On the Public Information Embedding Capacity Region Under Multiple Access Attacks[*]

Yangfan Zhong[†], Yadong Wang[‡], Fady Alajaji[†] and Tamás Linder[†]
[†] Dept. of Math. and Stat., Queen's University, Kingston, ON K7L 3N6, Canada
[‡] Bank of Montreal, 8th floor, 302 Bay St., Toronto, Canada
Email: {yangfan,fady,linder}@mast.queensu.ca
yadongwang@hotmail.com

Abstract— **We consider a public multi-user information embedding (watermarking) system in which two messages (watermarks) are independently embedded into two correlated covertexts and are transmitted through a multiple-access attack channel. The tradeoff between the achievable embedding rates and the average distortions for the two embedders is studied. For given distortion levels, inner and outer bounds for the embedding capacity region are obtained in single-letter form. Tighter bounds are also given for independent covertexts.**

I. Introduction

In the last decade, the single-user (point-to-point) information-hiding (information-embedding, watermarking) model has been thoroughly studied from an information-theoretic point of view; see [11], [1], [7] and the references therein. With the rapid development of wired and wireless communication networks, situations arise where privacy protection is no longer a point-to-point problem. Therefore, it is of interest to study information-hiding problems in multi-user settings.

In this paper, we consider the scenario in which two secret messages (watermarks) are independently embedded in two correlated sources (covertexts) and are then jointly decoded under multiple-access attacks. This scenario is motivated by, for example, the practical situation where audio and video frames are watermarked separately, but they are transmitted in a single bit stream and decoded by one multimedia player (cf. [9]). The model is depicted in Fig. 1. Assume that two users separately embed their watermarks W_1 and W_2 into two correlated discrete memoryless sources (DMSs), U_1 and U_2. Each user can only access one of the two covertexts. The watermarked messages (stegotexts) X_1^n and X_2^n are then sent through a multiple-access attack channel (MAAC) to a decoder which attempts to reconstruct the watermarks. For the two-user information embedding system, we are interested in determining the embedding capacity region, i.e., the two-dimensional set of all achievable embedding rate pairs under constraints on the embedding distortions.

Our first result is an inner bound for the embedding capacity region (Theorem 1). The proof is based on the approach of Gelfand and Pinsker [3] and a strong typicality coding/decoding argument. The encoders first map the watermarks W_1 and W_2 and the correlated covertexts U_1^n and U_2^n to auxiliary codewords T_1^n and T_2^n, and then generate two stegotexts X_1^n and X_2^n which are jointly typical with $(U_1^n, U_2^n, T_1^n, T_2^n)$. The decoder recovers the watermarks by examining the joint typicality of the received sequence Y^n and all auxiliary codeword pairs (T_1^n, T_2^n).

One major technical difficulty is the problem of how to separately construct the typical sequence encoders. In order to guarantee that the codewords together with the covertexts are jointly typical with a high probability, we adopt a "Markov" encoding scheme from [8], which was originally proposed for Gaussian multi-terminal source coding (see also [10] and [4]). The Markov encoders can be briefly described as follows. One of the encoders (embedders), say Encoder 1, first forms an estimate of the source sequence of the other encoder, and then generates T_1^n which is jointly typical with the observed source sequence U_1^n and the estimated source sequence. The other encoder, Encoder 2, first forms an estimate of the source sequence as well as the auxiliary codeword of Encoder 1, and then generates T_2^n which is jointly typical with the source sequence U_2^n and all the other sequences estimated. For the resulting scheme, an extended Markov lemma (Lemma 3) ensures that the auxiliary codewords T_1^n and T_2^n, although generated by separate encoders, are jointly typical with the source sequences with a high probability.

We also derive an outer bound for the embedding capacity region with single-letter characterization (Theorem 2), using Fano's inequality and a standard information-theoretical bounding argument. We next study the embedding capacity region when the two covertexts are independent of each other, and obtain inner and outer bounds for this case (Theorem 3). The inner bound is a consequence of Theorem 1, while in the converse part we sharpen the bound of Theorem 2 by making use of the independence condition.

We must point out that the multi-user information embedding problem studied in this paper is related to the works [9] and [6]. In [9], the authors present an achievable embedding region for correlated Gaussian covertexts and parallel (independent) additive Gaussian attack channels (as opposed to the MAAC considered here). In a recent work [6], the authors study the same system as ours and give an inner bound for the capacity region without a proof, stating that this inner bound can be easily proved via the coding procedure in [9]. However, the proof in [9] seems to be incorrect because the encoders

[*] This work was supported in part by NSERC of Canada.

978-1-4244-2571-6/08/$25.00

cannot guarantee the typicality of the output sequences with respect to the covertext sequences. Our code construction corrects this problem and in Theorem 1 we show that the main result in [9] (the achievable region) and the inner bound given in [6] are both correct; see Remark 3. We also point out that a similar setup concerning a multi-user reversible information embedding system was considered in [5] and [6] for two covertexts and a MAAC. Since in the reversible information embedding problem the secret messages and the covertexts are both reconstructed at the decoder, Gelfand and Pinsker coding is not required and the coding strategy is fundamentally different from ours.

II. Problem Formulation and Results

Let $|\mathcal{X}|$ denote the size of a finite set $\mathcal{X}$. If X is a random variable (RV) with distribution P_X, we denote its n-dimensional product distribution by $P_X^{(n)}$. Similar notation applies to joint and conditional distributions. For RVs X, Y, and Z with joint distribution P_{XYZ}, we use P_X, P_{XY}, $P_{YZ|X}$, etc., to denote the corresponding marginal and conditional probabilities induced by P_{XYZ}. The expectation of the RV X is denoted by $\mathbb{E}(X)$. All alphabets are finite, and all logarithms and exponentials are in base 2.

