_{w=1}^{W}\frac{1}{W}\sum_{P_U\in\Phi(\eta)}\sum_{\boldsymbol{u}\in\mathcal{T}^{(n)}_U} Q^{(n)}_U(\boldsymbol{u})d(\boldsymbol{u},\boldsymbol{x}(C_w(\boldsymbol{u})))\\ &\quad+d_m\sum_{w=1}^{W}\frac{1}{W}\sum_{P_U\notin\Phi(\eta)}\sum_{\boldsymbol{u}\in\mathcal{T}^{(n)}_U} Q^{(n)}_U(\boldsymbol{u})\\ &= \sum_{w=1}^{W}\frac{1}{W}\sum_{P_U\in\Phi(\eta)}\left[\sum_{\boldsymbol{u}\in\mathcal{T}^{(n)}_U\setminus\mathcal{E}(C_w(P_U),P_U)} Q^{(n)}_U(\boldsymbol{u})\times d(\boldsymbol{u},\boldsymbol{x}(C_w(\boldsymbol{u})))\right.\\ &\qquad\left.+\sum_{\boldsymbol{u}\in\mathcal{E}(C_w(P_U),P_U)} Q^{(n)}_U(\boldsymbol{u})d(\boldsymbol{u},\boldsymbol{x}(C_w(\boldsymbol{u})))\right]\\ &\quad+d_m\sum_{w=1}^{W}\frac{1}{W}\sum_{P_U\notin\Phi(\eta)}\sum_{\boldsymbol{u}\in\mathcal{T}^{(n)}_U} Q^{(n)}_U(\boldsymbol{u})\\ &\leq \Delta+\frac{\delta}{2}+d_m\sum_{w=1}^{W}\frac{1}{W}\sum_{P_U\in\Phi(\eta)}\sum_{\boldsymbol{u}\in\mathcal{T}^{(n)}_U} Q^{(n)}_U(\boldsymbol{u})\\ &\quad\times\mathbb{I}\left\{\boldsymbol{x}(C_w(\boldsymbol{u}))\notin\mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right\}\\ &\quad+d_m(n+1)^{|\mathcal{U}|}e^{-n\min_{P_U\notin\Phi(\eta)}D(P_U\|Q_U)} \quad (32)\end{aligned}$$

where in (32) we used the bound of (31), the definition of the set $\mathcal{E}(C_w(P_U), P_U)$ in (30), and the bound (12). Now taking the expectation of $D^{(n)}(C)$ with respect to the random choice of C, we have

$$\begin{aligned}\bar{D}^{(n)} &\triangleq \mathbb{E}[D^{(n)}(C)] \leq \Delta+\frac{\delta}{2}\\ &\quad+d_m(n+1)^{|\mathcal{U}|}e^{-n\min_{P_U\notin\Phi(\eta)}D(P_U\|Q_U)}\\ &\quad+d_m\sum_{w=1}^{W}\frac{1}{W}\sum_{P_U\in\Phi(\eta)}\sum_{\boldsymbol{u}\in\mathcal{T}^{(n)}_U} Q^{(n)}_U(\boldsymbol{u})\\ &\quad\times\Pr\left(X^n(C_w(\boldsymbol{u}))\notin\mathcal{T}^{(n)}_{[X\,|\,U]_\epsilon}(\boldsymbol{u})\right).\end{aligned}$$

From the continuity of $F(P_U, P_{X|U}, \Delta, R)$ in R (see Proposition 1) we have that $\min_{P_U\notin\Phi(\eta)} D(P_U\|Q_U)$ is arbitrarily

close to $F(Q_U, P_{X|U}, \Delta, \hat{R})$ if n is sufficiently large and η sufficiently small. By (23)

$$\begin{aligned}\bar{D}^{(n)} &\le \Delta + \frac{\delta}{2} + d_m(n+1)^{|\mathcal{U}|}e^{-n\min_{P_U \notin \Phi(\eta)} D(P_U\|Q_U)} \\ &\quad + d_m \exp\left(-\exp\left(\frac{n\eta}{4}\right)\right) \\ &\le \Delta + \delta \end{aligned} \tag{33}$$

for n sufficiently large and η sufficiently small.

F. The Existence of Good Codes

The last step of the proof is to show that there exists a sequence of codes $\{C = (f_n, \varphi_n)\}$ such that the probability of error $P_e^{(n)} = P_e^{(n)}(C)$ is bounded by $e^{-nE_{\mathrm{QW},r}(R_1,R_2)+o(n)}$ and simultaneously the distortion satisfies $D^{(n)} = D^{(n)}(C) \le \Delta + \delta$ for ϵ sufficiently small and n sufficiently large. In the proof, we follow a method in [20] and [22]. Without loss of generality, assume that $E_{\mathrm{QW},r}(R_1, R_2) > 0$. Let $\mathcal{C}_e \subseteq \mathcal{C}$ be the collection of all codes satisfying

$$P_e^{(n)}(C) \le \exp\left[(-nE_{\mathrm{QW},r}(R_1,R_2) + o(n))\left(1 - \frac{1}{\sqrt{n}}\right)\right].$$

Since each code C is randomly generated according to the distribution $q(C) = \prod_{w=1}^{W} q(C_w(P_U))$, it follows from Markov's inequality that

$$\Pr(C \in \mathcal{C}_e) \ge 1 - [\exp(-nE_{\mathrm{QW},r}(R_1,R_2) + o(n))]^{\frac{1}{\sqrt{n}}}$$

for ϵ sufficiently small n sufficiently large. This implies that

$$\begin{aligned}\sum_{\mathcal{C}_e} \frac{q(C)}{\Pr(C \in \mathcal{C}_e)} D^{(n)}(C) \\ \le \frac{\Delta + \delta}{1 - \exp\left[-\sqrt{n}\left(E_{\mathrm{QW},r}(R_1,R_2) + \frac{o(n)}{n}\right)\right]}.\end{aligned}$$

Since

$$\exp\left[-\sqrt{n}\left(E_{\mathrm{QW},r}(R_1,R_2) + \frac{o(n)}{n}\right)\right] \to 0$$

as $n \to \infty$, it is seen that there exists a sequence of codes simultaneously satisfying $P_e^{(n)}(C) \le [\exp(-nE_{\mathrm{QW},r}(R_1,R_2) + o(n))]^{1-\frac{1}{\sqrt{n}}}$ and $D^{(n)}(C) < \Delta + 2\delta$ for ϵ sufficiently small and n sufficiently large. By the definition of error exponent, we obtain the desired lower bound $E_{\mathrm{QW},r}(R_1, R_2)$. □

IV. Memoryless Gaussian Systems

We next extend our results to systems which consist of memoryless Gaussian host sources and attack channels with memoryless Gaussian additive noise. Let the host source Q_U be a memoryless Gaussian source (MGS) with alphabet $\mathcal{U} = \mathbb{R}$, mean zero, variance σ_U^2, and probability density function (pdf)

$$Q_U(u) = \frac{1}{\sqrt{2\pi\sigma_U^2}} \exp\left\{-\frac{u^2}{2\sigma_U^2}\right\}, \quad u \in \mathbb{R}$$

denoted by $Q_U \sim \mathcal{N}(0, \sigma_U^2)$. Let the attack channel $A_{Y|X}$ be a memoryless channel with additive Gaussian noise (referred to as a MGC) with common input, output, and noise alphabets $\mathcal{X} = \mathcal{Y} = \mathcal{Z} = \mathbb{R}$ and described by $Y_i = X_i + Z_i$, where Y_i, X_i, and Z_i are the channel's output, input, and noise symbols at time i. We assume that $\{Z_i\}$ is an i.i.d. sequence and $\{X_i\}$ and $\{Z_i\}$ are independent. The noise admits a zero-mean D_A-variance Gaussian pdf, denoted by $P_Z \sim \mathcal{N}(0, D_A)$, and thus the transition pdf of the channel is given by

$$A_{Y|X}(y|x) = P_Z(z) = \frac{1}{\sqrt{2\pi D_A}} \exp\left\{-\frac{z^2}{2D_A}\right\}, \quad z = y - x \in \mathbb{R}.$$

We consider the squared-error (quadratic) distortion measure so that $d(u, x) = (u - x)^2$ and

$$d(\boldsymbol{u}, \boldsymbol{x}) = \frac{1}{n}\sum_{i=1}^{k}(u_i - x_i)^2$$

for any $\boldsymbol{u}, \boldsymbol{x} \in \mathbb{R}^n$.

We next extend the concept of an ϵ-typical class for DMSs to MGSs. In [1, Sec. VI. A] and [23], a continuous-alphabet analog to the ϵ-typical class was studied for the MGS (referred to as Gaussian type classes in [1] and [23]). Given $\sigma^2 > 0$ and $\epsilon \in (0, \sigma^2)$, define the Gaussian ϵ-typical set by

$$\mathcal{T}_{[\sigma^2]_\epsilon}^{(n)} \triangleq \left\{\boldsymbol{u} \in \mathbb{R}^n : \left|\frac{1}{n}\boldsymbol{u}^T\boldsymbol{u} - \sigma^2\right| \le \epsilon\right\}$$

where $\boldsymbol{u}$ is viewed as a column vector and T denotes transposition. For $\Delta > 0, \sigma^2 > 0$, and $\gamma > \max(1, \frac{\sigma^2}{\Delta})$, define

$$f(\Delta, \sigma^2, \gamma) \triangleq \frac{\gamma(\sigma^2 + \Delta) - 2\sigma^2 + 2\sqrt{\sigma^2(\gamma\Delta - \sigma^2)(\gamma - 1)}}{\gamma^2}. \tag{34}$$

We point out that $f(\Delta, \sigma^2, \gamma)$ is the larger of the two roots of the equation

$$\frac{(\sigma^2 + \gamma x - \Delta)^2}{4\sigma^2} + x = \gamma x. \tag{35}$$

For any $\alpha > 0$, consider a "test channel" $P_{X|U}$

$$X = \alpha U + V$$

where $V \sim \mathcal{N}(0, f(\Delta, \sigma^2, \gamma))$ is independent of U. In other words, $P_{X|U}$ is an auxiliary scaled MGC. Following the notion of the Gaussian ϵ-typical set, define the conditional ϵ-typical set given $\boldsymbol{u}$ with respect to the test channel $P_{X|U}$ by

$$\begin{aligned}&\mathcal{T}_{[\alpha|\sigma^2]_\epsilon}^{(n)}(\boldsymbol{u}) \\ &\quad \triangleq \left\{\boldsymbol{x} : \begin{array}{l}\boldsymbol{x} = \alpha\boldsymbol{u} + \boldsymbol{v}, \\ \left|\frac{1}{n}\boldsymbol{v}^T\boldsymbol{v} - f(\Delta, \sigma^2, \gamma)\right| \le \epsilon, \quad \left|\frac{1}{n}\boldsymbol{v}^T\boldsymbol{u}\right| \le \epsilon\end{array}\right\}.\end{aligned}$$

Similarly to the discrete ϵ-typical set and conditional ϵ-typical set, the Gaussian ϵ-typical set and conditional ϵ-typical set have the following properties.

