

Perfectly Secure Steganography: Capacity, Error Exponents, and Code Constructions

Ying Wang, *Student Member, IEEE*, and Pierre Moulin, *Fellow, IEEE*

Abstract

An analysis of steganographic systems subject to the following *perfect undetectability* condition is presented in this paper. Following embedding of the message into the coverttext, the resulting stegotext is required to have *exactly* the same probability distribution as the coverttext. Then no statistical test can reliably detect the presence of the hidden message. We refer to such steganographic schemes as *perfectly secure*. A few such schemes have been proposed in recent literature, but they have vanishing rate. We prove that communication performance can potentially be vastly improved; specifically, we construct perfectly secure steganographic codes from public watermarking codes using binning methods and randomization of the code over an invariant group associated with the coverttext distribution (e.g., a permutation group in the case of independently and identically distributed coverttext). We derive (positive) capacity and random-coding exponents for perfectly secure steganographic systems.

In our steganographic problem, communication may be disrupted by an *active warden*, modelled here by a compound discrete memoryless channel. The transmitter and warden are subject to distortion constraints. In our basic setup, the coverttext samples are independently and identically distributed (i.i.d.) over a finite alphabet. A secret key is shared by the encoder and decoder and provides the desired perfect security via randomization of the steganographic code. We address the potential loss in communication performance due to the perfect security requirement. We show that no loss occurs if the coverttext distribution is uniform and the distortion metric is cyclically symmetric; steganographic capacity is then achieved by randomized linear codes. Finally, we extend our result to an abstract setting which unifies several types of coding strategies and is applicable to coverttexts with Markov dependencies and to coverttexts defined over continuous alphabets. This framework may also be useful for developing computationally secure steganographic systems that have near-optimal communication performance.

Index Terms

Steganography, watermarking, secret communication, timing channels, capacity, reliability function, error exponents, binning codes, randomized codes, universal codes, Markov processes.

This work was supported by NSF under grants CCR 02-08809 and CCR 03-25924, and presented in part at the 40th Conference on Information Sciences and Systems (CISS), Princeton, NJ, March 2004. Ying Wang was with the Department of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign and is now with Qualcomm Flarion Technologies, Bedminster, NJ 07921 USA (e-mail: yingw@qualcomm.com). Pierre Moulin is with the Beckman Institute, Coordinate Science Lab and Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61801 USA (e-mail: moulin@ifp.uiuc.edu).

I. INTRODUCTION

Information embedding refers to the embedding of data within a cover object (also referred to as *coverttext*) such as image, video, audio, graphics, text, or packet transmission times [1]–[5]. Applications include copyright protection, database annotation, transaction tracking, traitor tracing, timing channels, and multiuser communications. These applications often impose the requirement that embedding only slightly perturb the coverttext. The name *watermarking* has been widely used to describe information embedding techniques that are perceptually transparent, i.e., the marked object (after embedding) is perceptually similar to the cover object.

In some applications, the presence of the embedded information should be kept secret (see applications below). Then perceptual transparency is not sufficient, because statistical analysis could reveal the presence of hidden information. The problem of embedding information that is hard to detect is called *steganography*, and the marked object is called *stegotext* [3], [4], [6]–[8]. Steganography differs from cryptography in that the presence of the message needs to remain secret, rather than the value of the message. The dual problem to steganography is *steganalysis*, that is, detection of hidden information within a stegotext.

A famous model for steganography is Simmons’ prisoner problem [9]. Alice and Bob are locked up in different cells but are allowed to communicate under the vigilant eye of Willie, the prison warden. If Willie detects the presence of hidden information in the transmitted data, he terminates their communication and subjects them to a punishment. Willie is a *passive warden* if he merely observes and analyzes the transmitted data. He is an *active warden* if he introduces noise to make Alice and Bob’s task more difficult. In the information age, there are several application scenarios for steganography.

- 1) Steganography may be used to communicate over public networks such as the Internet. One may embed bits into inconspicuous files that are routinely sent over such networks: images, video, audio files, etc. Users of such technology may include intelligence and military personnel, people that are subject to censorship, and more generally, people who have a need for privacy.
- 2) Steganography may also be used to communicate over private networks. For instance, confidential documents within a commercial or governmental organization could be marked with identifiers that are hard to detect. The purpose is to trace unauthorized use of a document to a particular person who received a copy of this document. The recipient of the marked documents should not be aware of the presence of these identifiers.
- 3) Timing channels can be used to leak out information about computers. A pirate could modify the timing of packets sent by the computer, encoding data that reside on that computer. The pirate wishes to make this information leakage undetectable to avoid arousing suspicion. To disrupt potential information leakage, the network could jam packet timings — hence the network plays the role of an active warden.

The channel over which the stegotext is transmitted could be noiseless or noisy, corresponding to the case of a passive and an active warden, respectively. Moreover, the steganographer’s ability to choose the coverttext is often limited if not altogether nonexistent. In the private-network application above, the coverttext is generated by a content provider, not by the steganographer (i.e., the authority responsible for document security). Similarly in the

timing-channel application, the coverttext is generated by the computer, not by the pirate.

In view of these applications, the four basic attributes of a steganographic code are:

- 1) **detectability**: quantifying Willie's ability to detect the presence of hidden information;
- 2) **transparency (fidelity)**: closeness of coverttext and stegotext under an appropriate distortion (fidelity) metric;
- 3) **payload**: the number of bits embedded in the coverttext; and
- 4) **robustness**: quantifying decoding reliability in presence of channel noise (i.e., when Willie is an active warden).

If Alice had complete freedom for choosing the coverttext, the transparency requirement would be immaterial. A coverttext would not even be needed: it would suffice for Alice to generate objects that follow a prescribed coverttext distribution. This model has two shortcomings: (a) as mentioned above, in some applications Alice has little or no control over the choice of the coverttext; (b) even if she has, coverttexts have complicated distributions, and generating a size- M steganographic code by sampling the coverttext distribution would be highly impractical for large M . Information theory is a natural framework for studying steganography and steganalysis. Assuming a statistical model is available for coverttexts, the only truly secure strategy from the steganographer's point of view is to ensure that the probability distributions of the coverttext and stegotext are *identical*. This strong notion of security was proposed by Cachin [10] and is the steganographic counterpart of Shannon's notion of perfect security in cryptography. We refer to steganography that satisfies this strong property as *perfectly secure*.

If Alice is allowed to select the coverttext and Willie is passive, Alice may use the following perfectly secure steganographic code [10]. Alice and Bob agree on a hash function, and the value of the hashed stegotext is the message to be transmitted. Alice searches a database of coverttexts until she finds one that matches the desired hash value. This approach is perfectly secure irrespective of the distribution of the coverttext. The disadvantages are that the search is computationally infeasible for large message sets (communication rate is extremely low), and the underlying communication model is limited, as discussed above.

Cachin also proposed two less stringent requirements for steganographic codes [10]. One is ϵ -secure steganographic codes, where the Kullback-Leibler divergence between the coverttext and stegotext probability distributions is smaller than ϵ (perfect security requires $\epsilon = 0$). For random processes he redefined perfectly secure steganography by requiring that the above Kullback-Leibler divergence, normalized by the length N of the coverttext sequence, tends to zero as $N \rightarrow \infty$. Unfortunately this does not preclude the possibility that Kullback-Leibler divergence remains bounded away from zero, even grows to infinity (at a rate slower than N) as $N \rightarrow \infty$. If such is the case, Willie's error probability tends to zero asymptotically, and therefore the perfect-security terminology is misleading.

While Cachin focused on security and not on communication performance in terms of payload, robustness and fidelity, Kullback-Leibler divergence has become a popular metric for assessing the security of practical steganographic schemes subject to transparency, payload, and robustness requirements [11]–[18].

Many algorithms have been developed for steganography and steganalysis in recent years (see, e.g., [1], [6], [10]–[29] and references therein). For example, steganographic methods based on modification of least significant bits of digital photographs were popular in the early years of image steganography, because the embedding rate

is high (1 bit/sample) and the embedding is invisible to the human eye. These methods however fail to preserve the statistics of natural images, and thus cannot survive well-designed steganalysis tests [13], [24], [26]. Various improvements have been proposed (e.g., match first-order statistics) and broken soon after (e.g., test for mismatches in second-order statistics), prompting new rounds of improvements.

The tradeoffs between detectability, fidelity, payload, and robustness can be studied in an information-theoretic framework. The basic mathematical model for steganography is communications with side information at the encoder [30]. Moulin and O’Sullivan studied a general information-theoretic framework for information hiding and indicated its applicability to steganography [31, Section VII.C]. However, they did not study perfectly secure steganography and did not derive expressions for steganographic capacity. Galand and Kabatiansky [29] constructed steganographic binary codes, but the code rate vanishes as $\frac{\log N}{N}$. Fridrich *et al.* [27], [28] proposed positive-rate “wet paper” codes, which permit a change from the original cover distribution to a new stegodistribution. However they did not analyze the fundamental tradeoffs between payload, robustness, and detectability.

The goal of this paper is therefore to study the information-theoretic limits of *perfectly undetectable* steganography. As a first step towards this problem, we assume that coverttext samples are independently and identically distributed (i.i.d.) over a finite alphabet. In practice the i.i.d. model could be applied to transform coefficients or to blocks of coefficients. While this is just a simplifying approximation to actual statistics, it allows us to derive tangible mathematical results and to understand the effects of the perfect security constraint on transparency, payload, and robustness. Our first result is a connection between public watermarking codes [31]–[33] and perfectly secure steganographic codes. Given any public watermarking code that preserves the *first-order statistics* of the coverttext (this property will be referred to as *order-1 security*), we show that a perfectly secure steganographic code with the same error probability can be constructed using randomization over the set of all permutations of $\{1, 2, \dots, N\}$. We use this result to derive capacity and random-coding exponent formulas for perfectly secure steganography.