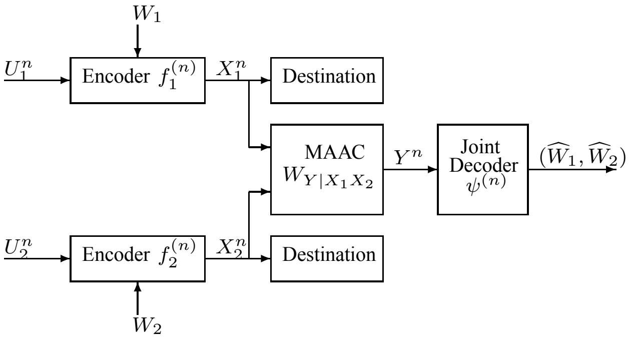

Fig. 1. A multi-user information embedding system with two embedders.

Let U_1 and U_2 be two discrete memoryless covertexts with alphabets $\mathcal{U}_1$ and $\mathcal{U}_2$ and joint distribution $Q_{U_1U_2}$. The watermarks W_1 and W_2 are independently and uniformly chosen from the sets $\mathcal{W}_1 \triangleq \{1,2,...,M_1\}$ and $\mathcal{W}_2 \triangleq \{1,2,...,M_2\}$, respectively. The attack channel is modeled as a two-sender one-receiver discrete memoryless MAAC $W_{Y|X_1X_2}$ having input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, output alphabet $\mathcal{Y}$, and transition probability distribution $W_{Y|X_1X_2}(y|x_1,x_2)$. The probability of receiving $\mathbf{y} \in \mathcal{Y}^n$ conditioned on sending $\mathbf{x}_1 \in \mathcal{X}_1^n$ and $\mathbf{x}_2 \in \mathcal{X}_2^n$ is hence given by $W_{Y|X_1X_2}^{(n)}(\mathbf{y}|\mathbf{x}_1,\mathbf{x}_2)$.

Let $d_i : \mathcal{U}_i \times \mathcal{X}_i \to [0,\infty)$ be single-letter distortion measures and define $d_i^{max} \triangleq \max\limits_{u_i,x_i} d_i(u_i,x_i)$ for $i=1,2$. For $\mathbf{u}_i \in \mathcal{U}_i^n$ and $\mathbf{x}_i \in \mathcal{X}_i^n$, let $d_i(\mathbf{u}_i,\mathbf{x}_i) = \sum_{j=1}^n d_i(u_{ij},x_{ij})$.

A two-sender one-receiver multiple-access embedding (MAE) code $(f_1^{(n)}, f_2^{(n)}, \psi^{(n)})$ with block length n consists of (see Fig. 1) two encoders (embedders) $f_1^{(n)} : \mathcal{W}_1 \times \mathcal{U}_1^n \longrightarrow \mathcal{X}_1^n$ and $f_2^{(n)} : \mathcal{W}_2 \times \mathcal{U}_2^n \longrightarrow \mathcal{X}_2^n$ with embedding rates $R_{f_1} = \frac{1}{n}\log_2 M_1$ and $R_{f_2} = \frac{1}{n}\log_2 M_2$, respectively, and a decoder $\psi^{(n)} : \mathcal{Y}^n \longrightarrow \mathcal{W}_1 \times \mathcal{W}_2$.

The system depicts a "public" embedding scenario since the covertexts are not available at the decoder. The probability of erroneously decoding the secret messages is given by

$$\begin{aligned} P_e^{(n)} &= P_e^{(n)}(f_1^{(n)}, f_2^{(n)}, \psi^{(n)}) \\ &\triangleq \Pr\left(\psi^{(n)}(Y^n) \neq (W_1,W_2)\right). \end{aligned}$$

Definition 1: Given $Q_{U_1U_2}$, $W_{Y|X_1X_2}$, a rate pair (R_1,R_2) is said to be achievable with respect to distortion levels (D_1,D_2) if there exists a sequence of MAE codes $(f_1^{(n)}, f_2^{(n)}, \psi^{(n)})$ at embedding rates no smaller than R_1 and R_2, respectively, such that $\lim_{n\to\infty} P_e^{(n)} = 0$ and $\limsup_{n\to\infty} \frac{1}{n}\mathbb{E}\left[d_i(U_i^n, f_i^{(n)}(W_i,U_i^n))\right] \le D_i$, $i=1,2$.

Definition 2: The embedding capacity region $\mathcal{R}(D_1,D_2)$ is the closure of the set of all achievable rate pairs (R_1,R_2).

Remark 1: It can be shown by using a time-sharing argument [2] that $\mathcal{R}(D_1,D_2)$ is convex.

Definition 3: Given $Q_{U_1U_2}$, $W_{Y|X_1X_2}$, and a pair of distortion levels (D_1,D_2), let $\mathcal{S}_{D_1,D_2}$ be the set of RVs $(U_1,T_1,U_2,T_2,X_1,X_2,Y) \in \mathcal{U}_1 \times \mathcal{T}_1 \times \mathcal{U}_2 \times \mathcal{T}_2 \times \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{Y}$ for some finite alphabets $\mathcal{T}_1$ and $\mathcal{T}_2$ such that the joint distribution $P_{U_1T_1U_2T_2X_1X_2Y}$ satisfies: (1) $P_{U_1T_1U_2T_2X_1X_2Y} = Q_{U_1U_2}P_{T_1X_1|U_1}P_{T_2X_2|U_2}W_{Y|X_1X_2}$, (2) $I(U_i;T_i) > 0$, and (3) $\mathbb{E}[d_i(U_i,X_i)] \le D_i$, for $i=1,2$.