Lemma 3: Let $\mathrm{Vol}\{A\} \triangleq \int_A d\boldsymbol{u}$ denote the volume (Lebesgue measure) of a Borel set $A \subset \mathbb{R}^n$. Let Q_U be an MGS such that $Q_U \sim \mathcal{N}(0, \sigma_U^2)$. Let $0 < \epsilon < \sigma^2$.

a) $\mathrm{Vol}\{\mathcal{T}_{[\sigma^2]_\epsilon}\} \le [2\pi e(\sigma^2 + \epsilon)]^{n/2}$.

b)

$$Q_U^{(n)}\left(\mathcal{T}_{[\sigma^2]_\epsilon}\right) \le \exp\left\{-n\left[\frac{1}{2}\left(\frac{\sigma^2}{\sigma_U^2}-\log\frac{\sigma^2}{\sigma_U^2}-1\right)+\zeta_1(\epsilon)\right]\right\}$$

where

$$\zeta_1(\epsilon) \triangleq -\frac{\epsilon}{2\sigma_U^2}-\frac{1}{2}\log\left(1+\frac{\epsilon}{\sigma^2}\right).$$

c) For any $0<\epsilon<\min(\sigma^2, f(\Delta,\sigma^2,\gamma))$ and $\boldsymbol{u}\in\mathcal{T}^{(n)}_{[\sigma^2]_\epsilon}$

$$\mathrm{Vol}\left\{\mathcal{T}^{(n)}_{[\alpha\,|\,\sigma^2]_\epsilon}(\boldsymbol{u})\right\} \ge \left[1-\frac{f(\Delta,\sigma^2,\gamma)+\sqrt{f(\Delta,\sigma^2,\gamma)\sigma_U^2}}{n\epsilon^2}\right] \times\left[2\pi e^{(1-\epsilon/f(\Delta,\sigma^2,\gamma))}f(\Delta,\sigma^2,\gamma)\right]^{n/2}.$$

Properties a)–c) can be found in [1] (note that in [1] the test channel as well as the conditional Gaussian ϵ-typical set are defined slightly differently). For the sake of completeness, we provide a proof for Lemma 3 in Appendix B.

For any $\sigma^2>0$ and an MGS $Q_U\sim\mathcal{N}(0,\sigma_U^2)$, define

$$\hat{F}(Q_U,\sigma^2)\triangleq\frac{1}{2}\left(\frac{\sigma^2}{\sigma_U^2}-\log\frac{\sigma^2}{\sigma_U^2}-1\right)$$

which is a continuous strictly increasing function of σ^2 for $\sigma^2\ge\sigma_U^2$ and is zero if and only if $\sigma^2=\sigma_U^2$. Given any $\Delta>0,\sigma^2>0,\gamma>0$, an MGS $Q_U\sim\mathcal{N}(0,\sigma_U^2)$, and an MGC $A_{Y\,|\,X}$ with noise $P_Z\sim\mathcal{N}(0,D_A)$, for any $R>0$, define

$$\hat{E}_r(Q_U,A_{Y\,|\,X},\Delta,\sigma^2,\gamma,R) \triangleq \max_{0\le\rho\le1}[\hat{E}_o(Q_U,A_{Y\,|\,X},\Delta,\sigma^2,\gamma,\rho)-\rho R] \quad (36)$$

where

$$\hat{E}_o(Q_U,A_{Y\,|\,X},\Delta,\sigma^2,\gamma,\rho) \triangleq -\log\int_{\mathcal{U}}Q_U(u)\int_{\mathcal{Y}}\left(\int_{\mathcal{X}}P_V(x-\alpha(\Delta,\sigma^2,\gamma)u)A_{Y\,|\,X}^{\frac{1}{1+\rho}}(y\,|\,x)dx\right)^{1+\rho}dydu$$

where $P_V\sim\mathcal{N}(0,f(\Delta,\sigma^2,\gamma))$, $f(\Delta,\sigma^2,\gamma)$ is defined in (34) and $\alpha(\Delta,\sigma^2,\gamma)$ is defined by

$$\alpha(\Delta,\sigma^2,\gamma)\triangleq\frac{\sigma^2+\gamma f(\Delta,\sigma^2,\gamma)-\Delta}{2\sigma^2}.$$

After some algebraic simplifications, we see that $\hat{E}_o(Q_U,A_{Y\,|\,X},\Delta,\sigma^2,\gamma,\rho)$ actually does not depend on σ^2 and can be expressed as

$$\hat{E}_o(Q_U,A_{Y\,|\,X},\Delta,\sigma^2,\gamma,\rho)=\frac{\rho}{2}\log\left(1+\frac{f(\Delta,\sigma_U^2,\gamma)}{D_A(1+\rho)}\right)$$

which is concave in ρ. It is easy to see that $\hat{E}_o(Q_U,A_{Y\,|\,X},\Delta,\sigma_U^2,\gamma,0)=0$ and that (see also (7))

$$\left.\frac{\partial\hat{E}_o(Q_U,A_{Y\,|\,X},\Delta,\sigma_U^2,\gamma,\rho)}{\partial\rho}\right|_{\rho=0}=\frac{1}{2}\log\left(1+\frac{f(\Delta,\sigma_U^2,\gamma)}{D_A}\right)=I_{Q_UP_{X|U}A_{Y\,|\,X}}(X;Y\,|\,U)$$

which implies that $\hat{E}_r(Q_U,A_{Y\,|\,X},\sigma^2,\gamma,R)>0$ if

$$R<\frac{1}{2}\log\left(1+\frac{f(\Delta,\sigma_U^2,\gamma)}{D_A}\right).$$

Defining the JQW error exponent $E_{\mathrm{QW}}(R_1,R_2)$ for the MGS-MGC system as in Definition 3 (with DMS and DMC replaced by MGS and MGC, respectively), we obtain the following.

Theorem 2: Given $R_1>0$ and $R_2>0$, for the MGS covertext Q_U and the attack MGC $A_{Y\,|\,X}$

$$E_{\mathrm{QW}}(R_1,R_2)\ge\hat{E}_{\mathrm{QW},r}(R_1,R_2) \triangleq\max_{\sigma^2\ge\sigma_U^2}\min\{\hat{F}(Q_U,\sigma^2),\hat{E}_r(Q_U,A_{Y\,|\,X},\Delta,\sigma^2,R_1)\} \quad (37)$$

where

$$\hat{E}_r(Q_U,A_{Y\,|\,X},\Delta,\sigma^2,R_1)=\sup_{\gamma\in\left[\max\left(1,\frac{\sigma_U^2}{\Delta}\right),e^{2(R_2-R_1)}\right)}\hat{E}_r(Q_U,A_{Y\,|\,X},\Delta,\sigma^2,\gamma,R_1).$$

It was shown in [9] that for an MGS Q_U with the quadratic distortion measure, an MGC $A_{Y\,|\,X}$ with noise variance D_A, and a distortion level $\Delta>0$, the private quantization/watermarking achievable region is given by (38) shown at the bottom of the following page.

Corollary 2: For the Gaussian JQW system, $\hat{E}_{\mathrm{QW},r}(R_1,R_2)>0$ for any $(R_1,R_2)\in\mathrm{int}(\hat{\mathcal{C}}(\Delta))$.

Proof: It suffices to show that if there exists a $\gamma^*\in[\max(1,\frac{\sigma_U^2}{\Delta}),e^{2R_2}]$ such that $R_1<R_2-\log\gamma^*$ and

$$R_1<\frac{1}{2}\log\left(1+\frac{f(\Delta,\sigma_U^2,\gamma^*)}{D_A}\right)\triangleq g\left(\sigma_U^2\right)$$

$$\hat{\mathcal{C}}(\Delta)=\left\{(R_1,R_2):\begin{array}{c}R_2\ge\max\left\{\frac{1}{2}\log\frac{\sigma_U^2}{\Delta},0\right\}\\ 0<R_1\le\max\limits_{\gamma\in[\max(1,\frac{\sigma_U^2}{\Delta}),e^{2R_2}]}\min\left\{R_2-\frac{1}{2}\log\gamma,\frac{1}{2}\log\left(1+\frac{f(\Delta,\sigma_U^2,\gamma)}{D_A}\right)\right\}\end{array}\right\}. \quad (38)$$

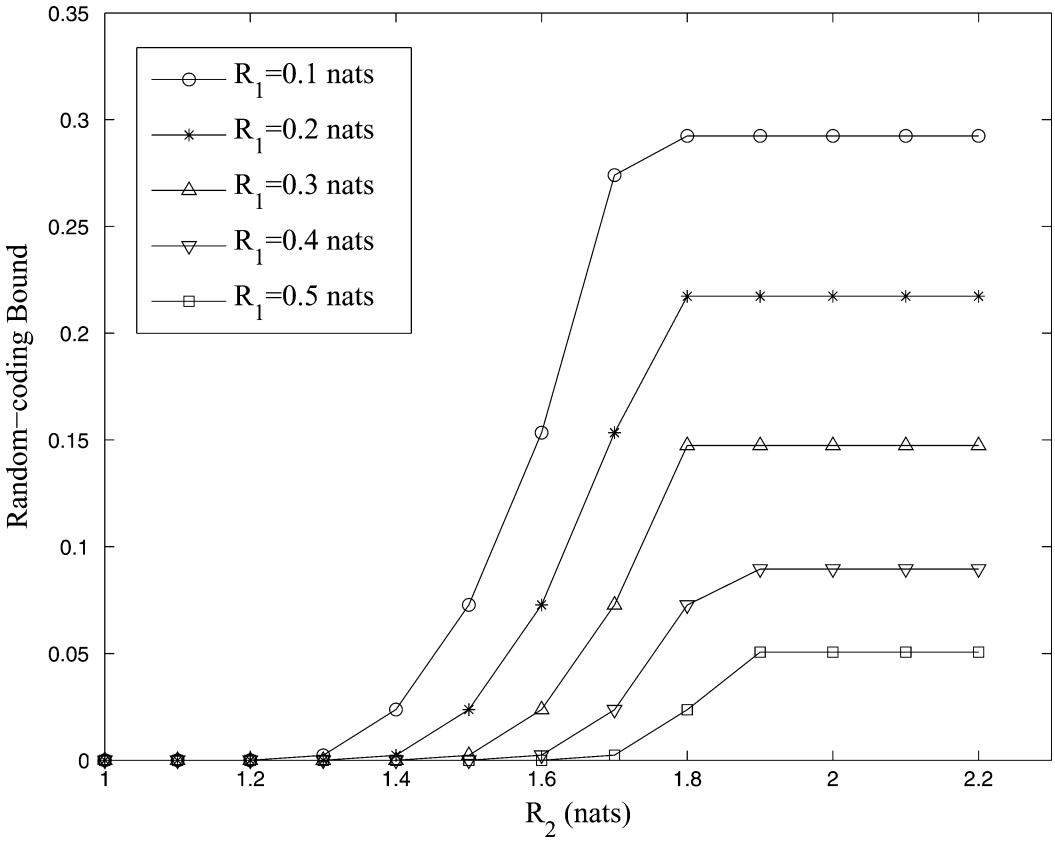

Fig. 4. The random-coding lower bound $\hat{E}_{\mathrm{QW},r}(R_1, R_2)$ versus R_2 for the Gaussian JQW system of Example 2.