The codes that achieve capacity and random-coding exponents are stacked-binning schemes as proposed in [34] for general problems of channel coding with side information. The random-coding exponent yields an asymptotic upper bound on achievable error probability. A stacked-binning code consists of a stack of variable-size codeword arrays indexed by the type of the coverttext sequence, and the corresponding decoder is a maximum penalized mutual information (MPMI) decoder. The analysis is based on the method of types [35], [36].

Due to the added perfect-security constraint, capacity and random-coding exponent for steganography cannot exceed those of the corresponding public watermarking problem. Nevertheless, we have identified a class of problems where the coverttext probability mass function (PMF) is uniform and the distortion function is symmetric, with the property that the perfect undetectability constraint does not cause any capacity loss. One special example in the general class is the case of Bernoulli($\frac{1}{2}$) coverttexts with the Hamming distortion metric [37]. For the binary-Hamming case, the perfect security condition has no effect on both the capacity and random-coding error exponent. Steganographic capacity is achieved by randomized nested linear codes.

This paper is organized as follows. Section II describes our notation, and Section III the problem statement. In Section IV we show how perfectly secure steganographic codes can be constructed from codes with the much weaker

order-1 security. Section V presents our main theorems on capacity and random-coding error exponent. Section VI discusses the role of secret keys in steganographic codes; simplified results for the no-attack case are stated in Section VII; a class of steganography problems for which perfect security comes at no cost is studied in Section VIII; as an example of the above class, the binary-Hamming problem is studied in Section IX. Generalizations and applications of our basic problem setup are studied in Section X. The paper concludes with discussion in Section XI.

II. NOTATION

We use uppercase letters for random variables, lowercase letters for their individual values, and boldface letters for sequences. The PMF of a random variable $X \in \mathcal{X}$ is denoted by $p_X = \{p_X(x), x \in \mathcal{X}\}$. The entropy of a random variable X is denoted by $H(X)$, and the mutual information between two random variables X and Y is denoted by $I(X; Y) = H(X) - H(X|Y)$. Should the dependency on the underlying PMFs be explicit, we use the PMFs as subscripts, e.g., $H_{p_X}(X)$ and $I_{p_X, p_{Y|X}}(X; Y)$. The Kullback-Leibler divergence between two PMFs p and q is denoted by $D(p||q)$; the conditional Kullback-Leibler divergence of $p_{Y|X}$ and $q_{Y|X}$ given p_X is denoted by $D(p_{Y|X}||q_{Y|X}|p_X) = D(p_{Y|X} p_X || q_{Y|X} p_X)$.

Let $p_{\mathbf{x}}$ denote the empirical PMF on \mathcal{X} induced by a sequence $\mathbf{x} \in \mathcal{X}^N$. Then $p_{\mathbf{x}}$ is called the type of \mathbf{x} . The type class $T_{\mathbf{x}}$ associated with $p_{\mathbf{x}}$ is the set of all sequences of type $p_{\mathbf{x}}$. Likewise, we define the joint type $p_{\mathbf{xy}}$ of a pair of sequences $(\mathbf{x}, \mathbf{y}) \in \mathcal{X}^N \times \mathcal{Y}^N$ and the type class $T_{\mathbf{xy}}$ associated with $p_{\mathbf{xy}}$. The conditional type $p_{\mathbf{y}|\mathbf{x}}$ of a pair of sequences (\mathbf{x}, \mathbf{y}) is defined as $\frac{p_{\mathbf{xy}}(x, y)}{p_{\mathbf{x}}(x)}$ for all $x \in \mathcal{X}$ such that $p_{\mathbf{x}}(x) > 0$. The conditional type class $T_{\mathbf{y}|\mathbf{x}}$ given \mathbf{x} is the set of all sequences $\tilde{\mathbf{y}}$ such that $(\mathbf{x}, \tilde{\mathbf{y}}) \in T_{\mathbf{xy}}$. We denote by $H(\mathbf{x})$ the empirical entropy for \mathbf{x} , i.e., the entropy of the empirical PMF $p_{\mathbf{x}}$. Similarly, we denote by $I(\mathbf{x}; \mathbf{y})$ the empirical mutual information for the joint PMF $p_{\mathbf{xy}}$. The above notation for types is adopted from Csiszár and Körner [35].

We let $\mathbb{U}(\Omega)$ denote the uniform PMF over a finite set Ω . We let $\mathcal{P}_{\mathcal{X}}$ and $\mathcal{P}_{\mathcal{X}}^N$ represent the set of all PMFs and all empirical PMFs, respectively, on the alphabet \mathcal{X} . Likewise, $\mathcal{P}_{\mathcal{Y}|X}$ and $\mathcal{P}_{\mathcal{Y}|X}^N$ denote the set of all conditional PMFs and all empirical conditional PMFs on the alphabet \mathcal{Y} . We use \mathbb{E} to denote mathematical expectation.

The shorthands $a_N \doteq b_N$, $a_N \dot{\leq} b_N$, and $a_N \dot{\geq} b_N$ are used to denote asymptotic equalities and inequalities in the exponential scale for $\lim_{N \rightarrow \infty} \frac{1}{N} \log \frac{a_N}{b_N} = 0$, $\limsup_{N \rightarrow \infty} \frac{1}{N} \log \frac{a_N}{b_N} \leq 0$, and $\liminf_{N \rightarrow \infty} \frac{1}{N} \log \frac{a_N}{b_N} \geq 0$, respectively. We define $|t|^+ \triangleq \max(t, 0)$, $\exp_2(t) \triangleq 2^t$, and the binary entropy function

$$h(t) \triangleq -t \log t - (1-t) \log(1-t), \quad t \in [0, 1].$$

We use $\ln x$ to denote the natural logarithm of x , and the logarithm $\log x$ is in base 2 if not specified otherwise. The notation $\mathbb{1}_{\{A\}}$ is the indicator function of the event A :

$$\mathbb{1}_{\{A\}} = \begin{cases} 1 & A \text{ is true;} \\ 0 & \text{else.} \end{cases}$$

Finally, we adopt the notional convention that the minimum (resp. maximum) of a function over an empty set is $+\infty$ (resp. 0).

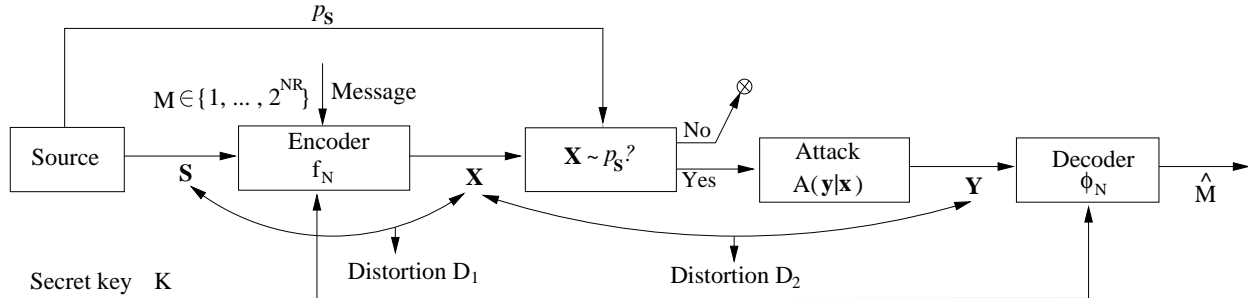


Fig. 1: Communication-theoretic view of perfectly secure steganography.

III. PROBLEM STATEMENT

Referring to Fig. 1, the covertext is modelled as a sequence $\mathbf{S} = (S_1, \dots, S_N)$ of i.i.d. samples drawn from a PMF $\{p_S(s), s \in \mathcal{S}\}$. A message M is to be embedded in \mathbf{S} and transmitted to a decoder; M is uniformly distributed over a message set \mathcal{M} . The encoder produces a stegotext \mathbf{X} through a function $f_N(\mathbf{S}, M)$, in an attempt to transmit the message M to the decoder reliably. The covertext and stegotext are required to be close according to some distortion metric.

A steganalyzer observes \mathbf{X} and tests whether \mathbf{X} is drawn i.i.d. from p_S . If not, the steganalyzer terminates the transmission, and obviously the decoder is unable to retrieve M . If \mathbf{X} is deemed innocuous, it is simply forwarded to the decoder in the no-attack or passive-warden case. An alternative is for the steganalyzer to produce a corrupted text \mathbf{Y} by passing \mathbf{X} through some attack channel $p_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x})$ (also called the active-warden case). In the latter case, the corrupted text and the stegotext are also required to be close according to some distortion metric. Clearly, \mathcal{X} and \mathcal{Y} , the alphabet sets for X and Y , respectively, should be the same as \mathcal{S} in order not to arouse apparent suspicion of hiding and attacking.

The decoder does not know $p_{\mathbf{Y}|\mathbf{X}}$ selected by the steganalyzer and does not have access to the original covertext \mathbf{S} . The decoder produces an estimate $\hat{M} = \phi_N(\mathbf{Y}) \in \mathcal{M}$ of the transmitted message. We assume that the encoder/decoder pair (f_N, ϕ_N) is *randomized*, i.e., the choice of (f_N, ϕ_N) is a function of a random variable known only to the encoder and decoder but not to the steganalyzer. We can think of this random variable as a *secret key* as in [31]–[33]. Note that in generic information-hiding games, this secret key provides some protection against adversaries with arbitrary memory and unlimited computational resources [4, Section X]. In steganography, the secret key plays a fundamental role in ensuring perfect undetectability: the covertext and the stegotext have the same PMF when the secret key is carefully designed. The randomized code will be denoted by (F_N, Φ_N) with a joint distribution $p(f_N, \phi_N)$.