Definition 4: Given $Q_{U_1U_2}$, $W_{Y|X_1X_2}$, and a pair of distortion levels (D_1,D_2), let $\mathcal{P}_{D_1,D_2}$ be the set of RVs $(U_1,T_1,U_2,T_2,X_1,X_2,Y) \in \mathcal{U}_1 \times \mathcal{T}_1 \times \mathcal{U}_2 \times \mathcal{T}_2 \times \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{Y}$ for some finite alphabets $\mathcal{T}_1$ and $\mathcal{T}_2$ such that the joint distribution $P_{U_1T_1U_2T_2X_1X_2Y}$ satisfies: (1) $P_{U_1T_1U_2T_2X_1X_2Y} = Q_{U_1U_2}P_{T_1T_2X_1X_2|U_1U_2}W_{Y|X_1X_2}$, and (2) $\mathbb{E}[d_i(U_i,X_i)] \le D_i$, for $i=1,2$.

By definition, $\mathcal{S}_{D_1,D_2} \subseteq \mathcal{P}_{D_1,D_2}$. The following are the main results of the paper.

Theorem 1: Let $\mathcal{R}_{in}(D_1,D_2)$ be the closure of the convex hull of all (R_1,R_2) satisfying

$$\begin{aligned} R_1 &< I(T_1;T_2,Y) - I(U_1;T_1), && (1) \\ R_2 &< I(T_2;T_1,Y) - I(U_2;T_2), && (2) \\ R_1+R_2 &< I(T_1,T_2;Y) - I(U_1,U_2;T_1,T_2), && (3) \end{aligned}$$

for some $(U_1,T_1,U_2,T_2,X_1,X_2,Y) \in \mathcal{S}_{D_1,D_2}$. Then $\mathcal{R}_{in}(D_1,D_2) \subseteq \mathcal{R}(D_1,D_2)$.

Remark 2: The cardinality of the alphabets of the auxiliary RVs T_1 and T_2 for $\mathcal{R}_{in}(D_1,D_2)$ can be bounded as $|\mathcal{T}_i| \le |\mathcal{U}_1||\mathcal{U}_2||\mathcal{X}_i| + 1$, $i=1,2$.

Remark 3: Although we only deal with discrete (finite-alphabet) sources and channels, it is not hard to see that, with the appropriate changes in the proof, the achievable region is also valid for a system that incorporates a pair of correlated memoryless Gaussian sources and a Gaussian MAAC. In particular, when the MAAC is a pair of parallel (independent) additive Gaussian channels, $\widehat{\mathcal{R}}_{in}(D_1,D_2)$ is the achievable region obtained in [9], even though the proof provided in [9] is not entirely correct. Note also that our inner bound

$\mathcal{R}_{in}(D_1,D_2)$ is the same as the one given without proof in [6, Proposition 1].

Theorem 2: Let $\mathcal{R}_{out}(D_1,D_2)$ be the closure of all the set of (R_1,R_2) satisfying conditions (1)–(3) for some $(U_1,T_1,U_2,T_2,X_1,X_2,Y)\in\mathcal{P}_{D_1,D_2}$. Then $\mathcal{R}(D_1,D_2)\subseteq\mathcal{R}_{out}(D_1+\delta,D_2+\delta)$ for all $\delta>0$.

Remark 4: The above theorem, which can be proved using a standard Fano's inequality based argument (as in [3], [11]), states that $\mathcal{R}(D_1,D_2)\subseteq\bigcap_{\delta>0}\mathcal{R}_{out}(D_1+\delta,D_2+\delta)$. If we could upper bound the cardinality of the alphabet sizes of the auxiliary RVs T_1 and T_2 in the definition of $\mathcal{R}_{out}(D_1,D_2)$, it would be easy to show that $\bigcap_{\delta>0}\mathcal{R}_{out}(D_1+\delta,D_2+\delta)=\mathcal{R}_{out}(D_1,D_2)$, so that $\mathcal{R}(D_1,D_2)\subseteq\mathcal{R}_{out}(D_1,D_2)$. However, without such an upper bound, we can only state the theorem in the present weaker form. The same remark applies to the outer bound in the next theorem.

We next consider the special case when the covertexts are independent, i.e., $Q_{U_1U_2}=Q_{U_1}Q_{U_2}$. We then have the following inner and outer bounds.

Theorem 3: Let $Q_{U_1U_2}=Q_{U_1}Q_{U_2}$. Let $\mathcal{R}^*_{in}(D_1,D_2)$ be the closure of the convex hull of all (R_1,R_2) satisfying

$$R_1 < I(T_1;Y|T_2)-I(U_1;T_1) \quad (4)$$

$$R_2 < I(T_2;Y|T_1)-I(U_2;T_2) \quad (5)$$

$$R_1+R_2 < I(T_1,T_2;Y)-I(U_1;T_1)-I(U_2;T_2) \quad (6)$$

for some $(U_1,T_1,U_2,T_2,X_1,X_2,Y)\in\mathcal{S}_{D_1,D_2}$, and let $\mathcal{R}^*_{out}(D_1,D_2)$ be the closure of all (R_1,R_2) satisfying (4)–(6) for some $(U_1,T_1,U_2,T_2,X_1,X_2,Y)\in\mathcal{P}_{D_1,D_2}$. Then

$$\mathcal{R}^*_{in}(D_1,D_2)\subseteq\mathcal{R}(D_1,D_2)\subseteq\mathcal{R}^*_{out}(D_1+\delta,D_2+\delta)$$

for all $\delta>0$.

Remark 5: The cardinality of the alphabets of the auxiliary RVs T_1 and T_2 for $\mathcal{R}^*_{in}(D_1,D_2)$ can be bounded as $|\mathcal{T}_i|\le|\mathcal{U}_i||\mathcal{X}_i|+1$, $i=1,2$.