then $\hat{E}_{\mathrm{QW},r}(R_1,R_2) > 0$. First, $R_1 < g(\sigma_U^2)$ implies that $\hat{E}_r(Q_U, A_{Y\,|\,X}, \Delta, \sigma_U^2, \gamma^*, R_1) > 0$. Noting that $\hat{E}_r(Q_U, A_{Y\,|\,X}, \Delta, \sigma_U^2, \gamma^*, R_1)$ is a continuous function of σ_U^2, there exists a $\sigma^2 = \sigma_U^2 + \epsilon$ for $\epsilon > 0$ small enough such that $\hat{E}_r(Q_U, A_{Y\,|\,X}, \Delta, \sigma^2, \gamma^*, R_1) > 0$. Second, since $\epsilon > 0$, we have $\hat{F}(Q_U, \sigma_U^2 + \epsilon) > 0$. Therefore, for such γ^*, by choosing $\sigma^2 = \sigma_U^2 + \epsilon$, we have

$$\hat{E}_{\mathrm{QW},r}(R_1,R_2) \geq \min\{\hat{F}(Q_U,\sigma^2), \hat{E}_r(Q_U, A_{Y\,|\,X}, \Delta, \sigma^2, \gamma^*, R_W)\} > 0. \quad \square$$

Example 2: Consider the Gaussian JQW system with $\sigma_U^2 = 1, D_A = 0.025$, and $\Delta = 0.1$. We plot the lower bound $\hat{E}_{\mathrm{QW},r}(R_1,R_2)$ against R_2 for different values of R_1 in Fig. 4. As expected, $\hat{E}_{\mathrm{QW},r}(R_1,R_2)$ is nonincreasing in R_1 and nondecreasing in R_2. Fig. 4 shows that just as in the discrete case, our lower bound does not depend on R_2 if R_2 is large enough. In Fig. 5, we plot the quantization–watermarking rate region. In $\mathbf{A}$ and $\mathbf{B}$, our lower bound $\hat{E}_{\mathrm{QW},r}(R_1,R_2)$ is positive, and in $\mathbf{C}$ (including the boundary), $\hat{E}_{\mathrm{QW},r}(R_1,R_2)$ is zero. The region $\mathbf{A} \cup \mathbf{B}$ is equal to the achievable rate region $\hat{\mathcal{C}}(\Delta)$ given in (38). The boundary between $\mathbf{A}$ and $\mathbf{B}$ determines the rate $R_2' = R_2'(R_1)$ such that $\hat{E}_{\mathrm{QW},r}(R_1,R_2) = \hat{E}_{\mathrm{QW},r}(R_1,R_2')$ for all $R_2 \geq R_2'$; i.e., for R_2 rates larger than R_2', our lower bound is constant with respect to R_2 and only depends on R_1. For example, when $R_1 = 0.3$ nats, $R_2' = 1.789$ nats, which means that $\hat{E}_{\mathrm{QW},r}(0.3,R_2) = \hat{E}_{\mathrm{QW},r}(0.3,1.789)$ for $R_2 \geq 1.789$ nats, and for $R_1 = 0.7$ nats, $R_2' = 1.933$ nats, which means that $\hat{E}_{\mathrm{QW},r}(0.7,R_2) = \hat{E}_{\mathrm{QW},r}(0.7,1.933)$ for $R_2 \geq 1.933$ nats. It has been shown in [9] that when $R_2 \geq R_2^* \triangleq \frac{1}{2}\log(1 + \frac{\sigma_U^2+\Delta}{D_A} + \frac{\sigma_U^2}{\Delta})$, the maximum watermarking rate is a constant and equal to $R_{1,\max} \triangleq \frac{1}{2}\log(1+\frac{\Delta}{D_A})$. For comparison, in our example, $R_2^* = 2.003$ nats and $R_{1,\max} = 0.804$ nats.

V. Proof of Theorem 2

The essential idea of the proof follows that of Theorem 1; i.e., it is based on the method of types and a random-coding argument.

Setup: Let $R_W = \frac{1}{n}\log\lceil e^{nR_1}\rceil$ and $R_Q = \frac{1}{n}\log\lfloor e^{nR_2}\rfloor$. Let the maximum in the definition of $\hat{E}_{\mathrm{QW},r}(R_1,R_2)$ be achieved by $\sigma_m^2 \geq \sigma_U^2$; i.e.,

$$\hat{E}_{\mathrm{QW},r}(R_1,R_2) = \min\left\{\hat{F}(Q_U,\sigma_m^2), \hat{E}_r(Q_U, A_{Y\,|\,X}, \Delta, \sigma_m^2, R_1)\right\}.$$

Fix $\gamma \in [\max(1, \frac{\sigma_m^2}{\Delta}), e^{2(R_Q - R_W - \eta)})$, where $\eta \in (0, R_Q - R_W)$ is arbitrary, and let

$$E(\gamma) = \min\left\{\hat{F}\left(Q_U,\sigma_m^2\right), \hat{E}_r\left(Q_U, A_{Y\,|\,X}, \Delta, \sigma_m^2, \gamma, R_1\right)\right\}.$$

We will show that $E(\gamma)$ is asymptotically achievable for all $\gamma \in [\max(1, \frac{\sigma_m^2}{\Delta}), e^{2(R_Q - R_W - \eta)})$.

Fix ϵ small enough such that $2K+1 \triangleq \sigma_m^2/\epsilon$ is an integer. We construct a sequence of Gaussian ϵ-typical sets $\mathcal{T}_i \triangleq \mathcal{T}^{(n)}_{[\sigma^2(i)]_\epsilon}$ with $\sigma^2(i) = 2i\epsilon, i = 1, 2, \ldots$; i.e.,

$$\mathcal{T}_i \triangleq \left\{\boldsymbol{u} : \left|\frac{1}{n}\boldsymbol{u}^T\boldsymbol{u} - 2i\epsilon\right| \leq \epsilon\right\}$$

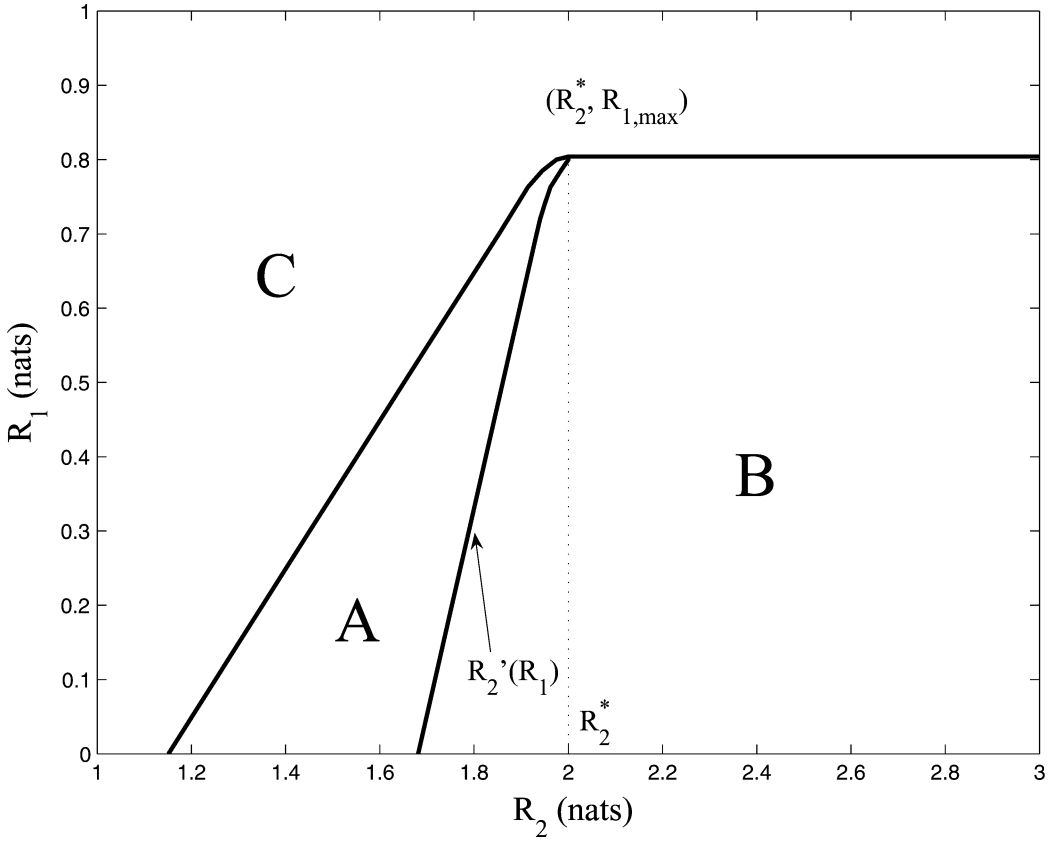

Fig. 5. The quantization–watermarking rate region of Example 2: $E_{\mathrm{QW},r}(R_1,R_2)>0$ in $\mathbf{A}$ and $\mathbf{B}$; $E_{\mathrm{QW},r}(R_1,R_2)=0$ in $\mathbf{C}$ (including its boundary).

$$= \left\{ \boldsymbol{u} : (2i-1)\epsilon \le \frac{1}{n}\boldsymbol{u}^T\boldsymbol{u} \le (2i+1)\epsilon \right\}, \quad i=1,2,3,\ldots. \tag{39}$$

Note that $\sigma^2(i) > \sigma_U^2$ for all $i > K$.