A. Steganographic Codes

A distortion function is any nonnegative function $d : \mathcal{S} \times \mathcal{S} \rightarrow \mathbb{R}^+ \cup \{0\}$. This definition is extended to length- N vectors using $d^N(\mathbf{s}, \mathbf{x}) = \frac{1}{N} \sum_{i=1}^N d(s_i, x_i)$. Let $D_{\max} = \max_{s,x} d(s, x)$. We assume without loss of generality that $d(s, x) \geq 0$, with equality if $s = x$.

Definition 1: A length- N **perfectly secure steganographic code** with maximum distortion D_1 is a triple $(\mathcal{M}, F_N, \Phi_N)$, where

- \mathcal{M} is the message set of cardinality $|\mathcal{M}|$;
- (F_N, Φ_N) has a joint distribution $p(f_N, \phi_N)$;
- $f_N : \mathcal{S}^N \times \mathcal{M} \rightarrow \mathcal{S}^N$ maps covertext \mathbf{s} and message m to stegotext $\mathbf{x} = f_N(\mathbf{s}, m)$. The mapping is subject to the maximum distortion constraint

$$d^N(\mathbf{s}, f_N(\mathbf{s}, m)) \leq D_1 \text{ almost surely} \quad (1)$$

and the **perfect undetectability** constraint

$$p_{\mathbf{x}} = p_{\mathcal{S}}; \quad (2)$$

- $\phi_N : \mathcal{S}^N \rightarrow \mathcal{M}$ maps the received sequence \mathbf{y} to a decoded message $\hat{m} = \phi_N(\mathbf{y})$.

The above definition is similar to the definitions for a length- N data-embedding or watermarking code in [31]–[33], with the additional steganographic constraint of (2) which requires perfect matching of N -dimensional distributions. Also observe that the distortion constraint is inactive if $D_1 \geq D_{\max}$, i.e., the covertext \mathbf{S} available to Alice plays no role. Given $p_{\mathcal{S}}$, define the set of conditional PMFs $p_{X|S}$ such that the marginals of $p_S p_{X|S}$ are equal ($p_X = p_S$) and the expected distortion between S and X does not exceed D_1 :

$$\mathcal{Q}_1^{Steg}(p_S, D_1) \triangleq \left\{ p_{X|S} : \sum_{s,x} p_{X|S}(x|s) p_S(s) d(s, x) \leq D_1, \quad p_X(x) = \sum_s p_{X|S}(x|s) p_S(s) = p_S(x), \forall x \in \mathcal{S} \right\}. \quad (3)$$

Next, we define CCC and RM codes which will be used to construct perfectly secure steganographic codes.

Definition 2: (CCC Code). A length- N code with **conditionally constant composition**, **order-1 steganographic property**, and **maximum distortion** D_1 is a quadruple $(\mathcal{M}, \Lambda, F_N, \Phi_N)$, where Λ is a mapping from $\mathcal{P}_{\mathcal{S}}^{[N]}$ to $\mathcal{P}_{\mathcal{X}|\mathcal{S}}^{[N]}$. The transmitted sequence $\mathbf{x} = f_N(\mathbf{s}, m)$ has conditional type $p_{\mathbf{x}|\mathbf{s}} = \Lambda(p_{\mathbf{s}})$. Moreover, $\Lambda(p_{\mathbf{s}}) \in \mathcal{Q}_1^{Steg}(p_{\mathbf{s}}, D_1)$.

Observe that such a code matches the first-order empirical marginal PMF of the covertext, but not necessarily higher-order empirical marginals. Hence such a code generally does not satisfy the perfect-undetectability property.

Definition 3: (RM Code). A length- N **randomly modulated** code is the randomized code defined via permutations of a prototype (f_N, ϕ_N) :

$$\mathbf{x} = f_N^\pi(\mathbf{s}, m) \triangleq \pi^{-1} f_N(\pi \mathbf{s}, m) \quad (4)$$

$$\phi_N^\pi(\mathbf{y}) \triangleq \phi_N(\pi \mathbf{y}), \quad (5)$$

where π is drawn uniformly from the set Π of all $N!$ permutations and is not revealed to Willie. The sequence $\pi \mathbf{x}$ is obtained by applying π to the elements of \mathbf{x} .

Definition 4: Given alphabets \mathcal{S} and \mathcal{U} , a **steganographic channel** $p_{XU|S}(x, u|s)$ subject to distortion D_1 is a conditional PMF whose conditional marginal $p_{X|S}$ belongs to $\mathcal{Q}_1^{Steg}(p_S, D_1)$ of (3). We denote by $\mathcal{Q}^{Steg}(L, p_S, D_1)$ the set of steganographic channels subject to distortion D_1 when the alphabet \mathcal{U} has cardinality L .

If the channel $p_{XU|S}$ satisfies the distortion constraint D_1 but not necessarily the steganographic constraint $p_X = p_S$, $p_{XU|S}$ is simply a covert channel in the sense of [31], [32]. We shall denote by $\mathcal{Q}(L, p_S, D_1)$ the set of all such covert channels. Clearly, $\mathcal{Q}^{Steg}(L, p_S, D_1) \subseteq \mathcal{Q}(L, p_S, D_1)$.

B. Attack Channels

A passive warden simply produces $\mathbf{Y} = \mathbf{X}$. An active warden passes \mathbf{X} through a discrete memoryless channel (DMC), producing a degraded sequence \mathbf{Y} .

Definition 5: A discrete memoryless attack channel $p_{Y|X}$ is feasible if the expected distortion between X and Y is at most D_2 :

$$\sum_{x,y} p_X(x) p_{Y|X}(y|x) d(x, y) \leq D_2. \quad (6)$$

Then the joint conditional PMF is given by

$$p_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}) = \prod_{i=1}^N p_{Y|X}(y_i|x_i).$$

We denote by

$$\mathcal{A}(p_X, D_2) = \left\{ p_{Y|X} \in \mathcal{P}_{Y|X} : \sum_{x,y} p_X(x) p_{Y|X}(y|x) d(x, y) \leq D_2 \right\}$$

the set of all such feasible DMCs. This set is a compound DMC family.

As an alternative to Def. 5, one may consider attack channels that have arbitrary memory but are subject to an almost sure distortion constraint [32]–[34]. In this case, the set of feasible attack channels is given by

$$\mathcal{A}'(p_{\mathbf{x}}, D_2) = \left\{ p_{\mathbf{Y}|\mathbf{X}} \in \mathcal{P}_{\mathbf{Y}|\mathbf{X}}^N : Pr [d^N(\mathbf{y}, \mathbf{x}) \leq D_2] = 1 \right\}.$$

There are three reasons why only memoryless channels are considered in this paper. First, it is shown in [34] that for watermarking problems, both DMCs with expected distortion and arbitrary memory attack channels with almost sure distortion result in the same capacity formula, and the former allows a smaller random-coding error exponent when D_2 is the same. Thus, in terms of minimizing the random-coding exponent, selecting $p_{Y|X}$ from the compound DMC class $\mathcal{A}(p_X, D_2)$ is a better strategy for the warden than selecting $p_{\mathbf{Y}|\mathbf{X}}$ from $\mathcal{A}'(p_{\mathbf{x}}, D_2)$. Second, the assumption of memorylessness simplifies the presentation of main ideas. Finally, note that the proofs for the compound DMC provide the basis for the proofs in the case of channels with arbitrary memory [33], [34].

C. Steganographic Capacity and Reliability Function

The average probability of error for a randomized code (F_N, Φ_N) under a channel $p_{\mathbf{Y}|\mathbf{X}}$ is given by

$$P_{e,N}(F_N, \Phi_N, p_{\mathbf{Y}|\mathbf{X}}) = Pr(\hat{M} \neq M), \quad (7)$$

where the average is over all possible covertexts \mathbf{S} and messages M .

Definition 6: A rate R is achievable if there exists a randomized code (F_N, Φ_N) such that $|\mathcal{M}| \geq 2^{NR}$ and

$$\sup_{p_{\mathbf{Y}|\mathbf{X}}} P_{e,N}(F_N, \Phi_N, p_{\mathbf{Y}|\mathbf{X}}) \rightarrow 0 \quad \text{as } N \rightarrow \infty. \quad (8)$$

Definition 7: The steganographic capacity $C^{Steg}(D_1, D_2)$ is the supremum of all achievable rates.

Definition 8: The steganographic reliability function $E^{Steg}(R)$ is defined as

$$E^{Steg}(R) = \liminf_{N \rightarrow \infty} \left[-\frac{1}{N} \log \inf_{F_N, \Phi_N} \sup_{p_{\mathbf{Y}|\mathbf{X}}} P_{e,N}(F_N, \Phi_N, p_{\mathbf{Y}|\mathbf{X}}) \right]. \quad (9)$$

IV. FROM ORDER-1 TO PERFECTLY SECURE STEGANOGRAPHIC CODES

Codes with conditionally constant composition (Def. 2) and randomly modulated codes (Def. 3) play a central role in our code constructions and coding theorems. The following proposition suggests a general construction for perfectly secure steganographic codes: first select some deterministic prototype f_N with the CCC and order-1 steganographic properties and maximum distortion D_1 (Def. 2), second construct a RM code from that prototype. In Section V we show that this strategy is an optimal one.

Proposition 1: Let $(\mathcal{M}, F_N, \Phi_N)$ be a RM code whose prototype (f_N, ϕ_N) has conditionally constant composition, order-1 security, and maximum distortion D_1 . Then $(\mathcal{M}, F_N, \Phi_N)$ is a perfectly secure steganographic code with maximum distortion D_1 and same error probability as the prototype (f_N, ϕ_N) .