Remark 6: In the simple case of independent covertexts $Q_{U_1U_2}=Q_{U_1}Q_{U_2}$ and parallel MAAC $W_{Y|X_1X_2}=W_{Y_1|X_1}W_{Y_2|X_2}$ (where $\mathcal{Y}=\mathcal{Y}_2\times\mathcal{Y}_2$), the inner and outer bounds of Theorem 3 coincide and reduce to the capacity formula of two parallel single-user watermarking systems [7], [11].

III. Proof of Theorem 1

We first recall some notation and facts regarding strongly ϵ-typicality.

Let $V\triangleq(X_1,X_2,...,X_m)$ be a superletter (a collection of RVs) taking values in a finite set $\mathcal{V}\triangleq\mathcal{X}_1\times\mathcal{X}_2\times\cdots\times\mathcal{X}_m$ and having joint distribution $P_V(x_1,...,x_m)$, which for simplicity we also denote by $P_V(v)$. Denote by $T_\epsilon^{(n)}(V)$ or $T_\epsilon^{(n)}$ the set of all strongly ϵ-typical sequences [2, p. 326] with respect to the joint distribution $P_V(v)$. Let $I_V\triangleq\{1,2,...,m\}$, and $I_G\subseteq I_V$. We then let $G=(X_{g_1},X_{g_2},...,X_{g_{|I_G|}})\in\mathcal{G}$ be a "sub-superletter" corresponding to I_G such that $g_i\in I_G$. Let G, K, and L be sub-superletters of V such that I_G, I_K, I_L are disjoint, and let P_G, P_K and $P_{G|K}$ be the marginal and conditional distributions induced by P_V, respectively. Denote by $T_\epsilon^{(n)}(G)$ the projection of $T_\epsilon^{(n)}(V)$ to the coordinates of G. Given any $\mathbf{k}\in\mathcal{K}^n$, denote $T_\epsilon^{(n)}(G|\mathbf{k})\triangleq\left\{(G^n,\mathbf{k})\in T_\epsilon^{(n)}(G,K)\right\}$. Clearly $T_\epsilon^{(n)}(G|\mathbf{k})=\emptyset$ if $\mathbf{k}\notin T_\epsilon^{(n)}(K)$. The following lemma (see, e.g., [2, pp. 342–343]) restates the well known exponential bounds for the cardinality of strongly typical sets. In the lemma $\eta=\eta(\epsilon,n)$ is a generic positive term such that $\lim_{\epsilon\to0}\lim_{n\to\infty}\eta(\epsilon,n)=0$.

Lemma 1: [2]

i) $2^{n(H(K)-\eta)}\le\left|\mathcal{T}_\epsilon^{(n)}(K)\right|\le2^{n(H(K)+\eta)}$.

ii) For any $\mathbf{k}\in\mathcal{T}_\epsilon^{(n)}(K)$, $2^{n(H(G|K)-\eta)}\le\left|\mathcal{T}_\epsilon^{(n)}(G|\mathbf{k})\right|\le 2^{n(H(G|K)+\eta)}$.

Finally, we recall the Markov lemma for joint strong ϵ-typicality.

Lemma 2: (Markov Lemma [2, p. 579]) Let $G\to K\to L$ form a Markov chain in this order. For any $0<\epsilon_0<1$ and $(\mathbf{g},\mathbf{k})\in T_\epsilon^{(n)}(G,K)$,

$$P_{L|K}^{(n)}\left((\mathbf{g},\mathbf{k},L^n)\in T_\epsilon^{(n)}(G,K,L)\middle|\,\mathbf{k}\right)>1-\epsilon_0$$

for n sufficiently large, independently of $(\mathbf{g},\mathbf{k})$.

A. Outline of Proof

We need to show that for given $Q_{U_1U_2}$, $W_{Y|X_1X_2}$, and any $(R_1,R_2)\in\mathcal{R}_{in}(D_1,D_2)$, there exists a sequence of codes $(f_1^{(n)},f_2^{(n)},\psi^{(n)})$ such that $P_e^{(n)}\to0$ as $n\to\infty$ and for any $\delta>0$, $\frac{1}{n}\mathbb{E}[d_i(U_i^n,f_i^{(n)}(W_i,U_i^n))]\le D_i+\delta$, $i=1,2$, for n sufficiently large.

Fix $(P_{T_1|U_1},P_{X_1|U_1T_1},P_{T_2|U_2},P_{X_2|U_2T_2})$ such that $I(U_i;T_i)>0$ and the following are satisfied for some $\epsilon'>0$,

$$R_1<I(T_1;T_2,Y)-I(U_1;T_1)-\epsilon', \quad (7)$$

$$R_2<I(T_2;T_1,Y)-I(U_2;T_2)-\epsilon', \quad (8)$$

$$R_1+R_2<I(T_1,T_2;Y)-I(U_1,U_2;T_1,T_2)-\epsilon', \quad (9)$$

$$\mathbb{E}[d_i(U_i,X_i)]\le D_i,\ i=1,2. \quad (10)$$

The encoders $f_1^{(n)}$ and $f_2^{(n)}$ are chosen in a random manner. For $\epsilon<\frac{\delta}{2\max\{d_1^{max},d_2^{max}\}}$, define

$$P_i^{(n)}\triangleq\Pr\Big(\frac{1}{n}d_i\big(U_i^n,f_i^{(n)}(W_i,U_i^n)\big)>D_i+\epsilon d_i^{max}\Big),\ i=1,2.$$