Also, we define $\mathcal{T}_0 \triangleq \{\boldsymbol{u} : \frac{1}{n}\boldsymbol{u}^T\boldsymbol{u} \le \epsilon\}$. Thus, $\{\mathcal{T}_0, \mathcal{T}_1, \mathcal{T}_2, \ldots\}$ is a partition of the whole space $\mathbb{R}^n$. We next define the channel $P_{X|U}$ by

$$X = \alpha^* U + V$$

where $V \sim \mathcal{N}(0, f(\Delta, \sigma_m^2, \gamma))$ and

$$\alpha^* = \alpha^*\left(\Delta, \sigma_m^2, \gamma\right) = \frac{\sigma_m^2 + \gamma f\left(\Delta, \sigma_m^2, \gamma\right) - \Delta}{2\sigma_m^2}. \tag{40}$$

Lemma 4: For $\boldsymbol{u} \in \mathcal{T}^{(n)}_{[\sigma^2]_\epsilon}$ and $\boldsymbol{x} \in \mathcal{T}^{(n)}_{[\alpha^* \mid \sigma^2]_\epsilon}(\boldsymbol{u})$, we have $\boldsymbol{x} \in \mathcal{T}^{(n)}_{[\sigma_X^2]_{\epsilon'}}$, where $\sigma_X^2 = \frac{\sigma^2}{\sigma_m^2}(\gamma-1)f(\Delta,\sigma_m^2,\gamma) + f(\Delta,\sigma_m^2,\gamma)$ and $\epsilon' = (\alpha^*+1)^2\epsilon$.

Lemma 5: For any $\eta > 0, \boldsymbol{u} \in \mathcal{T}^{(n)}_{[\sigma^2]_\epsilon}$, and $\boldsymbol{x} \in \mathcal{T}^{(n)}_{[\alpha^* \mid \sigma^2]_\epsilon}(\boldsymbol{u})$, we have

$$\mathrm{Vol}\left\{\mathcal{T}^{(n)}_{[\alpha^* \mid \sigma^2]_\epsilon}(\boldsymbol{u})\right\}^{-1} \le e^{n\eta} P_V^{(n)}(\boldsymbol{x} - \alpha^*\boldsymbol{u})$$

for ϵ sufficiently small and n sufficiently large.

The proofs of Lemmas 4 and 5 are given in Appendix B.

Random Code Generation: Let $P_U^{(i)} \sim \mathcal{N}(0, \sigma^2(i))$ for $i = 1, 2, \ldots, K$. For each $P_U^{(i)}$ we calculate

$$P_X^{(i)}(x) = \int_{\mathcal{U}} P_U^{(i)}(u) P_{X|U}(x \mid u) du \sim \mathcal{N}\left(0, \sigma_X^2(i)\right)$$

where

$$\sigma_X^2(i) = \frac{\sigma^2(i)}{\sigma_m^2}(\gamma-1) f\left(\Delta, \sigma_m^2, \gamma\right) + f\left(\Delta, \sigma_m^2, \gamma\right) \le \gamma f\left(\Delta, \sigma_m^2, \gamma\right) \tag{41}$$

since $\sigma^2(i) \le \sigma_m^2$ for $i \le K$. For each $\mathcal{T}_i, i = 1, 2, \ldots, K$, generate a codebook consisting of $W = e^{nR_W}$ "subcodebooks" $C(\mathcal{T}_i) = \{C_1(\mathcal{T}_i), C_2(\mathcal{T}_i), \ldots, C_W(\mathcal{T}_i)\}$, where each subcodebook $C_w(\mathcal{T}_i)$ consists of $M = \lfloor e^{n\hat{R}} \rfloor (\hat{R} = R_Q - R_W - \frac{1}{n}\log(K+1))$ codewords for each $w \in \mathcal{W}_n$; i.e.,

$$C_w(\mathcal{T}_i) = \{\boldsymbol{x}(w,1,\mathcal{T}_i), \boldsymbol{x}(w,2,\mathcal{T}_i), \ldots, \boldsymbol{x}(w,M,\mathcal{T}_i)\}$$

such that each codeword $\boldsymbol{x}(w,t,\mathcal{T}_i)(t = 1, 2, \ldots, M)$ is independently and uniformly drawn from the typical set $\mathcal{T}^{(n)}_{[\sigma_X^2(i)]_{\epsilon'}}$ with respect to the distribution $P_X^{(i)}(x)$, where $\epsilon' = (\alpha^*+1)^2\epsilon$.

It then follows that for all $i = 1, 2, \ldots, K$

$$I_{P_U^{(i)} P_{X|U}}(U;X) = \frac{1}{2}\log\frac{2\pi\sigma_X^2(i)}{2\pi f\left(\Delta, \sigma_m^2, \gamma\right)} \le \frac{1}{2}\log\gamma \le \hat{R} + \frac{1}{n}\log(K+1) - \eta. \tag{42}$$

For the sets $\mathcal{T}_0$ and $\mathcal{T}_i$ for $i > K$, the codebooks consist of $W = e^{nR_W}$ "subcodebooks"

$$C(\mathcal{T}_i) = \{C_1(\mathcal{T}_i), C_2(\mathcal{T}_i), \ldots, C_W(\mathcal{T}_i)\}$$

such that $C_w(\mathcal{T}_i) = \{\mathbf{0}\}$ for all $w \in \mathcal{W}$. Clearly, $\lim_{n\to\infty} \frac{1}{n}\log|\mathcal{W}_n| \geq R_1$ and $\lim_{n\to\infty} \frac{1}{n}\log|f_n| \leq R_2$.

Watermark Embedding: Given a watermark w and a covertext $\boldsymbol{u} \in \mathcal{T}_i$, the encoder chooses the first codeword $\boldsymbol{x}(w,t,\mathcal{T}_i)$ in the codebook $C_w(\mathcal{T}_i)$ such that $\boldsymbol{x}(w,t,\mathcal{T}_i)$ lies in the conditional ϵ-typical set $\mathcal{T}^{(n)}_{[\alpha^*\,|\,\sigma^2(i)]_\epsilon}(\boldsymbol{u})$ with respect to the test channel $P_{X|U}$. The output of the encoder is denoted by $\boldsymbol{x}(C_w(\mathcal{T}_i,\boldsymbol{u}))$. If none of the codewords is in the set $\mathcal{T}^{(n)}_{[\alpha^*\,|\,\sigma^2(i)]_\epsilon}(\boldsymbol{u})$, then the encoder outputs the first codeword. Note that $\boldsymbol{x}(C_w(\mathcal{T}_i,\boldsymbol{u}))$ is always $\mathbf{0}$ if $\boldsymbol{u} \in \mathcal{T}_i$ for $i = 0, K+1, K+2, \ldots$.

Decoding: The decoder has full knowledge of $\boldsymbol{u}$, and can thus generate all possible watermarked versions of $\boldsymbol{u}, \{\boldsymbol{x}(C_w(\mathcal{T}_i,\boldsymbol{u}))\}_{w=1}^{W}$. Upon receiving $\boldsymbol{y}$, a maximum-likelihood decoder is employed; i.e., the output of the decoder satisfies

$$\hat{w} = \arg\max_{w\in\mathcal{W}_n} A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\mathcal{T}_i,\boldsymbol{u}))).$$

Probability of Error Analysis: Let

$$\Gamma = \{1, 2, \ldots, K\}.$$

It can be shown in a similar manner as in (11) and (22) that the probability of error, given that w is transmitted, averaged over the random code choice, is upper-bounded by

$$\begin{aligned}\bar{P}^{(n)}_{e,w} \leq{}& \sum_{i\notin\Gamma}\int_{\boldsymbol{u}\in\mathcal{T}_i} Q^{(n)}_U(\boldsymbol{u})d\boldsymbol{u} + e^{nR_W}\sum_{i\in\Gamma}\int_{\boldsymbol{u}\in\mathcal{T}_i} Q^{(n)}_U(\boldsymbol{u})\\ &\times \Pr\left(X^n(C_w(\mathcal{T}_i),\boldsymbol{u}) \notin \mathcal{T}^{(n)}_{[\alpha^*\,|\,\sigma^2(i)]_\epsilon}(\boldsymbol{u})\right)d\boldsymbol{u}\\ &+ e^{n\rho R_W}\sum_{i\in\Gamma}\int_{\boldsymbol{u}\in\mathcal{T}_i} Q^{(n)}_U(\boldsymbol{u})\\ &\times\int_{\mathcal{Y}^n}\left(\int_{C_w(\mathcal{T}_i):\boldsymbol{x}(C_w(\mathcal{T}_i,\boldsymbol{u}))\in\mathcal{T}^{(n)}_{[\alpha^*\,|\,\sigma^2(i)]_\epsilon}(\boldsymbol{u})} q(C_w(\mathcal{T}_i))\right.\\ &\left.\times A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w(\mathcal{T}_i,\boldsymbol{u})))^{\frac{1}{1+\rho}}dC_w(P_U)\right)^{1+\rho}d\boldsymbol{y}d\boldsymbol{u}\end{aligned} \tag{43}$$

where

$$q(C_w(\mathcal{T}_i)) = \prod_{t=1}^{M} q(\boldsymbol{x}(w,t,\mathcal{T}_i))$$

and $dC_w(\mathcal{T}_i) = d\boldsymbol{x}(w,1,\mathcal{T}_i)\cdots d\boldsymbol{x}(w,M,\mathcal{T}_i)$. We next bound the three terms in (43). Applying Lemma 3 to $\mathcal{T}_i$, and noting that

$$\zeta_1(\epsilon) = -\frac{\epsilon}{2\sigma_U^2} - \frac{1}{2}\log\left(1+\frac{\epsilon}{\sigma^2(i)}\right)$$