Proof: First we verify the perfect security condition. For RM codes (Def. 3), we have

$$p_{\mathbf{X}|\pi, \mathbf{S}, M}(\mathbf{x}|\pi, \mathbf{s}, m) = \mathbb{1}_{\{\pi\mathbf{x} = f_N(\pi\mathbf{s}, m)\}}.$$

Also note that for any $\mathbf{x}, \mathbf{z} \in T_{\mathbf{s}}$, there exists a permutation π_0 such that $\mathbf{x} = \pi_0\mathbf{z}$. Hence the value of the sum $\sum_{\pi} \mathbb{1}_{\{\pi\mathbf{x} = \mathbf{z}\}}$ is independent of \mathbf{z} (conditioned on $\mathbf{z} \in T_{\mathbf{s}}$), and so

$$\sum_{\pi} \mathbb{1}_{\{\pi\mathbf{x} = \mathbf{z}\}} = \frac{1}{|T_{\mathbf{s}}|} \sum_{\mathbf{z} \in T_{\mathbf{s}}} \sum_{\pi} \mathbb{1}_{\{\pi\mathbf{x} = \mathbf{z}\}} = \frac{1}{|T_{\mathbf{s}}|} \sum_{\pi} 1 = \frac{N!}{|T_{\mathbf{s}}|}. \quad (10)$$

Hence for any type class $T_{\mathbf{s}}$ we have

$$\begin{aligned} p_{\mathbf{X}|T_{\mathbf{s}}}(\mathbf{x}|T_{\mathbf{s}}) &= \frac{1}{N!} \sum_{\pi} \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \frac{1}{|T_{\mathbf{s}}|} \sum_{\mathbf{s}' \in T_{\mathbf{s}}} p_{\mathbf{X}|\pi, \mathbf{S}, M}(\mathbf{x}|\pi, \mathbf{s}', m) \\ &= \frac{1}{N!} \sum_{\pi} \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \frac{1}{|T_{\mathbf{s}}|} \sum_{\mathbf{s}' \in T_{\mathbf{s}}} \mathbb{1}_{\{\pi\mathbf{x} = f_N(\pi\mathbf{s}', m)\}} \\ &\stackrel{(a)}{=} \frac{1}{N!} \sum_{\pi} \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \frac{1}{|T_{\mathbf{s}}|} \sum_{\mathbf{s}'' \in T_{\mathbf{s}}} \mathbb{1}_{\{\pi\mathbf{x} = f_N(\mathbf{s}'', m)\}} \\ &= \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \frac{1}{|T_{\mathbf{s}}|} \sum_{\mathbf{s}'' \in T_{\mathbf{s}}} \frac{1}{N!} \sum_{\pi} \mathbb{1}_{\{\pi\mathbf{x} = f_N(\mathbf{s}'', m)\}} \\ &\stackrel{(b)}{=} \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \frac{1}{|T_{\mathbf{s}}|} \sum_{\mathbf{s}'' \in T_{\mathbf{s}}} \frac{1}{|T_{\mathbf{s}}|} \mathbb{1}_{\{\mathbf{x} \in T_{\mathbf{s}}\}} \end{aligned}$$

$$= \frac{1}{|T_{\mathbf{s}}|} \mathbb{1}_{\{\mathbf{x} \in T_{\mathbf{s}}\}}, \quad (11)$$

where in (a) we have made the change of variables $\mathbf{s}'' = \pi \mathbf{s}'$, and in (b) we have used (10) with $\mathbf{z} = f_N(\mathbf{s}'', m)$.

From (11) we obtain

$$p_{\mathbf{X}}(\mathbf{x}) = \sum_{T_{\mathbf{s}}} p_{\mathbf{S}}(T_{\mathbf{s}}) p_{\mathbf{X}|T_{\mathbf{s}}}(\mathbf{x}|T_{\mathbf{s}}) = \sum_{T_{\mathbf{s}}} p_{\mathbf{S}}(T_{\mathbf{s}}) \frac{1}{|T_{\mathbf{s}}|} \mathbb{1}_{\{\mathbf{x} \in T_{\mathbf{s}}\}} = p_{\mathbf{S}}(\mathbf{x}), \quad \forall \mathbf{x} \in \mathcal{S}^N,$$

hence the perfect security condition (2) is satisfied.

Now verifying the maximum-distortion constraint (1), for every π we have

$$d^N(\mathbf{s}, f_N^\pi(\mathbf{s}, m)) \stackrel{(a)}{=} d^N(\mathbf{s}, \pi^{-1} f_N(\pi \mathbf{s}, m)) \stackrel{(b)}{=} d^N(\pi \mathbf{s}, f_N(\pi \mathbf{s}, m)) \stackrel{(c)}{\leq} D_1$$

where (a) uses the definition of f_N^π in (4), (b) holds because the distortion measure is additive, and (c) holds because of our initial assumption on the prototype f_N . Therefore (1) holds.

Finally, let us evaluate the error probability for the RM code. Since the covert text source and the attack channel are memoryless, we have

$$p_S^N(\mathbf{s}) = p_S^N(\pi \mathbf{s}) \quad \text{and} \quad p_{Y|X}^N(\mathbf{y}|\mathbf{x}) = p_{Y|X}^N(\pi \mathbf{y}|\pi \mathbf{x}) \quad (12)$$

for any permutation π . The error probability for the prototype code takes the form

$$P_{e,N}(f_N, \phi_N, p_{Y|X}) = \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \sum_{\mathbf{s} \in \mathcal{S}^N} p_S^N(\mathbf{s}) \sum_{\mathbf{x} \in \mathcal{S}^N} \mathbb{1}_{\{\mathbf{x} = f_N(\mathbf{s}, m)\}} \sum_{\mathbf{y} \in \mathcal{S}^N} p_{Y|X}^N(\mathbf{y}|\mathbf{x}) \mathbb{1}_{\{\phi_N(\mathbf{y}) \neq m\}}.$$

For the prototype code modulated with permutation π , we have

$$\begin{aligned} P_{e,N}(f_N^\pi, \phi_N^\pi, p_{Y|X}) &= \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \sum_{\mathbf{s} \in \mathcal{S}^N} p_S^N(\mathbf{s}) \sum_{\mathbf{x} \in \mathcal{S}^N} \mathbb{1}_{\{\pi \mathbf{x} = f_N(\pi \mathbf{s}, m)\}} \sum_{\mathbf{y} \in \mathcal{S}^N} p_{Y|X}^N(\mathbf{y}|\mathbf{x}) \mathbb{1}_{\{\phi_N(\pi \mathbf{y}) \neq m\}} \\ &\stackrel{(a)}{=} \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \sum_{\mathbf{s} \in \mathcal{S}^N} p_S^N(\pi \mathbf{s}) \sum_{\mathbf{x} \in \mathcal{S}^N} \mathbb{1}_{\{\pi \mathbf{x} = f_N(\pi \mathbf{s}, m)\}} \sum_{\mathbf{y} \in \mathcal{S}^N} p_{Y|X}^N(\pi \mathbf{y}|\pi \mathbf{x}) \mathbb{1}_{\{\phi_N(\pi \mathbf{y}) \neq m\}} \\ &\stackrel{(b)}{=} \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \sum_{\pi^{-1} \mathbf{s}' \in \mathcal{S}^N} p_S^N(\mathbf{s}') \sum_{\pi^{-1} \mathbf{x}' \in \mathcal{S}^N} \mathbb{1}_{\{\mathbf{x}' = f_N(\mathbf{s}', m)\}} \sum_{\pi^{-1} \mathbf{y}' \in \mathcal{S}^N} p_{Y|X}^N(\mathbf{y}'|\mathbf{x}') \mathbb{1}_{\{\phi_N(\mathbf{y}') \neq m\}} \\ &\stackrel{(c)}{=} \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \sum_{\mathbf{s}' \in \mathcal{S}^N} p_S^N(\mathbf{s}') \sum_{\mathbf{x}' \in \mathcal{S}^N} \mathbb{1}_{\{\mathbf{x}' = f_N(\mathbf{s}', m)\}} \sum_{\mathbf{y}' \in \mathcal{S}^N} p_{Y|X}^N(\mathbf{y}'|\mathbf{x}') \mathbb{1}_{\{\phi_N(\mathbf{y}') \neq m\}} \\ &= P_{e,N}(f_N, \phi_N, p_{Y|X}), \end{aligned} \quad (13)$$

where (a) holds because of (12), (b) is obtained using the change in variables $\mathbf{s}' = \pi \mathbf{s}$, $\mathbf{x}' = \pi \mathbf{x}$, $\mathbf{y}' = \pi \mathbf{y}$, and (c) holds because the three sums run over all elements $(\mathbf{s}', \mathbf{x}', \mathbf{y}')$ of $\mathcal{S}^N \times \mathcal{S}^N \times \mathcal{S}^N$, and so the order of summation is inconsequential. Since (13) holds for every permutation π , the error probability for the RM code is equal to

$$P_{e,N}(F_N, \Phi_N, p_{Y|X}) = \frac{1}{N!} \sum_{\pi} P_{e,N}(f_N^\pi, \phi_N^\pi, p_{Y|X}) = P_{e,N}(f_N, \phi_N, p_{Y|X}).$$

This completes the proof. ■

V. STEGANOGRAPHIC CAPACITY AND RANDOM CODING ERROR EXPONENT

The steganographic codes in our achievability proofs are randomly-modulated binning codes with conditionally constant composition. The existence of a good deterministic prototype is established using a random coding argument. An arbitrarily large integer L is selected, defining an alphabet $\mathcal{U} = \{1, 2, \dots, L\}$ for the auxiliary random variable U in the binning construction. Given the covertext s and the message m , the encoder selects an appropriate sequence \mathbf{u} in the binning code and then generates the stegotext randomly according to the uniform distribution over an optimized type class $T_{\mathbf{x}|\mathbf{u},s}$. Proofs of the theorem and propositions in this section appear in Appendices I-III.