We will prove that for any $0<\epsilon_1\le\frac{\delta}{6\max\{d_1^{max},d_2^{max}\}}$, the probabilities $P_e^{(n)}$, $P_1^{(n)}$, and $P_2^{(n)}$, when averaged over the random choice of $f_1^{(n)}$ and $f_2^{(n)}$, satisfy $\mathbb{E}[P_e^{(n)}]\le\epsilon_1$, $\mathbb{E}[P_1^{(n)}]\le\epsilon_1$, $\mathbb{E}[P_2^{(n)}]\le\epsilon_1$ for n sufficiently large. Then $\mathbb{E}\{P_e^{(n)}+P_1^{(n)}+P_2^{(n)}\}\le3\epsilon_1$, which guarantees that there exists at least one pair of codes $(f_1^{(n)},f_2^{(n)})$ such that $P_e^{(n)}+P_1^{(n)}+P_2^{(n)}\le3\epsilon_1$ and hence $P_e^{(n)}\le3\epsilon_1$, $P_1^{(n)}\le3\epsilon_1$, $P_2^{(n)}\le3\epsilon_1$ are simultaneously satisfied for n sufficiently large. Finally, it can be easily shown that $P_i^{(n)}\le3\epsilon_1$ implies for n sufficiently large that

$$\frac{1}{n}\mathbb{E}\left[d_i(U_i^n,f_i^{(n)}(W_i,U_i^n)\right]\le D_i+\epsilon d_i^{max}+P_i^{(n)}d_i^{max}\le D_i+\delta.$$

B. Random Code Design

In what follows, the strongly ϵ-typical set $\mathcal{T}_\epsilon^{(n)}$ is defined under the joint distribution $P_{U_1U_2T_1T_2X_1X_2Y}$ which can be factorized as $Q_{U_1U_2}P_{T_1|U_1}P_{X_1|U_1T_1}P_{T_2|U_2}P_{X_2|U_2T_2}W_{Y|X_1X_2}$. The parameter ϵ, which is chosen to be sufficiently small, will be specified later in the proof.

Generation of codebooks. For $i = 1, 2$ and every $w_i \in \mathcal{W}_i$, generate a codebook

$$\mathcal{C}_{w_i} = \{\mathbf{t}_i(w_i, 1), \mathbf{t}_i(w_i, 2), ..., \mathbf{t}_i(w_i, L_i)\}$$

with $L_i = \lceil 2^{n[I(U_i;T_i)+4\epsilon]}\rceil$ codewords such that each $\mathbf{t}_i(w_i, l_i)$ is independently selected with uniform distribution from the typical set $\mathcal{T}_\epsilon^{(n)}(T_i)$. Denote the entire codebook for Encoder i by $\mathcal{C}^{(i)} = \{\mathcal{C}_{w_i}\}_{w_i=1}^{M_i}$, where we recall that $M_i = \lceil 2^{nR_i}\rceil$. For each $\mathbf{u}_i$ and codeword $\mathbf{t}_i(w_i, l_i)$ $(1 \le w_i \le M_i, 1 \le l_i \le L_i)$, generate a codeword $\mathbf{x}_i$ according to $P^{(n)}_{X_i|U_iT_i}(\mathbf{x}_i|\mathbf{u}_i, \mathbf{t}_i)$. Denote the codebook of all the codewords $\mathbf{x}_i$ by $\mathcal{B}^{(i)}$.

Encoder $f_1^{(n)}$: Encoder $f_1^{(n)}$ is the concatenation of a pre-encoder $\varphi_1^{(n)} : \mathcal{W}_1 \times \mathcal{U}_1^n \longrightarrow \mathcal{T}_1^n$ and a mapping $g_1^{(n)} : \mathcal{U}_1^n \times \mathcal{T}_1^n \longrightarrow \mathcal{X}_1^n$.

To define $\varphi_1^{(n)}$, we need the following notation adopted from [8]. We let

$$\begin{aligned} &A^{(n)}(\mathbf{u}_1, \mathbf{t}_1) \\ &\quad\triangleq\; P^{(n)}_{U_2T_2|U_1T_1}\left((U_2^n, T_2^n) \in \mathcal{T}_\epsilon^{(n)}(U_2T_2|\mathbf{u}_1, \mathbf{t}_1)\Big|\, \mathbf{u}_1, \mathbf{t}_1\right), \end{aligned}$$

and for $\mu \in (0, 1)$ define

$$\mathcal{F}^{(n)}_{\mu,\epsilon}(U_1, T_1) \triangleq \left\{(\mathbf{u}_1, \mathbf{t}_1) : A^{(n)}(\mathbf{u}_1, \mathbf{t}_1) \ge 1 - \mu\right\}.$$

By definition, we have $\mathcal{F}^{(n)}_{\mu,\epsilon}(U_1, T_1) \subseteq \mathcal{T}_\epsilon^{(n)}(U_1, T_1)$.

We now describe the pre-encoding function $\varphi_1^{(n)} = \varphi_1^{(n)}(w_1, \mathbf{u}_1)$ which maps every pair $(w_1, \mathbf{u}_1)$ to a codeword in $\mathcal{C}^{(1)} \subseteq \mathcal{T}_1^n$. Given $w_1 \in \{1, 2, ..., M_1\}$ and $\mathbf{u}_1$, $\varphi_1^{(n)}$ seeks the first codeword $\mathbf{t}_1(w_1, l_1)$ (if any) in $\mathcal{C}_{w_1}$ such that $(\mathbf{u}_1, \mathbf{t}_1(w_1, l_1)) \in \mathcal{F}^{(n)}_{\mu,\epsilon}(U_1, T_1)$. If there is no such codeword, $\varphi_1^{(n)}$ outputs $\mathbf{t}_1(w_1, 1)$. Next, for each output $\mathbf{t}_1(w_1, l_1)$ and $\mathbf{u}_1$, $g_1^{(n)}$ sends out the associated codeword $\mathbf{x}_1(w_1, \mathbf{u}_1)$ to the channel. Thus, $f_1^{(n)}(w_1, \mathbf{u}_1) = g_1^{(n)}\left(\mathbf{u}_1, \varphi_1^{(n)}(w_1, \mathbf{u}_1)\right)$.