(defined in Lemma 3) is increasing in i, we can upper-bound the first term of (43) as

$$\begin{aligned}P_1 &= \sum_{i\notin\Gamma}\int_{\boldsymbol{u}\in\mathcal{T}_i} Q^{(n)}_U(\boldsymbol{u})d\boldsymbol{u}\\ &= \int_{\boldsymbol{u}\in\mathcal{T}_0} Q^{(n)}_U(\boldsymbol{u})d\boldsymbol{u} + \sum_{i=K+1}^{\infty}\int_{\boldsymbol{u}\in\mathcal{T}_i} Q^{(n)}_U(\boldsymbol{u})d\boldsymbol{u}\\ &\leq Q^{(n)}_U(\boldsymbol{u}^T\boldsymbol{u} \leq n\epsilon)\\ &\quad + \sum_{i=K+1}^{\infty}\exp\left\{-n\left[\frac{1}{2}\left(\frac{\sigma^2(i)}{\sigma_U^2}\right.\right.\right.\\ &\qquad\left.\left.\left. - \log\frac{\sigma^2(i)}{\sigma_U^2} - 1\right) + \zeta(\epsilon)\right]\right\}\end{aligned} \tag{44}$$

where

$$\begin{aligned}\zeta(\epsilon) &= \min_{i\geq K+1}\zeta_1(\epsilon)\\ &= -\frac{\epsilon}{2\sigma_U^2} - \frac{1}{2}\log\left(1+\frac{\epsilon}{\sigma_m^2+\epsilon}\right)\end{aligned}$$

is independent of i. Similar to (23), by applying Lemmas 3 and 4 and (42), we can bound the second term of (43) as

$$\begin{aligned}P_2 &= e^{nR_W}\sum_{i\in\Gamma}\int_{\boldsymbol{u}\in\mathcal{T}_i} Q^{(n)}_U(\boldsymbol{u})\\ &\quad\times\Pr\left(X^n(C_w(\mathcal{T}_i,\boldsymbol{u})) \notin \mathcal{T}^{(n)}_{[\alpha^*\,|\,\sigma^2(i)]_\epsilon}(\boldsymbol{u})\right)d\boldsymbol{u}\\ &\leq \exp\left(-\exp\left(\frac{n\eta}{4}\right) + nR_W\right)\end{aligned}$$

which vanishes double-exponentially. Just as in (28), by applying Lemmas 4 and 5, we can bound the third term of (43) by

$$\begin{aligned}P_3 &= e^{n\rho R_W}\sum_{i\in\Gamma}\int_{\boldsymbol{u}\in\mathcal{T}_i} Q^{(n)}_U(\boldsymbol{u})\\ &\quad\times\int_{\mathcal{Y}^n}\left(\int_{C_w(P_U)\in\mathcal{A}(\boldsymbol{u})} q(C_w(P_U))\cdot\right.\\ &\quad\left.\times A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x}(C_w,\boldsymbol{u}))^{\frac{1}{1+\rho}}dC_w(P_U)\right)^{1+\rho}d\boldsymbol{y}d\boldsymbol{u}\\ &\leq \min_{0\leq\rho\leq 1}\left[4e^{n(\rho R_1+\eta)}\int_{\mathcal{U}^n} Q^{(n)}_U(\boldsymbol{u})\right.\\ &\quad\times\int_{\mathcal{Y}^n}\left(\int_{\mathcal{X}^n} P^{(n)}_V(\boldsymbol{x}-\alpha^*\boldsymbol{u})\right.\\ &\quad\left.\left.\times A^{(n)}_{Y\,|\,X}(\boldsymbol{y}\,|\,\boldsymbol{x})^{\frac{1}{1+\rho}}d\boldsymbol{x}\right)^{1+\rho}d\boldsymbol{y}d\boldsymbol{u}\right]\end{aligned} \tag{45}$$

for ϵ sufficiently small and n sufficiently large. By the large deviation property for the i.i.d. Gaussian sequences ([7]) we have

$$\lim_{n\to\infty} -\frac{1}{n}\log Q^{(n)}_U(\boldsymbol{u}^T\boldsymbol{u} \leq n\epsilon) = \frac{1}{2}\left(\frac{\epsilon}{\sigma_U^2} - \log\frac{\epsilon}{\sigma_U^2} - 1\right) \tag{46}$$

which can be arbitrarily large by choosing ϵ sufficiently small. On the other hand, we recall the following fact [1]: if A, B, and C are positive reals, and D is a real constant, then

$$\begin{aligned}\lim_{n\to\infty}\frac{1}{n}\log\left\{\sum_{i=1}^{\infty}\exp\left[n(\log(Ai+B) - Ci + D) + o(n)\right]\right\}&\\ = \max_{i\geq 1}[\log(Ai+B) - Ci + D].&\end{aligned} \tag{47}$$

Applying this to the second term of (44), we obtain

$$\begin{aligned}
&\lim_{n\to\infty} -\frac{1}{n}\log \sum_{i=K+1}^{+\infty} \exp\left\{-n\left[\frac{1}{2}\left(\frac{\sigma^2(i)}{\sigma_U^2} - \log\frac{\sigma^2(i)}{\sigma_U^2} - 1\right) + \zeta(\epsilon)\right]\right\} \\
&= \min_{i\geq K+1} \frac{1}{2}\left(\frac{\sigma^2(i)}{\sigma_U^2} - \log\frac{\sigma^2(i)}{\sigma_U^2} - 1\right) \\
&\quad - \frac{\epsilon}{2\sigma_U^2} - \frac{1}{2}\log\left(1+\frac{\epsilon}{\sigma_m^2+\epsilon}\right) \\
&= \frac{1}{2}\left(\frac{\sigma_m^2+\epsilon}{\sigma_U^2} - \log\frac{\sigma_m^2+\epsilon}{\sigma_U^2} - 1\right) \\
&\quad - \frac{\epsilon}{2\sigma_U^2} - \frac{1}{2}\log\left(1+\frac{\epsilon}{\sigma_m^2+\epsilon}\right) \qquad (48) \\
&= \frac{1}{2}\left(\frac{\sigma_m^2}{\sigma_U^2} - \log\frac{\sigma_m^2}{\sigma_U^2} - 1\right) - \frac{1}{2}\log\frac{\sigma_m^2+2\epsilon}{\sigma_m^2} \\
&\geq E(\gamma) - \frac{1}{2}\log\frac{\sigma_m^2+2\epsilon}{\sigma_m^2} \qquad (49)
\end{aligned}$$

where (48) follows from the fact that $\hat{F}(Q_U,\sigma^2)$ is an increasing function of σ^2 for $\sigma^2 \geq \sigma_U^2$ and the minimum is achieved at $i = K+1$. Now taking (46), (49), (45), and (43) into account and letting first $n\to\infty$, then $\epsilon\to 0$ and $\eta\to 0$, it is readily shown that

$$\liminf_{n\to\infty} -\frac{1}{n}\log \bar{P}_e^{(n)} \geq E(\gamma) \qquad (50)$$

or equivalently

$$\bar{P}_e^{(n)} \leq e^{-nE(\gamma)+o(n)}$$

for n sufficiently large. By minimizing the upper bound in γ over $[\max(1,\frac{\sigma_m^2}{\Delta}), e^{2(R_Q-R_W-\eta)})$ we obtain

$$\bar{P}_e^{(n)} \leq e^{-n\hat{E}_{\mathrm{QW},r}(R_1,R_2)+o(n)}.$$

Distortion Analysis: Define

$$\mathcal{E}(C_w(\mathcal{T}_i),i) \triangleq \left\{\boldsymbol{u}\in\mathcal{T}_i : \boldsymbol{x}(C_w(\mathcal{T}_i,\boldsymbol{u})) \notin \mathcal{T}^{(n)}_{[\alpha^*\,|\,\sigma^2(i)]_\epsilon}(\boldsymbol{u})\right\}. \qquad (51)$$

Lemma 6: For $i\in\{1,\ldots,K\}, \boldsymbol{u}\in\mathcal{T}_i$ and $\boldsymbol{x}\in\mathcal{T}^{(n)}_{[\alpha^*\,|\,\sigma^2(i)]_\epsilon}(\boldsymbol{u})$, the distortion is upper-bounded by $d(\boldsymbol{u},\boldsymbol{x})\leq \Delta+\frac{\delta}{4}$ for n sufficiently large.

The proof of this lemma is deferred to Appendix B. Due to Lemma 6, the distortion for a fixed code C is hence bounded by

$$\begin{aligned}
D^{(n)} &= \sum_{w=1}^{W}\frac{1}{W}\sum_{i=0}^{+\infty}\int_{\boldsymbol{u}\in\mathcal{T}_i} Q_U^{(n)}(\boldsymbol{u}) d(\boldsymbol{u},\boldsymbol{x}(C_w(\mathcal{T}_i,\boldsymbol{u})))d\boldsymbol{u} \\
&= \sum_{w=1}^{W}\frac{1}{W}\sum_{i=1}^{K}\int_{\boldsymbol{u}\in\mathcal{T}_i} Q_U^{(n)}(\boldsymbol{u}) d(\boldsymbol{u},\boldsymbol{x}(C_w(\mathcal{T}_i,\boldsymbol{u})))d\boldsymbol{u} \\
&\quad + \sum_{w=1}^{W}\frac{1}{W}\sum_{i\notin\Gamma}\int_{\boldsymbol{u}\in\mathcal{T}_i} Q_U^{(n)}(\boldsymbol{u})\frac{1}{n}\boldsymbol{u}^T\boldsymbol{u}\,d\boldsymbol{u} \\
&= \sum_{w=1}^{W}\frac{1}{W}\sum_{i=1}^{K}\int_{\boldsymbol{u}\in\mathcal{T}_i\setminus\mathcal{E}(C_w(\mathcal{T}_i),i)} \\
&\qquad \times Q_U^{(n)}(\boldsymbol{u})\underbrace{d(\boldsymbol{u},\boldsymbol{x}(C_w(\mathcal{T}_i,\boldsymbol{u})))}_{\leq\Delta+\delta/4} d\boldsymbol{u} \qquad (52) \\
&\quad + \sum_{w=1}^{W}\frac{1}{W}\sum_{i=1}^{K}\int_{\boldsymbol{u}\in\mathcal{E}(C_w(\mathcal{T}_i),i)} \\
&\qquad \times Q_U^{(n)}(\boldsymbol{u}) d(\boldsymbol{u},\boldsymbol{x}(C_w(\mathcal{T}_i,\boldsymbol{u})))d\boldsymbol{u} \\
&\quad + \sum_{w=1}^{W}\frac{1}{W}\int_{\boldsymbol{u}\in\mathcal{T}_0} Q_U^{(n)}(\boldsymbol{u})\underbrace{\frac{1}{n}\boldsymbol{u}^T\boldsymbol{u}}_{\leq\epsilon} d\boldsymbol{u} \\
&\quad + \sum_{w=1}^{W}\frac{1}{W}\sum_{i=K+1}^{+\infty}\int_{\boldsymbol{u}\in\mathcal{T}_i} Q_U^{(n)}(\boldsymbol{u})\frac{1}{n}\boldsymbol{u}^T\boldsymbol{u}\,d\boldsymbol{u} \qquad (53) \\
&\leq \Delta + \frac{\delta}{4} + \sum_{w=1}^{W}\frac{1}{W}\sum_{i=1}^{K}\int_{\boldsymbol{u}\in\mathcal{T}_i} Q_U^{(n)}(\boldsymbol{u}) d(\boldsymbol{u},\boldsymbol{x}(C_w(\mathcal{T}_i,\boldsymbol{u}))) \\
&\quad \times \mathbb{I}\left\{\boldsymbol{x}(C_w(\mathcal{T}_i,\boldsymbol{u})) \notin \mathcal{T}^{(n)}_{[\alpha^*\,|\,\sigma^2(i)]_\epsilon}(\boldsymbol{u})\right\} d\boldsymbol{u} \\
&\quad + \epsilon + \sum_{w=1}^{W}\frac{1}{W}\sum_{i=K+1}^{+\infty}\int_{\boldsymbol{u}\in\mathcal{T}_i} Q_U^{(n)}(\boldsymbol{u})\frac{1}{n}\boldsymbol{u}^T\boldsymbol{u}\,d\boldsymbol{u} \qquad (54)
\end{aligned}$$