The following difference between two mutual informations:

$$J_L(p_S, p_{XU|S}, p_{Y|XUS}) \triangleq I(U; Y) - I(U; S) \quad (14)$$

plays a fundamental role in the analysis.

Theorem 1: Under Def. 1 for steganographic codes and Def. 5 for the compound attack channel, steganographic capacity is given by

$$C^{Steg}(D_1, D_2) = \lim_{L \rightarrow \infty} C_L^{Steg}(D_1, D_2), \quad (15)$$

where

$$C_L^{Steg}(D_1, D_2) \triangleq \max_{p_{XU|S} \in \mathcal{Q}^{Steg}(L, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} J_L(p_S, p_{XU|S}, p_{Y|X}) \quad (16)$$

and $(U, S) \rightarrow X \rightarrow Y$ forms a Markov chain.

The proof of Theorem 1 is given in two parts. The converse part is proved in Appendix I. The direct part is a corollary of a stronger result stated in Proposition 2 below, which provides a lower bound on the achievable error exponent (hence an upper bound on the average probability of error).

Proposition 2: Under Def. 1 for steganographic codes and Def. 5 for the compound attack channel, the following random-coding error exponent is achievable:

$$E_r^{Steg}(R) = \lim_{L \rightarrow \infty} E_{r,L}^{Steg}(R), \quad (17)$$

where

$$E_{r,L}^{Steg}(R) \triangleq \min_{\tilde{p}_S \in \mathcal{P}_S} \max_{p_{XU|S} \in \mathcal{Q}^{Steg}(L, \tilde{p}_S, D_1)} \min_{\tilde{p}_{Y|XUS} \in \mathcal{P}_{Y|XUS}} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} \left[D(\tilde{p}_S p_{XU|S} \tilde{p}_{Y|XUS} \| p_S p_{XU|S} p_{Y|X}) + |J_L(\tilde{p}_S, p_{XU|S}, \tilde{p}_{Y|XUS}) - R|^+ \right]. \quad (18)$$

Moreover, $E_r^{Steg}(R) = 0$ if and only if $R \geq C^{Steg}$.

Remark 1: The capacity and error exponent formulas in (15)-(18) coincide with those for public watermarking [33], [34], the only difference being that here the maximization over $p_{XU|S}$ is subject to a steganographic constraint. Clearly $E_{r,L}^{Steg}(R) \leq E_{r,L}^{PubWM}(R)$ and $C^{Steg} \leq C^{PubWM}$.

Remark 2: The proof of Proposition 2 is given in Appendix II. Using a random binning technique, we first prove the existence of a prototype CCC code with order-1 steganographic property, maximum distortion D_1 , and error

exponent $E^{Steg}(R)$. The decoder is an MPMI decoder. The main steps in this part of the proof are similar to those in the proof of Theorem 3.2 in [34], with the additional order-1 steganographic constraint on the encoder. Then we apply Proposition 1 and conclude that random modulation of this prototype yields a perfectly-secure steganographic code with maximum distortion D_1 , and error exponent $E^{Steg}(R)$.

Remark 3. As mentioned earlier, the covertext plays no role in the special case $D_1 \geq D_{\max}$, and so Alice can generate \mathbf{X} independently of \mathbf{S} . The capacity formula (15) becomes simply

$$C^{Steg} = \min_{p_{Y|S} \in \mathcal{A}(p_S, D_2)} I(S; Y),$$

and the random-coding exponent is

$$E_r^{Steg}(R) = \min_{\tilde{p}_S} \min_{\tilde{p}_{Y|S} \in \mathcal{P}_{Y|S}} \min_{p_{Y|S} \in \mathcal{A}(p_S, D_2)} [D(\tilde{p}_{Y|S} \tilde{p}_S \| p_{Y|S} p_S) + |I_{\tilde{p}_S \tilde{p}_{Y|S}}(S; Y) - R|^+].$$

The binning codes are degenerate in this case; the expressions for capacity and random-coding exponents reduce to classical formulas for compound DMCs without side information [35] and are achieved using constant-composition codes. Further specializing this result to the case of a passive warden ($D_2 = 0$, hence $p_{Y|X} = \mathbb{1}_{\{Y=X\}}$), we obtain $C^{Steg} = H(S)$ and $E_r^{Steg}(R)$ is given by (29), see Section VII.

The operation of the prototype code is illustrated in Fig. 2. The codebook \mathcal{C} consists of a stack of codeword arrays indexed by the possible covertext sequence types. Given an input \mathbf{s} , the encoder evaluate its type $p_{\mathbf{s}}$ and selects the corresponding codeword array

$$\mathcal{C}(p_{\mathbf{s}}) = \{\mathbf{u}(l, m, p_{\mathbf{s}}), 1 \leq l \leq 2^{N\rho(p_{\mathbf{s}})}, 1 \leq m \leq |\mathcal{M}|\}, \quad (19)$$

in which the codewords are drawn from an optimized type class $T_{\mathbf{u}} \triangleq T_U^*(p_{\mathbf{s}})$. Each array $\mathcal{C}(p_{\mathbf{s}})$ has $|\mathcal{M}|$ columns and $2^{N\rho(p_{\mathbf{s}})}$ rows, where $\rho(p_{\mathbf{s}})$ is a function of the corresponding covertext type $p_{\mathbf{s}}$ and is termed the depth parameter of the array. Given \mathbf{y} , the decoder seeks a codeword in $\mathcal{C} = \bigcup_{p_{\mathbf{s}}} \mathcal{C}(p_{\mathbf{s}})$ that maximizes the penalized empirical mutual information and outputs its column index as the estimated message:

$$\hat{m} = \arg \max_m \max_{l, p_{\mathbf{s}}} [I(\mathbf{u}(l, m, p_{\mathbf{s}}); \mathbf{y}) - \rho(p_{\mathbf{s}})]. \quad (20)$$

By letting $\rho(p_{\mathbf{s}}) = I(\mathbf{u}; \mathbf{s}) + \epsilon$, where $T_{\mathbf{us}} \triangleq T_{US}^*(p_{\mathbf{s}})$ is an optimized joint type and ϵ is an arbitrarily small positive number, an optimal balance between the probability of encoding error and the probability of decoding error is achieved. The former vanishes double-exponentially while the latter vanishes at a rate given by the random coding error exponent in (18). The above MPMI decoder can be thought of as an empirical generalized maximum a posterior (MAP) decoder [34, Section 3.1].

VI. SECRET KEY

In standard information-hiding problems with a compound DMC attack channel, *deterministic* codes are enough to achieve capacity; random coding is used as a method of proof to establish the existence of a deterministic code without actually specifying the code [38]. In our steganography problem, a *randomized* code is used to satisfy the perfect-undetectability condition of (2). Without the secret key, a deterministic code generally could not satisfy the

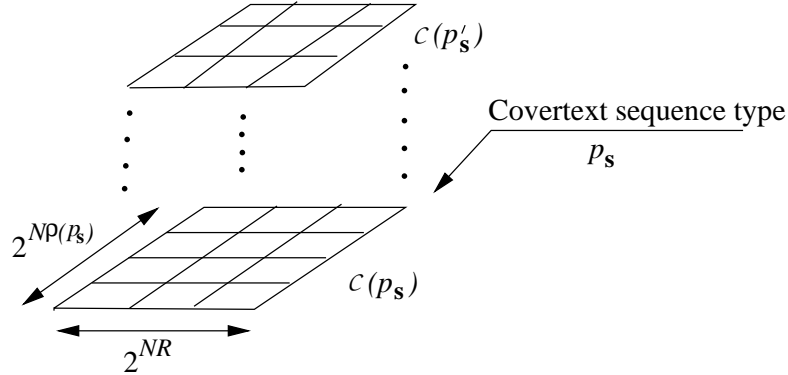


Fig. 2: A binning scheme with a stack of variable-size codeword arrays indexed by the covertext sequence type.

perfect-undetectability condition. Also note that a randomized code is generally needed if the attacks have arbitrary memory [32]–[34]. For example, in watermarking games, knowing a deterministic code the adversary would decode and remove the message; deterministic codes are vulnerable to this kind of “surgical attack” [4].

For randomized codes, the secret key shared between encoder and decoder is the source of common randomness. For RM codes, the secret key specifies the value of the permutation π . The entropy rate of the secret key is

$$H_K^{RM} = \frac{1}{N} \log_2 N! < \log_2 N. \quad (21)$$

VII. PASSIVE WARDEN

A passive warden introduces no degradation to the stegotext; in this case, $D_2 = 0$ and $Y = X$, i.e.,

$$p_{Y|X} = \mathbb{1}_{\{Y=X\}}. \quad (22)$$

This results in simplified expressions for the perfectly secure steganographic capacity in (15) and the random-coding error exponent in (17), see Propositions 3 and 4 below.

Proposition 3: For the passive-warden case ($D_2 = 0$), the maximization in (16) is achieved by $U = X$ and

$$C^{Steg}(D_1, 0) = \max_{p_{X|S} \in \mathcal{Q}_1^{Steg}(p_S, D_1)} H(X|S). \quad (23)$$

Proof: By (22), $J_L(p_S, p_{XU|S}, p_{Y|X})$ is reduced to

$$J_L(p_S, p_{XU|S}, p_{Y|X}) = I(U; X) - I(U; S).$$

Choosing $U = X$ yields the lower bound

$$\begin{aligned} C^{Steg}(D_1, 0) &\geq \max_{p_{X|S} \in \mathcal{Q}_1^{Steg}(p_S, D_1)} I(X; X) - I(X; S) \\ &= \max_{p_{X|S} \in \mathcal{Q}_1^{Steg}(p_S, D_1)} H(X|S). \end{aligned} \quad (24)$$

On the other hand,

$$\begin{aligned} J_L(p_S, p_{XU|S}, p_{Y|X}) &= I(U; X) - I(U; S) \\ &\leq I(U; X|S) \end{aligned} \quad (25)$$

$$\begin{aligned} &= H(X|S) - H(X|U, S) \\ &\leq H(X|S). \end{aligned} \quad (26)$$

Note that (25) follows from the chain rule of mutual information

$$I(U; XS) = I(U; X) + I(U; S|X) = I(U; S) + I(U; X|S)$$

and $I(U; S|X) \geq 0$. Choosing $U = X$ achieves equality in both (25) and (26).