Encoder $f_2^{(n)}$: Encoder $f_2^{(n)}$ is the concatenation of a pre-encoder $\varphi_2^{(n)} : \mathcal{W}_2 \times \mathcal{U}_2^n \longrightarrow \mathcal{T}_2^n$ and a mapping $g_2^{(n)} : \mathcal{U}_2^n \times \mathcal{T}_2^n \longrightarrow \mathcal{X}_2^n$.

To define $\varphi_2^{(n)}$, let

$$\begin{aligned} B^{(n)}_{\varphi_1}(\mathbf{u}_2, \mathbf{t}_2) \triangleq \frac{1}{2^{nR_1}} \sum_{w_1=1}^{M_1} P^{(n)}_{U_1|U_2T_2}&\left((U_1^n, \varphi_1^{(n)}(w_1, U_1^n))\right. \\ &\left.\in \mathcal{T}_\epsilon^{(n)}(U_1T_1|\mathbf{u}_2, \mathbf{t}_2)\Big|\, \mathbf{u}_2, \mathbf{t}_2\right), \end{aligned}$$

and for $\nu \in (0, 1)$ define

$$\mathcal{F}^{(n)}_{\varphi_1,\nu,\epsilon}(U_2, T_2) \triangleq \left\{(\mathbf{u}_2, \mathbf{t}_2) : B^{(n)}_{\varphi_1}(\mathbf{u}_2, \mathbf{t}_2) \ge 1 - \nu\right\}.$$

By definition, $\mathcal{F}^{(n)}_{\varphi_1,\nu,\epsilon}(U_2, T_2) \subseteq \mathcal{T}_\epsilon^{(n)}(U_2, T_2)$.

The pre-encoding function $\varphi_2^{(n)} = \varphi_2^{(n)}(w_2, \mathbf{u}_2)$ which maps every pair $(w_2, \mathbf{u}_2)$ to a codeword in $\mathcal{C}^{(2)} \subseteq \mathcal{T}_2^n$ is defined as below. Given $w_2 \in \{1, 2, ..., M_2\}$ and $\mathbf{u}_2$, $\varphi_2^{(n)}$ seeks the first codeword $\mathbf{t}_2(w_2, l_2)$ (if any) in $\mathcal{C}_{w_2}$ such that $(\mathbf{u}_2, \mathbf{t}_2(w_2, l_2)) \in \mathcal{F}^{(n)}_{\varphi_1,\nu,\epsilon}(U_2, T_2)$. If there is no such codeword, $\varphi_2^{(n)}$ outputs $\mathbf{t}_2(w_2, 1)$. Next, for each output $\mathbf{t}_2(w_2, l_2)$, $g_2^{(n)}$ sends out the associated codeword $\mathbf{x}_2(w_2, \mathbf{u}_2)$ to the channel. Thus, $f_2^{(n)}(w_2, \mathbf{u}_2) = g_2^{(n)}\left(\mathbf{u}_2, \varphi_2^{(n)}(w_2, \mathbf{u}_2)\right)$.

Decoder $\psi^{(n)}$: Given $\mathbf{y}$, $\psi^{(n)}$ seeks $\mathbf{t}_1(\widehat{w}_1, \widehat{l}_1) \in \mathcal{C}^{(1)}$ and $\mathbf{t}_2(\widehat{w}_2, \widehat{l}_2) \in \mathcal{C}^{(2)}$ such that

$$(\mathbf{t}_1(\widehat{w}_1, \widehat{l}_1), \mathbf{t}_2(\widehat{w}_2, \widehat{l}_2), \mathbf{y}) \in \mathcal{T}_\epsilon^{(n)}(T_1, T_2, Y).$$

If such a pair $(\mathbf{t}_1(\widehat{w}_1, \widehat{l}_1), \mathbf{t}_2(\widehat{w}_2, \widehat{l}_2))$ exists for a unique $(\widehat{w}_1, \widehat{w}_2)$, then $\psi^{(n)}$ outputs $\widehat{w}_1$ and $\widehat{w}_2$ as the decoded messages. If there is no such pair $(\widehat{w}_1, \widehat{w}_2)$, or it is not unique, a decoding error is declared. Letting $\mathbf{t}_i(w_i, l_i) = \varphi_i^{(n)}(w_i, \mathbf{u}_i)$, it is easy to see that if there is a decoding error, then at least one of the following events occurs:

i) E_1: $(\mathbf{t}_1(w_1, l_1), \mathbf{t}_2(w_2, l_2), \mathbf{y}) \notin \mathcal{T}_\epsilon^{(n)}(T_1, T_2, Y)$,

ii) E_2: there exist l_1' and $w_1' \ne w_1$ and l_2' (l_2' may or may not be equal to l_2) such that $(\mathbf{t}_1(w_1', l_1'), \mathbf{t}_2(w_2, l_2'), \mathbf{y}) \in \mathcal{T}_\epsilon^{(n)}(T_1, T_2, Y)$,

iii) E_3: there exist l_2' and $w_2' \ne w_2$ and l_1' (l_1' may or may not be equal to l_1) such that $(\mathbf{t}_1(w_1, l_1'), \mathbf{t}_2(w_2', l_2'), \mathbf{y}) \in \mathcal{T}_\epsilon^{(n)}(T_1, T_2, Y)$,

iv) E_4: there exist l_1' and $w_1' \ne w_1$ and l_2' and $w_2' \ne w_2$ such that $(\mathbf{t}_1(w_1', l_1'), \mathbf{t}_2(w_2', l_2'), \mathbf{y}) \in \mathcal{T}_\epsilon^{(n)}(T_1, T_2, Y)$.