where in (52) we used Lemma 6, in (53) we used the fact that $\Gamma=\{1,\ldots,K\}$ and the definition of the set $\mathcal{T}_i$, and in (54) we used the definition of $\mathcal{E}(C_w(\mathcal{T}_i),i)$. For $\boldsymbol{u}\in\mathcal{T}_i$ such that $i\leq K$

$$\frac{1}{n}\boldsymbol{u}^T\boldsymbol{u} \leq (2i+1)\epsilon \leq \sigma_m^2$$

and since all codewords $\boldsymbol{x}(w,t)$ for each $\mathcal{T}_i, i\leq K$, are drawn from the set $\mathcal{T}^{(n)}_{[\sigma_X^2(i)]_{\epsilon'}}$ with respect to the distribution $P_X^{(i)}(x)$, where $\epsilon' = (\alpha^*+1)^2\epsilon$, we have (see (41))

$$\begin{aligned}
\frac{1}{n}\boldsymbol{x}(C_w(\boldsymbol{u}))^T\boldsymbol{x}(C_w(\boldsymbol{u})) &\leq \sigma_X^2(i)+\epsilon' \\
&\leq \gamma f\left(\Delta,\sigma_m^2,\gamma\right) + (\alpha^*+1)^2\epsilon. \qquad (55)
\end{aligned}$$

Thus, for $\boldsymbol{u}\in\mathcal{T}_i$ such that $i\leq K$

$$\begin{aligned}
d(\boldsymbol{u},\boldsymbol{x}(C_w(\boldsymbol{u}))) &\leq \frac{1}{n}\left[2\boldsymbol{u}^T\boldsymbol{u} + 2\boldsymbol{x}(C_w(\mathcal{T}_i,\boldsymbol{u}))^T\boldsymbol{x}(C_w(\boldsymbol{u}))\right] \\
&\leq 2\sigma_m^2 + 2\gamma f\left(\Delta,\sigma_m^2,\gamma\right) + 2(\alpha^*+1)^2\epsilon \qquad (56)
\end{aligned}$$

independently of n. On the other hand, noting that

$$\sigma^2(K+1) = 2(K+1)\epsilon = \sigma_m^2+\epsilon > \sigma_U^2$$

we have for any $\epsilon'>0$

$$\begin{aligned}
&\sum_{i=K+1}^{+\infty}\int_{\boldsymbol{u}\in\mathcal{T}_i} Q_U^{(n)}(\boldsymbol{u})\frac{1}{n}\boldsymbol{u}^T\boldsymbol{u}\,d\boldsymbol{u} \\
&= \int_{\boldsymbol{u}^T\boldsymbol{u}\geq n(\sigma_m^2+\epsilon)} Q_U^{(n)}(\boldsymbol{u})\frac{1}{n}\boldsymbol{u}^T\boldsymbol{u}\,d\boldsymbol{u} \\
&\leq \sigma_U^2 - \int_{n(\sigma_U^2-\epsilon')\leq\boldsymbol{u}^T\boldsymbol{u}\leq n(\sigma_m^2+\epsilon)} Q_U^{(n)}(\boldsymbol{u})\frac{1}{n}\boldsymbol{u}^T\boldsymbol{u}\,d\boldsymbol{u}
\end{aligned}$$

$$\leq \sigma_U^2 - (\sigma_U^2 - \epsilon') \int_{n(\sigma_U^2-\epsilon') \leq \boldsymbol{u}^T\boldsymbol{u} \leq n(\sigma_m^2+\epsilon)} Q_U^{(n)}(\boldsymbol{u}) d\boldsymbol{u}$$
$$= \epsilon' + (\sigma_U^2 - \epsilon') \left[\Pr\left(\frac{1}{n}\sum_{i=1}^n U_i^2 < \sigma_U^2 - \epsilon' \right) + \Pr\left(\frac{1}{n}\sum_{i=1}^n U_i^2 > \left(\sigma_m^2 + \epsilon\right) \right) \right]. \quad (57)$$

By the weak law of large numbers, the probabilities in (57) converge to zero, and we can make the above bound arbitrarily small by choosing ϵ' small enough and n large enough. Thus, taking the expectation of $D^{(n)}$ over the random choice of the codes $\mathcal{C}$, and using (45), we obtain

$$\bar{D}^{(n)} \leq \Delta + \frac{\delta}{4} + \left(2\sigma_m^2 + 2\gamma f\left(\Delta, \sigma_m^2, \gamma\right) + 2(\alpha^* + 1)^2 \epsilon\right) \exp\left\{ -\exp\left(\frac{n\eta}{4}\right)\right\} + \epsilon + \frac{\delta}{4} \leq \Delta + \delta$$

for ϵ sufficiently small and n sufficiently large.

The Existence of Good Codes: It can be shown in a similar manner as in the last step of proof of Theorem 1 (see Section III-F) that there exists at least a sequence of codes $\{C = (f_n, \varphi_n)\}$ that achieves the exponent $\hat{E}_{\mathrm{QW},r}(R_1, R_2)$ satisfies the distortion constraint simultaneously. □

VI. Concluding Remarks

In this paper, we developed lower bounds for the discrete and Gaussian JQW error exponents. In both cases, we showed that our lower bounds are positive in the interior of the achievable quantization and watermarking rate region derived in [8] and [9]. We have not been able to find matching upper bounds or to disprove the tightness of our bounds.

Numerical examples reveal an interesting property of the derived bounds. In both the discrete and the Gaussian case, for a fixed embedding rate, there exists a certain threshold quantization rate, which is strictly less than the maximum possible rate (the log-cardinality of the stegotext's alphabet in the discrete case and infinity in the Gaussian case), such that the error exponent is constant for all quantization rates larger than this threshold (see Examples 1 and 2). If our bounds were tight, this would indicate that in designing a JQW system for a given embedding rate, only quantization rates below this threshold should be considered since allocating more rate for quantization would not improve the system's error probability performance. This property is analogous to the observation made in [9] that for the Gaussian JQW problem there exists a quantization rate threshold above which quantization does not hinder the detection of the watermark; i.e., the watermarking capacity can be as high as in the case of no compression.

Appendix A
Proof of Proposition 1

For $P_U \in \mathcal{P}(\mathcal{U})$ and $P_{X|U} \in \mathcal{P}(\mathcal{X}\,|\,\mathcal{U})$, introduce the notation

$$I(P_U, P_{X|U}) \triangleq I_{P_U P_{X|U}}(U; X),$$
$$d(P_U, P_{X|U}) \triangleq \mathbb{E}_{P_U P_{X|U}} d(U, X).$$

Define

$$A(R) \triangleq \{P_U : I(P_U, P_{X|U}) \geq R\},$$
$$B(\Delta) \triangleq \{P_U : d(P_U, P_{X|U}) \geq \Delta\}.$$

Then whenever $A(R) \cup B(\Delta) \neq \emptyset$, we have

$$F(Q_U, P_{X|U}, \Delta, R) = \min_{P_U \in A(R) \cup B(\Delta)} D(P_U \| Q_U) \quad (58)$$

since $A(R)$ and $B(\Delta)$ are closed subsets of $\mathcal{P}(\mathcal{U})$.

If $R \leq C(P_{X\,|\,Y})$, then $A(R) \neq \emptyset$, so (58) gives

$$F(Q_U, P_{X|U}, \Delta, R) = \min_{P_U \in A(R) \cup B(\Delta)} D(P_U \| Q_U) = \min\left(\min_{P_U \in A(R)} D(P_U \| Q_U), \min_{P_U \in B(\Delta)} D(P_U \| Q_U) \right).$$

Since $\min_{P_U \in B(\Delta)} D(P_U \| Q_U)$ is a constant independent of R, to prove the continuity of $F(Q_U, P_{X|U}, \Delta, R)$, it is enough to show that

$$G(R) \triangleq \min_{P_U \in A(R)} D(P_U \| Q_U)$$

is continuous in $[0, C(P_{X|U})]$.

Let $0 \leq R_1 < R_2 \leq C(P_{X\,|\,Y})$ and let $P_U^1 \in A(R_1)$ and $P_U^2 \in A(R_2)$ be such that

$$G(R_1) = D\left(P_U^1 \| Q_U\right), \quad G(R_2) = D\left(P_U^2 \| Q_U\right).$$

Letting $P_U^* = \alpha P_U^1 + (1-\alpha) P_U^2$ for some $0 < \alpha < 1$, we have

$$\alpha G(R_1) + (1-\alpha) G(R_2) = \alpha D\left(P_U^1 \| Q_U\right) + (1-\alpha) D\left(P_U^2 \| Q_U\right) \geq D(P_U^* \| Q_U)$$

since $D(P\|Q)$ is convex in P. On the other hand, since $I(P, P_{X|U})$ is concave in P, we have

$$I(P_U^*, P_{X|U}) \geq \alpha I\left(P_U^1, P_{X|U}\right) + (1-\alpha) I\left(P_U^2, P_{X|U}\right) \geq \alpha R_1 + (1-\alpha) R_2$$

since $P_U^i \in A(R_i)$ implies $I(P_U^i, P_{X|U}) \geq R_i$ for $i = 1, 2$. Since the last inequality means that $P_U^* \in A(\alpha R_1 + (1-\alpha) R_2)$, we obtain

$$G(\alpha R_1 + (1-\alpha) R_2) \leq D(P^* \| Q_U) \leq \alpha G(R_1) + (1-\alpha) G(R_2)$$

so that $G(R)$ is convex in $[0, C(P_{X|U})]$.