From (26), we obtain

$$\begin{aligned} C^{Steg}(D_1, 0) &= \lim_{L \rightarrow \infty} \max_{p_{XU|S} \in \mathcal{Q}^{Steg}(L, p_S, D_1)} J_L(p_S, p_{XU|S}, p_{Y|X}) \\ &\leq \lim_{L \rightarrow \infty} \max_{p_{XU|S} \in \mathcal{Q}^{Steg}(L, p_S, D_1)} H(X|S) \\ &= \max_{p_{X|S} \in \mathcal{Q}^{Steg}(p_S, D_1)} H(X|S). \end{aligned} \quad (27)$$

Combining (24) and (27) yields (23) and proves the proposition. \blacksquare

Remark. Since $H(X|S) = H(X) - I(S; X) = H(S) - I(S; X)$, we have

$$C^{Steg}(D_1, 0) = H(S) - \min_{p_{X|S} \in \mathcal{Q}^{Steg}(p_S, D_1)} I(S; X).$$

For the problem of encoding a source S subject to distortion D_1 , the minimum rate for representing the source is given by the rate-distortion function

$$R_S(D_1) = \min_{p_{X|S} : \text{Ed}(S, X) \leq D_1} I(S; X) \leq \min_{p_{X|S} \in \mathcal{Q}_1^{Steg}(p_S, D_1)} I(S; X)$$

where the inequality holds because $p_{X|S} \in \mathcal{Q}_1^{Steg}(p_S, D_1)$ implies $\text{Ed}(S, X) \leq D_1$. Hence

$$C^{Steg}(D_1, 0) \leq H(S) - R_S(D_1) \quad (28)$$

and the capacity-achieving codes for the passive-warden case are analogous to rate-distortion codes. Equality holds in (28) if the distribution that achieves the rate-distortion bound satisfies the steganographic property $p_X = p_S$.

Proposition 4: For the passive-warden case ($D_2 = 0$), the random-coding exponent is given by

$$E_r^{Steg}(R) = \min_{\tilde{p}_S \in \mathcal{P}_S} \max_{p_{X|S} \in \mathcal{Q}_1^{Steg}(\tilde{p}_S, D_1)} \left[D(\tilde{p}_S || p_S) + |H_{\tilde{p}_S, p_{X|S}}(X|S) - R|^+ \right]. \quad (29)$$

Proof: Since $p_{Y|X} = \mathbb{1}_{\{Y=X\}}$, the term $D(\tilde{p}_S p_{XU|S} \tilde{p}_{Y|XUS} || p_S p_{XU|S} p_{Y|X})$ in (18) is infinite if $\tilde{p}_{Y|XUS} \neq p_{Y|X}$. Hence, the minimizing $\tilde{p}_{Y|XUS}$ in (18) is given by

$$\tilde{p}_{Y|XUS}^* = p_{Y|X} = \mathbb{1}_{\{Y=X\}}.$$

Consequently, the two terms of the cost function of (18) are reduced to

$$D(\tilde{p}_S p_{XU|S} \tilde{p}_{Y|XUS}^* || p_S p_{XU|S} p_{Y|X}) = D(\tilde{p}_S || p_S)$$

and

$$\left| J_L(\tilde{p}_S, p_{XU|S}, \tilde{p}_{Y|XUS}^*) - R \right|^+ = \left| J_L(\tilde{p}_S, p_{XU|S}, p_{Y|X}) - R \right|^+,$$

respectively. This yields

$$E_r^{Steg}(R) = \min_{\tilde{p}_S \in \mathcal{P}_S} \left[D(\tilde{p}_S || p_S) + \lim_{L \rightarrow \infty} \max_{p_{XU|S} \in \mathcal{Q}^{Steg}(L, \tilde{p}_S, D_1)} \left| J_L(\tilde{p}_S, p_{XU|S}, p_{Y|X}) - R \right|^+ \right]. \quad (30)$$

Similarly to the steps in the proof of Proposition 3, we derive that

$$\forall L \geq 2 : \max_{p_{XU|S} \in \mathcal{Q}^{Steg}(L, \tilde{p}_S, D_1)} \left| J_L(\tilde{p}_S, p_{XU|S}, p_{Y|X}) - R \right|^+ = \max_{p_{X|S} \in \mathcal{Q}_1^{Steg}(p_S, D_1)} |H_{\tilde{p}_S, p_{X|S}}(X|S) - R|^+. \quad (31)$$

The maximum on the left side is achieved by $U = X$. Combining (30) and (31) proves the proposition. \blacksquare

VIII. PENALTY FOR PERFECT SECURITY

The capacity expressions for public watermarking in [31], [33] and for steganography in (15) take the same form, except that here the maximization of $p_{XU|S}$ is subject to the steganographic constraint. Consequently, we have

$$C^{Steg} \leq C^{PubWM} \quad (32)$$

and similarly

$$E_r^{Steg}(R) \leq E_r^{PubWM}(R). \quad (33)$$

For some special cases, it is possible that the optimal covert channel for public watermarking automatically satisfies the perfect security condition, and (32) and (33) hold with equality. Proposition 5 below states sufficient conditions on the covertext PMF p_S and the distortion function $d(\cdot, \cdot)$ that ensure the perfect security constraint causes no penalty in communication performance.

We consider $\mathcal{S} = \mathbb{Z}_q = \{0, 1, 2, \dots, q-1\}$, which is a group under addition modulo q . We shall use the notation $\underline{k} \triangleq k \bmod q$. The covertext S is uniformly distributed over \mathbb{Z}_q , i.e.,

$$p_S = \mathbb{U}(\mathcal{S}).$$

The associated distortion function $d : \mathcal{S} \times \mathcal{S} \rightarrow \mathbb{R}^+ \cup \{0\}$ satisfies

$$d(i, i) = 0 \text{ and } d(i, j) = d(0, \underline{j-i}),$$

If we write $\{d(i, j)\}_{i, j=0}^{q-1}$ in a matrix form, the distortion matrix is cyclic-Toeplitz.

Definition 9: Let $\mathcal{V} \triangleq \{0, 1, \dots, L-1\}$, $p_S = \mathbb{U}(\mathcal{S})$, and $\mathcal{U} \triangleq \{0, 1, 2, \dots, qL-1\}$. Given any covert channel $p_{XV|S} \in \mathcal{Q}(L, p_S, D_1)$, where $v \in \mathcal{V}$, we define an associated covert channel $p_{XU|S} \in \mathcal{P}_{XU|S}$, where $U \in \mathcal{U}$, by

$$p_{XU|S}(x, qv + i | s) = \frac{1}{q} p_{XV|S}(\underline{x-i}, v | \underline{s-i}), \quad \forall v \in \mathcal{V}, \forall i, s, x \in \mathcal{S}. \quad (34)$$

For any stochastic matrix $p_{XV|S} \in \mathcal{Q}(L, p_S, D_1)$, by (34), the new channel $p_{XU|S}$ contains all of its q cyclically shifted versions (with respect to X and S) and these shifted versions are equally likely. Since the distortion function is cyclic, it is easy to verify that

$$\mathbb{E}_{p_S, p_{XU|S}}[\mathbf{d}(S, X)] = \mathbb{E}_{p_S, p_{XV|S}}[\mathbf{d}(S, X)] \leq D_1.$$

Moreover, the marginal PMF \hat{p}_X induced by $p_S = \mathbb{U}(S)$ and $p_{XU|S}$ is given by

$$\hat{p}_X(x) = \frac{1}{q} \sum_{i=0}^{q-1} p_X(x-i) = \frac{1}{q} \equiv p_S(x), \quad \forall x \in \mathcal{S}, \quad (35)$$

where p_X is the marginal PMF induced by $p_S = \mathbb{U}(S)$ and $p_{XV|S} \in \mathcal{Q}(L, p_S, D_1)$. That is,

$$p_{XU|S} \in \mathcal{Q}^{Steg}(qL, p_S, D_1).$$

Definition 10: The class $\mathcal{Q}_{cyc}^{Steg}(qL, p_S, D_1)$ is the set of all such $p_{XU|S}$ defined in (34).

Clearly, we have

$$\mathcal{Q}_{cyc}^{Steg}(qL, p_S, D_1) \subset \mathcal{Q}^{Steg}(qL, p_S, D_1) \subset \mathcal{Q}(qL, p_S, D_1). \quad (36)$$

Definition 11: The class of cyclic attack channels subject to distortion D_2 is defined as

$$\begin{aligned} \mathcal{A}_{cyc}(D_2) \triangleq & \left\{ p_{Y|X} \in \mathcal{P}_{Y|X} : p_{Y|X}(y|x) = p_{Y|X}(y-x|0), \quad \forall x, y \in \mathcal{S}, \right. \\ & \left. \text{and } \frac{1}{q} \sum_{y=0}^{q-1} p_{Y|X}(y|0) \mathbf{d}(y, 0) \leq D_2 \right\}. \end{aligned} \quad (37)$$

Any stochastic matrix $p_{Y|X} \in \mathcal{A}_{cyc}(D_2)$ is cyclic-Toeplitz. Also note that for any $p_X \in \mathcal{P}_X$,

$$\mathcal{A}_{cyc}(D_2) \subset \mathcal{A}(p_X, D_2). \quad (38)$$

Proposition 5: For the above q -ary information-hiding problem, the capacities for both the perfectly secure steganography game and the public watermarking game are the same. That is, the perfect security constraint in (2) does not cause any capacity loss. Moreover, there is no loss of optimality in restricting the maximization in (16) to $\mathcal{Q}_{cyc}^{Steg}(qL, p_S, D_1)$ and the minimization to $\mathcal{A}_{cyc}(D_2)$:

$$\begin{aligned} C^{PubWM}(D_1, D_2) &= C^{Steg}(D_1, D_2) \\ &= \lim_{L \rightarrow \infty} \max_{p_{XU|S} \in \mathcal{Q}_{cyc}^{Steg}(qL, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}_{cyc}(D_2)} J_L(p_S, p_{XU|S}, p_{Y|X}). \end{aligned} \quad (39)$$

The proof is given in Appendix III.