In the following, we will bound the probabilities $P_e^{(n)}$, $P_1^{(n)}$, and $P_2^{(n)}$ averaged over the random choice of the codes $\mathcal{C}^{(1)}$, and $\mathcal{C}^{(2)}$. To simplify the notation we abbreviate $\mathbb{E}_{\mathcal{C}^{(1)},\mathcal{C}^{(2)}}[\,\cdot\,]$ to $\mathbb{E}_\Omega[\,\cdot\,]$.

C. Bounding $\mathbb{E}_\Omega[P_e^{(n)}]$

To analyze the average probability of error, we need the following lemma.

Lemma 3: For any $w_1 \in \mathcal{W}_1$, $w_2 \in \mathcal{W}_2$, and any $\epsilon_0, \epsilon \in (0, 1)$, one can choose $\mu, \nu \in (0, 1)$ small enough such that

$$\begin{aligned} \mathbb{E}_{\mathcal{C}^{(1)},\mathcal{C}^{(2)}}\Big[P^{(n)}_{U_1U_2}&\left((\varphi_1^{(n)}(w_1, U_1^n), U_1^n, U_2^n, \varphi_2^{(n)}(w_2, U_2^n))\right. \\ &\left.\in \mathcal{T}_\epsilon^{(n)}(T_1, U_1, U_2, T_2)\right)\Big] \ge 1 - \epsilon_0 \end{aligned}$$

for n sufficiently large, where the expectation is taken with respect to the random codes $\mathcal{C}^{(1)}$ and $\mathcal{C}^{(2)}$.

The proof is very similar to the proof of the extended Markov lemma in [8, Lemma 3] for correlated Gaussian sources and is hence omitted.

Since the watermarks are independently and uniformly distributed, and by the symmetry of the code construction, we can assume without the loss of generality that some fixed $w_1 \in \mathcal{W}_1$ and $w_2 \in \mathcal{W}_2$ are the transmitted watermarks. Thus we bound the probability of error as

$$\begin{aligned} P_e^{(n)} &= \Pr\left(\left\{\psi^{(n)}(Y^n) \ne (w_1, w_2)\right\}\right) \\ &\le \Pr(A_1) + \Pr\left(\left\{\psi^{(n)}(Y^n) \ne (w_1, w_2)\right\}\Big|\, A_1^c\right) \quad (11) \end{aligned}$$

where A_1 is the event that

$$(\mathbf{t}_1(w_1,l_1),\mathbf{u}_1,\mathbf{u}_2,\mathbf{t}_2(w_2,l_2),\mathbf{x}_1,\mathbf{x}_2) \notin \mathcal{T}_\epsilon^{(n)}(T_1,U_1,U_2,T_2,X_1,X_2).$$

Recall that $\mathbf{t}_i(w_i,l_i)=\varphi_i^{(n)}(w_i,\mathbf{u}_i)$, $i=1,2$. We also let $\mathbf{t}_i(w_i,l_i')$ and $\mathbf{t}_i(w_i',l_i')$ be the l_i'-th codeword in the codebook $\mathcal{C}_{w_i}$ and $\mathcal{C}_{w_i'}$, respectively. We then introduce the event

$$A_0 : (\mathbf{t}_1(w_1,l_1),\mathbf{u}_1,\mathbf{u}_2,\mathbf{t}_2(w_2,l_2)) \notin \mathcal{T}_\epsilon^{(n)}(T_1,U_1,U_2,T_2).$$

Taking expectation in (11) and using the union bound, we have

$$\begin{aligned}\mathbb{E}_\Omega[P_e^{(n)}] \quad \le \quad & \mathbb{E}_\Omega \mathrm{Pr}\left(A_0\right)+\mathbb{E}_\Omega \mathrm{Pr}\left(A_1|A_0^c\right) \\ & +\mathbb{E}_\Omega \mathrm{Pr}\left(E_1|A_1^c\right)+\sum_{k=2}^{4}\mathbb{E}_\Omega \mathrm{Pr}\left(E_k|A_1^c\right)\end{aligned}\tag{12}$$

It immediately follows from Lemma 3 that

$$\mathbb{E}_\Omega \mathrm{Pr}\left(A_0\right)=\mathbb{E}_{\mathcal{C}^{(1)},\mathcal{C}^{(2)}}\mathrm{Pr}\left(A_0\right)\le \epsilon_0 \tag{13}$$

for n sufficiently large, where we set $\epsilon_0=\epsilon_1/7$ for a given $\epsilon_1\ge 0$ throughout the proof. Since X_1^n and X_2^n are drawn according to the conditional probabilities $P_{X_1|U_1T_1}^{(n)}(\cdot|\mathbf{u}_1,\mathbf{t}_1)$ and $P_{X_2|U_2T_2}^{(n)}(\cdot|\mathbf{u}_2,\mathbf{t}_2)$, respectively, and Y^n is drawn according to the conditional distribution $W_{Y|X_1X_2}^{(n)}(\cdot|\mathbf{x}_1,\mathbf{x}_2)$, it follows from two successive applications of Lemma 2 that

$$\mathbb{E}_\Omega \mathrm{Pr}\left(\left.A_1\right| A_0^c\right)\le \mathbb{E}_\Omega[\epsilon_0]=\epsilon_0 \tag{14}$$

and

$$\mathbb{E}_\Omega \mathrm{Pr}\left(\left.E_1\right| A_1^c\right)\le \mathbb{E}_\Omega[\epsilon_0]=\epsilon_0 \tag{15}$$