The convexity of $G(R)$ implies that it is continuous in $(0, C(P_{X|U}))$. Since $G(R)$ is nondecreasing and convex, it must also be continuous at zero. Thus, $G(R)$ is continuous in $[0, C(P_{X|U}))$.

To complete the proof, we need to show that $G(R)$ is left-continuous at $R = C(P_{X|U})$. Let R_n be an increasing sequence such that $R_n \to R$ as $n \to \infty$. For each n, let $P_U^n \in \mathcal{P}(\mathcal{U})$ be a distribution achieving $G(R_n)$; i.e.,

$$I\left(P_U^n, P_{X|U}\right) \geq R_n, \quad G(R_n) = D\left(P_U^n \| Q_U\right).$$

Since $\mathcal{P}(\mathcal{U})$ is compact we can pick a subsequence $P_U^{n_k}$ such that $P_U^{n_k} \to \hat{P}_U$ (say in total variation) for some $\hat{P}_U \in \mathcal{P}(\mathcal{U})$. Since $\mathcal{U}$ and $\mathcal{X}$ are finite sets, both $D(P_U \| Q_U)$ and $I(P_U, P_{X|U})$ are continuous in P_U. Thus

$$I(\hat{P}_U, P_{X|U}) = \lim_{k \to \infty} I\left(P_U^{n_k}, P_{X|U}\right) \geq \lim_{k \to \infty} R_{n_k} = R$$

so that $\hat{P}_U \in A(R)$, implying in turn that

$$G(R) \le D(\hat{P}_U \| Q_U) = \lim_{k\to\infty} D\left(P_U^{n_k} \| Q_U\right) = \lim_{k\to\infty} G(R_{n_k}).$$

Since G is nondecreasing and R_{n_k} is an increasing sequence, the last inequality implies that G is left-continuous at R. □

APPENDIX B
PROOF OF LEMMAS

Proof of Lemma 3:

Proof of Part a): Consider an auxiliary MGS $P_U \sim \mathcal{N}(0, \sigma^2+\epsilon)$. Then part a) follows from

$$\begin{aligned} 1 &\ge \int_{\{\boldsymbol{u}:|\boldsymbol{u}^T\boldsymbol{u}-n\sigma^2|\le n\epsilon\}} \frac{1}{\left[\sqrt{2\pi(\sigma^2+\epsilon)}\right]^n} e^{-\frac{\boldsymbol{u}^T\boldsymbol{u}}{2(\sigma^2+\epsilon)}} d\boldsymbol{u} \\ &\ge \int_{\{\boldsymbol{u}:|\boldsymbol{u}^T\boldsymbol{u}-n\sigma^2|\le n\epsilon\}} \frac{1}{\left[\sqrt{2\pi(\sigma^2+\epsilon)}\right]^n} e^{-\frac{n((\sigma^2+\epsilon))}{2(\sigma^2+\epsilon)}} d\boldsymbol{u} \\ &= \frac{1}{[2\pi e(\sigma^2+\epsilon)]^{n/2}} \mathrm{Vol}\left\{\mathcal{T}_{[\sigma^2]_\epsilon}\right\}. \end{aligned}$$

Proof of Part b): Part b) follows from

$$\begin{aligned} Q_U^{(n)}\left(\mathcal{T}_{[\sigma^2]_\epsilon}\right) &= \int_{\{\boldsymbol{u}:|\boldsymbol{u}^T\boldsymbol{u}-n\sigma^2|\le n\epsilon\}} \frac{1}{\left[\sqrt{2\pi\sigma_U^2}\right]^n} e^{-\frac{\boldsymbol{u}^T\boldsymbol{u}}{2\sigma_U^2}} d\boldsymbol{u} \\ &\le \int_{\{\boldsymbol{u}:|\boldsymbol{u}^T\boldsymbol{u}-n\sigma^2|\le n\epsilon\}} \frac{1}{\left[\sqrt{2\pi\sigma_U^2}\right]^n} e^{-\frac{n(\sigma^2-\epsilon)}{2\sigma_U^2}} d\boldsymbol{u} \\ &\le e^{-\frac{n(\sigma^2-\epsilon)}{2\sigma_U^2}} \left[\frac{e(\sigma^2+\epsilon)}{\sigma_U^2}\right]^{n/2} \end{aligned}$$

where the last inequality follows from part a).

Proof of Part c): First note that the volume of the conditional ϵ-typical set $\mathcal{T}^{(n)}_{[\alpha\,|\,\sigma^2]_\epsilon}(\boldsymbol{u})$ is independent of $\boldsymbol{u}$; i.e.,

$$\begin{aligned} &\mathrm{Vol}\left\{\mathcal{T}^{(n)}_{[\alpha\,|\,\sigma^2]_\epsilon}(\boldsymbol{u})\right\} \\ &= \mathrm{Vol}\left\{\boldsymbol{v}\in\mathbb{R}^n : \left|\frac{1}{n}\boldsymbol{v}^T\boldsymbol{v} - f(\Delta,\sigma^2,\gamma)\right| \le \epsilon, \quad \left|\frac{1}{n}\boldsymbol{v}^T\boldsymbol{u}\right| \le \epsilon\right\}. \end{aligned}$$

Consider an auxiliary MGS $P_V \sim \mathcal{N}(0, f(\Delta,\sigma^2,\gamma))$. It follows that

$$\begin{aligned} &P_V^{(n)}\left(\mathcal{T}^{(n)}_{[\alpha\,|\,\sigma^2]_\epsilon}(\boldsymbol{u})\right) \\ &= \int_{\mathcal{T}^{(n)}_{[\alpha\,|\,\sigma^2]_\epsilon}(\boldsymbol{u})} \frac{1}{\left[\sqrt{2\pi f(\Delta,\sigma^2,\gamma)}\right]^n} e^{-\frac{\boldsymbol{v}^T\boldsymbol{v}}{2f(\Delta,\sigma^2,\gamma)}} d\boldsymbol{v} \\ &\le \int_{\mathcal{T}^{(n)}_{[\alpha\,|\,\sigma^2]_\epsilon}(\boldsymbol{u})} \frac{1}{\left[\sqrt{2\pi f(\Delta,\sigma^2,\gamma)}\right]^n} e^{-\frac{n(1-\epsilon/f(\Delta,\sigma^2,\gamma))}{2}} d\boldsymbol{v} \\ &= \frac{1}{\left[2\pi e^{(1-\epsilon/f(\Delta,\sigma^2,\gamma))} f(\Delta,\sigma^2,\gamma)\right]^{n/2}} \mathrm{Vol}\left\{\mathcal{T}^{(n)}_{[\alpha\,|\,\sigma^2]_\epsilon}(\boldsymbol{u})\right\}. \end{aligned} \tag{59}$$

On the other hand, we can bound the probability by using the union bound and Chebyshev's inequality

$$\begin{aligned} &1 - P_V^{(n)}\left(\mathcal{T}^{(n)}_{[\alpha\,|\,\sigma^2]_\epsilon}(\boldsymbol{u})\right) \\ &\le P_V^{(n)}\left(\left|\frac{1}{n}\boldsymbol{v}^T\boldsymbol{v} - f(\Delta,\sigma^2,\gamma)\right| > \epsilon\right) \\ &\quad + P_V^{(n)}\left(\left|\frac{1}{n}\boldsymbol{v}^T\boldsymbol{u} - 0\right| > \epsilon\right) \\ &\le \frac{2f(\Delta,\sigma^2,\gamma)^2}{n\epsilon^2} + \frac{f(\Delta,\sigma^2,\gamma)\sigma_U^2}{n\epsilon^2}. \end{aligned} \tag{60}$$

Thus part c) follows by combining (59) and (60). □

Proof of Lemma 4: By definition, for $\boldsymbol{u} \in \mathcal{T}^{(n)}_{[\sigma^2]_\epsilon}$ and $\boldsymbol{x} \in \mathcal{T}^{(n)}_{[\alpha^*\,|\,\sigma^2]_\epsilon}(\boldsymbol{u})$, we have

$$\begin{aligned} &\frac{1}{n}\left[\alpha^*\boldsymbol{u}+\boldsymbol{v}\right]^T\left[\alpha^*\boldsymbol{u}+\boldsymbol{v}\right] \\ &\quad \le (\alpha^*)^2(\sigma^2+\epsilon) + 2\alpha^*\epsilon + f\left(\Delta,\sigma_m^2,\gamma\right) + \epsilon \\ &\quad = (\alpha^*)^2\sigma^2 + f\left(\Delta,\sigma_m^2,\gamma\right) + (\alpha^*+1)^2\epsilon \\ &\quad = \frac{\sigma^2}{\sigma_m^2}(\gamma-1)f\left(\Delta,\sigma_m^2,\gamma\right) + f\left(\Delta,\sigma_m^2,\gamma\right) + (\alpha^*+1)^2\epsilon \end{aligned} \tag{61}$$

where the last equality follows from (40) and the identity (35). Similarly, we can show that

$$\begin{aligned} &\frac{1}{n}\left[\alpha^*\boldsymbol{u}+\boldsymbol{v}\right]^T\left[\alpha^*\boldsymbol{u}+\boldsymbol{v}\right] \\ &\quad \ge \frac{\sigma^2}{\sigma_m^2}(\gamma-1)f\left(\Delta,\sigma_m^2,\gamma\right) + f\left(\Delta,\sigma_m^2,\gamma\right) - (\alpha^*+1)^2\epsilon. \end{aligned} \tag{62}$$

Now (61) together with (62) implies that $\boldsymbol{x} \in \mathcal{T}^{(n)}_{[\sigma_X^2]_{\epsilon'}}$. □