IX. EXAMPLE: BINARY-HAMMING CASE

We illustrate the above results through the following example, where $\mathcal{S} = \{0, 1\}$, and the covertext is Bernoulli($\frac{1}{2}$) sequence, i.e.,

$$Pr[S = 1] = Pr[S = 0] = \frac{1}{2}.$$

The Hamming distortion metric is used: $\mathbf{d}(x, y) = \mathbb{1}_{\{x \neq y\}}$.

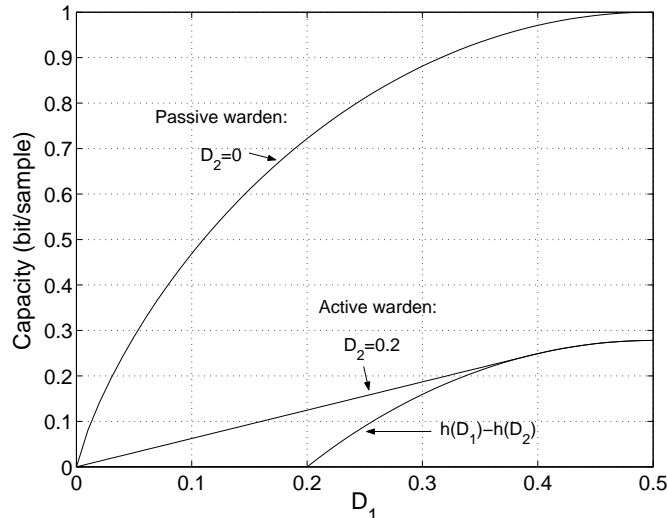


Fig. 3: Capacity for a perfectly secure steganography game when the covertext \mathbf{S} is a Bernoulli($\frac{1}{2}$) sequence.

A. Capacity

The capacity in the public watermarking game setting is given in [34] as follows

$$C = \begin{cases} \frac{D_1}{d_{D_2}}[h(d_{D_2}) - h(D_2)], & \text{if } 0 \leq D_1 \leq d_{D_2}; \\ h(D_1) - h(D_2), & \text{if } d_{D_2} \leq D_1 \leq 1/2; \\ 1 - h(D_2), & \text{if } D_1 > 1/2, \end{cases} \quad (40)$$

where $d_{D_2} = 1 - 2^{-h(D_2)}$. When $D_2 = 0$,

$$C = \begin{cases} h(D_1) & \text{if } 0 \leq D_1 \leq 1/2; \\ 1 & \text{if } D_1 \geq 1/2. \end{cases} \quad (41)$$

Fig. 3 shows the above two capacity functions.

The optimal attack channel is a binary symmetric channel (BSC) with crossover probability D_2 . If $d_{D_2} \leq D_1 \leq 1/2$, the optimal covert channel is also a binary symmetric channel: BSC(D_1) (i.e., $|\mathcal{U}| = 2$, $U = X$, and $p_{XU|S} = p_{X|S}$); otherwise, the capacity is achieved by time sharing: no embedding on a fraction of $1 - \frac{D_1}{d_{D_2}}$ samples and embedding with the optimal covert channel BSC(d_{D_2}) on the rest of samples. Since the covertext \mathbf{S} is a Bernoulli($\frac{1}{2}$) sequence, the output of the above optimal BSC(p) covert channel is also Bernoulli($\frac{1}{2}$). That is, the optimal covert channel for the public watermarking game satisfies $p_X = p_S$, and the perfect security constraint does not cause any loss in capacity, as stated by Proposition 5.

B. Random-Coding Exponent

In [34], we numerically computed the random-coding exponent for public watermarking in the case of $D_1 = 0.4$, $D_2 = 0.2$, and $|\mathcal{U}| = 2$ as shown in Fig. 4. We found that the optimal covert channel is still a BSC(D_1) ($p_{XU|S} =$

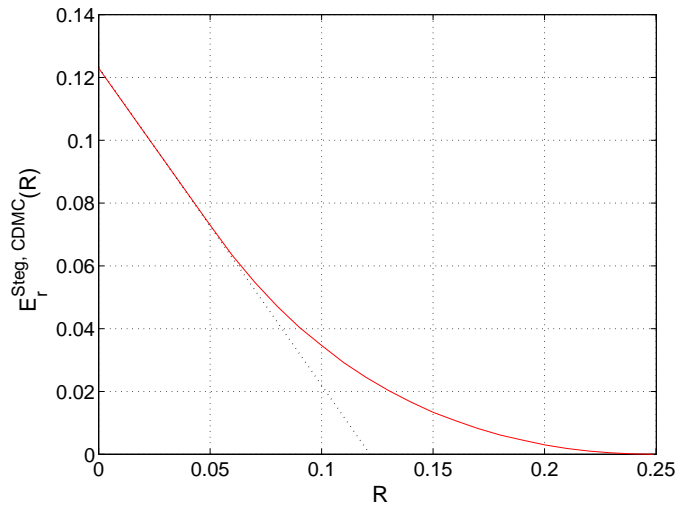


Fig. 4: Random-coding exponent for perfectly secure steganography game when the covertext \mathbf{S} is a Bernoulli($\frac{1}{2}$) sequence, $D_1 = 0.4$, $D_2 = 0.2$, and $|\mathcal{U}| = 2$.

$p_{X|S}$) with the time sharing strategy. It implies that at least for the case of $|\mathcal{U}| = 2$, $p_X = p_S$ and the perfect security constraint causes no loss in random-coding exponent either.

C. Randomized Nested Linear Codes—A Capacity-Achieving Code Construction

For information-embedding problems with a fixed attack channel $\text{BSC}(D_2)$, *deterministic* nested binary linear codes were proposed to realize capacity, where \mathcal{C}_1 , a good source code with Hamming distance D_1 , is nested in \mathcal{C}_2 , a good channel code over $\text{BSC}(D_2)$ [39], [40]. When $|\mathcal{C}_2| \doteq 2^{N[1-h(D_2)]}$ and $|\mathcal{C}_1| \doteq 2^{N[1-h(D_1)]}$, the asymptotic code rate

$$R = \lim_{N \rightarrow \infty} \frac{1}{N} \log_2 \frac{|\mathcal{C}_2|}{|\mathcal{C}_1|} = h(D_1) - h(D_2)$$

is equal to the capacity for the no-time-sharing scenario; otherwise, the time-sharing strategy described in (40) is applied. The same nested linear codes work for the watermarking scenario as well since $\text{BSC}(D_2)$ is the optimal discrete memoryless attack channel. By this coding scheme, the transmitted stegotext codewords are uniformly distributed over the fine code \mathcal{C}_2 [39], [40]. Clearly, unless $D_2 = 0$, the fine code \mathcal{C}_2 is only a subset of the whole space $\mathbb{F}_2^N \triangleq \{0, 1\}^N$.

Randomization via the secret key plays an important role in achieving perfect security. Specifically, the random secret key makes the transmitted stegotext uniformly distributed over \mathbb{F}_2^N , and so this construction results in *randomized* nested binary linear codes.

We partition the whole space \mathbb{F}_2^N into a disjoint union of \mathcal{C}_2 and its cosets:

$$\mathbb{F}_2^N = \bigcup_{\mathbf{c} \in \Omega_2} \mathcal{C}_2 \oplus \mathbf{c}, \quad (42)$$

where $\mathcal{C}_2 \oplus \mathbf{c}$ is a coset of \mathcal{C}_2 , the element $\mathbf{c} \in \Omega_2$ is a coset leader, and the set Ω_2 contains all coset leaders. Clearly,

$$|\Omega_2| = \frac{2^N}{|\mathcal{C}_2|} \doteq 2^{Nh(D_2)}. \quad (43)$$

Let the secret key \mathbf{K} be uniformly distributed over Ω_2 . For any $\mathbf{k} \in \Omega_2$, the randomized encoder output is given by

$$\mathbf{x} = f_N^{\mathbf{k}}(m, \mathbf{s}) = f_N^0(m, \mathbf{s} \oplus \mathbf{k}) \oplus \mathbf{k}, \quad (44)$$

where $f_N^0(\cdot, \cdot)$ is the deterministic encoder used for the information-embedding or watermarking problem. The decoding function is

$$\hat{m} = \phi_N^{\mathbf{k}}(\mathbf{y}) = \phi_N^0(\mathbf{y} \oplus \mathbf{k}), \quad (45)$$

where $\phi_N^0(\cdot)$ is the corresponding deterministic decoder.

Since the output of the deterministic encoder is uniformly distributed over \mathcal{C}_2 and the secret key \mathbf{K} is uniformly distributed over Ω_2 , the output of the randomized encoder of (44) is uniformly distributed over \mathbb{F}_2^N by (42). Hence perfect security is achieved, and by (43) the entropy rate of the secret key is $h(D_2)$, which is lower than $\log_2 N$ required for general RM codes in (21).

For the passive-warden case ($D_2 = 0$), we simply let \mathcal{C}_2 be \mathbb{F}_2^N , and perfect security is achieved even without a secret key.