for n sufficiently large. It remains to bound $\mathbb{E}_\Omega \mathrm{Pr}\left\{\left.E_k\right| A_1^c\right\}$ for $k=2,3,4$. Applying the union bound, Lemma 1, and assumption (7), we can obtain the upper bound

$$\begin{aligned}\mathbb{E}_\Omega \mathrm{Pr}\left(\left.E_2\right| A_1^c\right) & \le 2^{n[R_1+I(U_1;T_1)+4\epsilon-I(T_1;T_2,Y)+2\eta]} \\ & \le 2^{n[R_1+I(U_1;T_1)-I(T_1;T_2,Y)+\epsilon']} \\ & \le \epsilon_0\end{aligned}\tag{16}$$

for ϵ sufficiently small and n sufficiently large. Similarly, using the union bound, Lemma 1, and assumption (8) yields

$$\mathbb{E}_\Omega \mathrm{Pr}\left(\left.E_3\right| A_1^c\right)\le \epsilon_0 \tag{17}$$

for ϵ small enough and n sufficiently large. Next, applying the union bound, Lemma 1, and assumption (9), we have

$$\begin{aligned}&\mathbb{E}_\Omega \mathrm{Pr}\left(\left.E_4\right| A_1^c\right) \\ &\quad \le 2^{n[R_1+R_2+I(U_1;T_1)+I(U_2;T_2)-I(T_1,T_2;Y)-I(T_1;T_2)+8\epsilon+3\eta]} \\ &\quad \le 2^{n[R_1+I(U_1,U_2;T_1,T_2)-I(T_1,T_2;Y)+\epsilon']} \\ &\quad \le \epsilon_0\end{aligned}\tag{18}$$

for n sufficiently large and ϵ small enough (such that $8\epsilon+3\eta<\epsilon'$). Here the second inequality holds by the Markov chain relation $T_1\to U_1\to U_2\to T_2$. Finally, substituting (13)–(15), (16), (17) and (18) into (12) yields $\mathbb{E}_\Omega[P_e^{(n)}]\le 7\epsilon_0=\epsilon_1$ for ϵ sufficiently small and n sufficiently large.

D. Bounding $\mathbb{E}_\Omega[P_i^{(n)}]$

We only bound $\mathbb{E}_\Omega[P_i^{(n)}]$ for $i=1$, since the case $i=2$ can be dealt with similarly. When $(\mathbf{u}_1,\mathbf{x}_1(w_1,\mathbf{u}_1))\in\mathcal{T}_\epsilon^{(n)}(U_1,X_1)$,

$$\frac{1}{n}d_1\big(\mathbf{u}_1,\mathbf{x}_1(w_1,\mathbf{u}_1)\big)\le \mathbb{E}[d_1(U_1,X_1)]+\epsilon d_1^{max}\le D_1+\epsilon d_1^{max}$$

for n sufficiently large, where the first inequality follows from the definition of strong typicality and the second inequality follows from (10). This means that if $\frac{1}{n}d_1\big(U_1^n,f_1^{(n)}(W_1,U_1^n)\big)>D_1+\epsilon d_1^{max}$, then we must have $\big(U_1^n,f_1^{(n)}(W_1,U_1^n)\big)\notin\mathcal{T}_\epsilon^{(n)}(U_1,X_1)$ for n sufficiently large. Thus, applying Lemmas 3 and 2 we can bound

$$\mathbb{E}_\Omega[P_1^{(n)}]\le \mathrm{Pr}\left(\big(U_1^n,f_1^{(n)}(W_1,U_1^n)\big)\notin\mathcal{T}_\epsilon^{(n)}(U_1,X_1)\right)\le\epsilon_1$$

for n sufficiently large. ■

IV. Conclusion

We study a multi-user information embedding system consisting of two information embedders and one joint decoder. We obtain an inner bound for the capacity region in a computable single-letter form. We also derive an outer bound for the capacity region in a single-letter form, but it is not clear how to explicitly calculate the resulting region since we are not able to bound the cardinality of its auxiliary RVs. We also address the special case when the covertexts are independent of each other and inner and outer bounds for the capacity region of this simplified system are provided.

References

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

[2] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2^{nd} Edition, Wiley, 2006.

[3] S. Gelfand and M. Pinsker, "Coding for a channel with random parameters," *Problems of Control and Information Theory*, vol. 9, pp. 19–31, 1980.

[4] T. S. Han and K. Kobayashi, "A unified achievable rate region for a general class of multiterminal source coding systems," *IEEE Trans. Inform. Theory*, vol. 26, no. 3, pp. 396–412, May 1980.

[5] S. Kotagiri and J. N. Laneman, "Reversible information embedding in multi-user channels," *Proc. Allerton Conf. Communications, Control, and Computing*, Monticello, IL, Sept. 2005.

[6] S. Kotagiri and J. N. Laneman, "Variations on information embedding in multiple access and broadcast channels," submitted to *IEEE Trans. Inform. Theory*, Nov. 2007. Draft available at http://www.nd.edu/~jnl/group/shivaprasad-kotagiri/

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

[8] Y. Oohama, "Gaussian multiterminal source coding," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1912–1923, Nov. 1997.

[9] W. Sun and E. H. Yang, "On achievable regions of public multiple-access Gaussian watermarking systems," *Proc. 6th Int. Inform. Hiding Workshop*, Toronto, Canada, May 23–25, 2004.

[10] S. Y. Tung, "Multiterminal source coding," Ph.D dissertation, School of Electrical Engineering, Cornell Univ., Ithaca, NY, May 1978.

[11] F. M.J. Willems, "An information-theoretical approach to information embedding," Proc. *21st Symposium on Information Theory*, pp. 255–260, Wassenaar, The Netherlands, May 25–26, 2000.