Proof of Lemma 5: It follows from Lemma 3 c) that

$$\begin{aligned} \mathrm{Vol}\left\{\mathcal{T}^{(n)}_{[\alpha^*\,|\,\sigma^2]_\epsilon}(\boldsymbol{u})\right\} &\ge \left[1 - \frac{f(\Delta,\sigma^2,\gamma)+\sqrt{f(\Delta,\sigma^2,\gamma)\sigma_U^2}}{n\epsilon^2}\right] \\ &\quad \times \left[2\pi e^{(1-\epsilon/f(\Delta,\sigma^2,\gamma))} f(\Delta,\sigma^2,\gamma)\right]^{n/2} \\ &\ge \left[1 - \frac{f(\Delta,\sigma^2,\gamma)+\sqrt{f(\Delta,\sigma^2,\gamma)\sigma_U^2}}{n\epsilon^2}\right] \\ &\quad \times \left[2\pi f(\Delta,\sigma^2,\gamma)\right]^{n/2} \end{aligned}$$

for ϵ small enough. Clearly, for any $\eta > 0, \boldsymbol{u} \in \mathcal{T}^{(n)}_{[\sigma^2]_\epsilon}$ and $\boldsymbol{x} \in \mathcal{T}^{(n)}_{[\alpha^*\,|\,\sigma^2]_\epsilon}(\boldsymbol{u})$

$$\begin{aligned} &P_V^{(n)}\left(\boldsymbol{x}-\alpha^*\boldsymbol{u}\right) \\ &\quad = \left[2\pi f(\Delta,\sigma^2,\gamma)\right]^{-n/2} e^{-\frac{(\boldsymbol{x}-\alpha^*\boldsymbol{u})^T(\boldsymbol{x}-\alpha^*\boldsymbol{u})}{2nf(\Delta,\sigma^2,\gamma)}} \\ &\quad \ge \left[2\pi f(\Delta,\sigma^2,\gamma)\right]^{-n/2} e^{-\frac{f(\Delta,\sigma^2,\gamma)+\epsilon}{2f(\Delta,\sigma^2,\gamma)}} \\ &\quad \ge e^{-\frac{f(\Delta,\sigma^2,\gamma)+\epsilon}{2f(\Delta,\sigma^2,\gamma)}} \left[1 - \frac{f(\Delta,\sigma^2,\gamma)+\sqrt{f(\Delta,\sigma^2,\gamma)\sigma_U^2}}{n\epsilon^2}\right]^{-1} \end{aligned}$$

$$\times \mathrm{Vol}\left\{\mathcal{T}^{(n)}_{[\alpha^*\,|\,\sigma^2]_\epsilon}(\boldsymbol{u})\right\}^{-1}$$
$$\geq e^{-n\eta}\mathrm{Vol}\left\{\mathcal{T}^{(n)}_{[\alpha^*\,|\,\sigma^2]_\epsilon}(\boldsymbol{u})\right\}^{-1}$$

for ϵ sufficiently small and n sufficiently large. □

Proof of Lemma 6: For $\boldsymbol{u} \in \mathcal{T}^{(n)}_{[\sigma^2(i)]_\epsilon}$ and $\boldsymbol{x} \in \mathcal{T}^{(n)}_{[\alpha^*\,|\,\sigma^2(i)]_\epsilon}(\boldsymbol{u})$, we have

$$\begin{aligned}
&\frac{1}{n}(\boldsymbol{u}-\boldsymbol{x})^T(\boldsymbol{u}-\boldsymbol{x}) \\
&\quad = (\alpha^*-1)^2\frac{1}{n}\boldsymbol{u}^T\boldsymbol{u} - 2(\alpha^*-1)\frac{1}{n}\boldsymbol{u}^T\boldsymbol{v} + \frac{1}{n}\boldsymbol{v}^T\boldsymbol{v} \\
&\quad \leq (\alpha^*-1)^2(\sigma^2(i)+\epsilon) + 2(\alpha^*-1)\epsilon \\
&\qquad + f\left(\Delta,\sigma_m^2,\gamma\right)+\epsilon \\
&\quad \leq (\alpha^*-1)^2(\sigma_m^2+\epsilon) + 2(\alpha^*-1)\epsilon + f\left(\Delta,\sigma_m^2,\gamma\right)+\epsilon \\
&\quad = (\alpha^*)^2\sigma_m^2 - 2\alpha^*\sigma_m^2 + \sigma_m^2 + f\left(\Delta,\sigma_m^2,\gamma\right) + (\alpha^*)^2\epsilon
\end{aligned} \tag{63}$$

where (63) follows from the fact that $\sigma^2(i) \leq \sigma_m^2$ for $i \leq K$. Substituting

$$\alpha^* = \frac{\sigma_m^2 + \gamma f\left(\Delta,\sigma_m^2,\gamma\right) - \Delta}{2\sigma_m^2}$$

into the above bound and using the identity (35)

$$(\alpha^*)^2 = \frac{(\gamma-1)f\left(\Delta,\sigma_m^2,\gamma\right)}{\sigma_m^2}$$

yields

$$\frac{1}{n}(\boldsymbol{u}-\boldsymbol{x})^T(\boldsymbol{u}-\boldsymbol{x}) \leq \Delta + (\alpha^*)^2\epsilon.$$ □

REFERENCES

[1] E. Arikan and N. Merhav, "Guessing subject to distortion," *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 1041–1056, May 1998.

[2] A. S. Cohen and A. Lapidoth, "The Gaussian watermarking game," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1639–1667, Jun. 2002.

[3] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York: Wiley, 2006.

[4] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York: Academic, 1981.

[5] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1968.

[6] S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*. Norwood, MA: Artech House, 2000.

[7] S. Ihara and M. Kubo, "Error exponent for coding of memoryless Gaussian sources with fidelity criterion," *IEICE Trans. Fundamentals*, vol. E83-A, no. 10, pp. 1891–1897, Oct. 2000.

[8] D. Karakos, "Digital Watermarking, Fingerprinting and Compression: An Information-Theoretic Perspective," Ph.D. dissertation, Univ. Maryland, College Park, MD, 2002.

[9] D. Karakos and A. Papamarcou, "A relationship between quantization and watermarking rates in the presence of additive Gaussian attacks," *IEEE Trans. Inf. Theory*, vol. 49, no. 8, pp. 1970–1982, Aug. 2003.

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

[11] A. Maor and N. Merhav, "On joint information embedding and lossy compression in the presence of a memoryless attack," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3166–3175, Sep. 2005.

[12] K. Marton, "Error exponent for source coding with a fidelity criterion," *IEEE Trans. Inf. Theory*, vol. IT-20, no. 2, pp. 197–199, Mar. 1974.

[13] N. Merhav, "On random coding error exponent of watermarking systems," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 420–430, Mar. 2000.

[14] P. Moulin and J. O'Sullivan, "Information-theoretic analysis of information hiding," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 563–593, Mar. 2003.

[15] P. Moulin and M. K. Mihcak, "The parallel-Gaussian watermarking game," *IEEE Trans. Inf. Theory*, vol. 50, no. 2, pp. 272–289, Feb. 2004.

[16] P. Moulin and W. Ying, "Capacity and random-coding exponents for channel coding with side information," *IEEE Trans. Inf. Theory*, vol. 53, no. 4, pp. 1326–1347, Apr. 2007.

[17] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[18] A. Somekh-Baruch and N. Merhav, "On the error exponent and capacity games of private watermarking systems," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 537–563, Mar. 2003.

[19] A. Somekh-Baruch and N. Merhav, "On the capacity game of public watermarking systems," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 511–524, Mar. 2004.

[20] W. Sun, "Joint Compression and Digital Watermarking: Information-Theoretic Study and Algorithms Development," Ph.D. dissertation, Univ. Waterloo, Waterloo, ON, Canada, 2006.

[21] Y. D. Wang, F. Alajaji, and T. Linder, "A random coding error exponent for joint quantization and watermarking of Gaussian sources under memoryless Gaussian attacks," in *Proc. 2007 Canadian Workshop on Information Theory*, Edmonton, AB, Canada, Jun. 2007, pp. 152–155.

[22] E.-h. Yang and W. Sun, "On watermarking and compression rates of joint compression and private watermarking systems with abstract alphabets," in *Proc. 2005 Canadian Workshop on Information Theory*, Montreal, QC, Canada, Jun. 2005, pp. 296–299.

[23] Y. Zhong, F. Alajaji, and L. L. Campbell, "On the excess distortion exponent for memoryless Gaussian source-channel pairs," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, Jul. 2006, pp. 2139–2143

Yangfan Zhong (S'04) was born in Chengdu, China, on May 19, 1980. He received the B.E. degree in communication and information engineering from the University of Electronic Science and Technology of China, Chengdu, in 2002 and the M.Sc.E. and Ph.D. degrees in mathematics and engineering from Queen's University, Kingston, ON, Canada, in 2003 and 2008, respectively.

He is currently a Senior Business Analyst with the Bank of Montreal Financial Group, Toronto, ON, Canada. His research interests lie in the general area of single- and multiuser information theory, in particular, joint source–channel coding and error control coding.

Fady Alajaji (S'90–M'94–SM'00) was born in Beirut, Lebanon, on May 1, 1966. He received the B.E. degree with distinction from the American University of Beirut, Lebanon, and the M.Sc. and Ph.D. degrees from the University of Maryland, College Park, all in electrical engineering, in 1988, 1990, and 1994, respectively.

He held a postdoctoral appointment in 1994 at the Institute for Systems Research, University of Maryland. In 1995, he joined the Department of Mathematics and Statistics at Queen's University, Kingston, ON, Canada, where he is currently a Professor of Mathematics and Engineering. Since 1997, he has also been cross-appointed in the Department of Electrical and Computer Engineering at the same university. His research interests include information theory, digital communications, error control coding, joint source–channel coding, and data compression.

Dr. Alajaji currently serves as Area Editor and Editor for Source and Source-Channel Coding for the IEEE TRANSACTIONS ON COMMUNICATIONS. He served as Co-Chair of the 1999 Canadian Workshop on Information Theory, as Co-Chair of the Technical Program Committee (TPC) of the 2004 Biennial Symposium on Communications, and as a TPC member of several international conferences and workshops. He received the Premier's Research Excellence Award from the Province of Ontario.

Tamás Linder (S'92–M'93–SM'00) was born in Budapest, Hungary, in 1964. He received the M.S. degree in electrical engineering from the Technical University of Budapest in 1988 and the Ph.D. degree in electrical engineering from the Hungarian Academy of Sciences, Budapest, in 1992.

He was a Postdoctoral Researcher at the University of Hawaii, Honolulu, in 1992 and a Visiting Fulbright Scholar at the Coordinated Science Laboratory, University of Illinois at Urbana-Champaign during 1993–1994. From 1994 to 1998, he was a faculty member in the Department of Computer Science and Information Theory at the Technical University of Budapest. From 1996 to 1998, he was also a visiting Research Scholar in the Department of Electrical and Computer Engineering, University of California, San Diego. In 1998, he joined

Queen's University, Kingston, ON, Canada, where he is now a Professor of Mathematics and Engineering in the Department of Mathematics and Statistics. His research interests include communications and information theory, source coding and vector quantization, machine learning, and statistical pattern recognition.

Dr. Linder received the Premier's Research Excellence Award of the Province of Ontario in 2002 and the Chancellor's Research Award of Queen's University in 2003. He was an Associate Editor for Source Coding of the IEEE TRANSACTIONS ON INFORMATION THEORY during 2003–2004.