X. GENERALIZATIONS AND APPLICATIONS

It is interesting to note that perfect security is achieved using randomization via permutations in general, but that randomization via coset shifts is sufficient for the nested linear codes of Section IX-C. This suggests taking a more abstract view of the problem, which unifies both problems above, and is applicable to more general settings – e.g., covertexts with memory and covertexts defined over continuous alphabets.

A. Invariant Signal, Distortion, and Channel Representations

Consider a fairly general covertext distribution $p_{\mathbf{S}}$ which admits an invariant group \mathcal{G} , such that

$$p_{\mathbf{S}}(\mathbf{s}) = p_{\mathbf{S}}(g\mathbf{s}) \quad \forall \mathbf{s} \in \mathcal{S}^N, g \in \mathcal{G}.$$

Decompose the covertext space as

$$\mathcal{S}^N = \cup_{v \in \mathcal{V}} T_v,$$

where each subset T_v is \mathcal{G} -invariant, i.e.,

$$gT_v = T_v \quad \forall v \in \mathcal{V}, g \in \mathcal{G},$$

and T_v is the orbit of any of its elements under the group action:

$$T_v = \{g\mathbf{s}, g \in \mathcal{G}\}, \quad \forall \mathbf{s} \in T_v.$$

We shall assume that the cardinality of \mathcal{V} is subexponential in N . Given an element s of T_v , we write $p_s^{\mathcal{G}}$ and $T_s^{\mathcal{G}}$ to designate v and T_v , respectively. We refer to $p_s^{\mathcal{G}}$ and $T_s^{\mathcal{G}}$ as the \mathcal{G} -type and the \mathcal{G} -type class associated with s . We denote by $\mathcal{P}_S^{[N, \mathcal{G}]}$ the set of all \mathcal{G} -types for sequences defined over \mathcal{S}^N . All these notions coincide with the usual type notions when the source \mathbf{S} is i.i.d. over a finite alphabet and $\mathcal{G} = \Pi$, the group of permutations of $\{1, 2, \dots, N\}$.

It is easy to extend this formalism to pairs of sequences. Given two sequences \mathbf{s}, \mathbf{x} , we define their joint \mathcal{G} -type class $T_{\mathbf{xy}}^{\mathcal{G}}$ as the orbit of (\mathbf{x}, \mathbf{y}) under the group action, and the conditional \mathcal{G} -type class $T_{\mathbf{y}|\mathbf{x}}^{\mathcal{G}}$ as the set of sequences \mathbf{y}' such that $T_{\mathbf{xy}'}^{\mathcal{G}} = T_{\mathbf{xy}}^{\mathcal{G}}$. We denote by $p_{\mathbf{xy}}^{\mathcal{G}}$ and $p_{\mathbf{y}|\mathbf{x}}^{\mathcal{G}}$ the corresponding joint \mathcal{G} -type and conditional \mathcal{G} -type and by $\mathcal{P}_{XY}^{[N, \mathcal{G}]}$ and $\mathcal{P}_{Y|X}^{[N, \mathcal{G}]}$ the set of all joint \mathcal{G} -types and conditional \mathcal{G} -types, respectively, for pairs of sequences over $\mathcal{X}^N \times \mathcal{Y}^N$.

Next, assume the distortion function d^N is \mathcal{G} -invariant, that is,

$$d^N(g\mathbf{s}, g\mathbf{x}) = d^N(\mathbf{s}, \mathbf{x}) \quad \forall g \in \mathcal{G}, \mathbf{s}, \mathbf{x} \in \mathcal{S}^N.$$

Also assume the attack channel $p_{\mathbf{Y}|\mathbf{X}}$ is \mathcal{G} -invariant, i.e.,

$$p_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}) = p_{\mathbf{Y}|\mathbf{X}}(g\mathbf{y}|g\mathbf{x}) \quad \forall g \in \mathcal{G}, \mathbf{x}, \mathbf{y} \in \mathcal{S}^N.$$

Next we define CCC(\mathcal{G}) and RM(\mathcal{G}) codes, analogously to Definitions 2 and 3.

Definition 12: (CCC(\mathcal{G}) code). A length- N code with conditionally constant composition with respect to \mathcal{G} , order-1 steganographic property, and maximum distortion D_1 is a quadruple $(\mathcal{M}, \Lambda, F_N, \Phi_N)$, where Λ is a mapping from $\mathcal{P}_S^{[N, \mathcal{G}]}$ to $\mathcal{P}_{X|S}^{[N, \mathcal{G}]}$. The transmitted sequence $\mathbf{x} = f_N(\mathbf{s}, m)$ has conditional \mathcal{G} -type $p_{\mathbf{x}|\mathbf{s}}^{\mathcal{G}} = \Lambda(p_s^{\mathcal{G}})$. Moreover, $\Lambda(p_s^{\mathcal{G}}) \in \mathcal{Q}^{Steg}(p_s^{\mathcal{G}}, D_1)$.

Definition 13: (RM(\mathcal{G}) code). A length- N randomly modulated code over \mathcal{G} is the randomized code defined by applying group element g to a prototype (f_N, ϕ_N) :

$$\begin{aligned} f_N^g(\mathbf{s}, m) &= g^{-1} f_N(g\mathbf{s}, m) \\ \phi_N^g(\mathbf{y}) &= \phi_N(g\mathbf{y}), \end{aligned}$$

where g is drawn uniformly from \mathcal{G} and is not revealed to Willie.

Consider a length- N RM code over a subgroup \mathcal{G}^{sub} of \mathcal{G} . The entropy rate for the key is $H_K = \frac{1}{N} \log |\mathcal{G}^{sub}|$. We now ask when this randomized code is a perfectly secure steganographic code; the smaller the subgroup, the lower the key rate.

Proposition 6: Let (f_N, ϕ_N) be a CCC(\mathcal{G}) code with order-1 security and maximum distortion D_1 . There exists a subgroup \mathcal{G}^{sub} of \mathcal{G} such that the code (f_N, ϕ_N) randomized over \mathcal{G}^{sub} is a perfectly secure steganographic code with maximum distortion D_1 , and the same error probability as that for the prototype (f_N, ϕ_N) .

Proof: Choose $\mathcal{G}^{sub} = \mathcal{G}$. The derivations parallel those in the proof of Proposition 1, replacing permutations π with group elements g and types with \mathcal{G} -types. Thus (11) becomes $p(\mathbf{x}|T_s^{\mathcal{G}}) = \frac{1}{|T_s^{\mathcal{G}}|} \mathbb{1}_{\{\mathbf{x} \in T_s^{\mathcal{G}}\}}$, from which it follows that $p_{\mathbf{X}} = p_{\mathbf{S}}$, and the perfect-security condition holds. Checking the maximum-distortion condition, we

have

$$d^N(\mathbf{s}, f_N^g(\mathbf{s}, m)) = d^N(\mathbf{s}, g^{-1} f_N(g\mathbf{s}, m)) = d^N(g\mathbf{s}, f_N(g\mathbf{s}, m)) \leq D_1.$$

Similarly to (13), the error probability for the modulated code (f_N^g, ϕ_N^g) is identical to that of (f_N, ϕ_N) , hence

$$P_{e,N}(F_N, \Phi_N, p_{Y|X}) = \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} P_{e,N}(f_N^g, \phi_N^g, p_{Y|X}) = P_{e,N}(f_N, \phi_N, p_{Y|X}).$$

This completes the proof. \blacksquare

While we chose $\mathcal{G}^{sub} = \mathcal{G}$ to prove Proposition 6, in some cases the perfect security property can be achieved using a smaller subgroup. This is the case of the nested linear codes of Section IX-C: there $\mathcal{G} = \Pi$, but \mathcal{G}^{sub} is homomorphic to Ω_2 .

B. Coverttexts With Memory

As an application of Proposition 6, consider the class of order-1 Markov coverttext processes. Denote by W the $|\mathcal{S}| \times |\mathcal{S}|$ transition matrix for this process. The order-2 type of a sequence \mathbf{s} is the empirical PMF for the sequence of pairs $(s_i, s_{i+1}), 1 \leq i \leq N-1$ [36] and is denoted by $p_{\mathbf{s}}^{(2)}$ — a PMF over \mathcal{S}^2 . The order-2 type class $T_{\mathbf{s}}^{(2)}$ is the set of sequences that have the same order-2 type $p_{\mathbf{s}}^{(2)}$. Denoting by \mathcal{V} the collection of order-2 types (the cardinality of \mathcal{V} is polynomial in N), we observe that each order-2 type class is an invariant set for $p_{\mathbf{s}}$ and therefore also a \mathcal{G} -type class where \mathcal{G} is a subgroup of Π , the group of all permutations of $\{1, 2, \dots, N\}$.

Since \mathcal{G} is a subgroup of Π , any additive distortion function is \mathcal{G} -invariant, and any memoryless channel $p_{\mathbf{Y}|\mathbf{X}}$ is also \mathcal{G} -invariant. Moreover the output $\mathbf{x} = f_N(\mathbf{s}, m)$ of a CCC(\mathcal{G}) code has the property that \mathbf{x} belongs to a fixed conditional order-2 type class given \mathbf{s} , as m ranges over the message set. If the code has the order-1 security property, then the second-order types of \mathbf{s} and \mathbf{x} match.¹ By Proposition 6, randomization (over \mathcal{G}) of such a CCC(\mathcal{G}) code with order-1 security and maximum distortion D_1 yields a perfectly-secure steganographic code with maximum distortion D_1 and the same error probability as the prototype CCC(\mathcal{G}) code.

These notions can be naturally extended to Markov processes of order r . The r -th order type of a sequence \mathbf{s} is the empirical PMF for the r -uple $(s_i, s_{i+1}, \dots, s_{i+r}), 1 \leq i \leq N-r$, that is, an empirical PMF over \mathcal{S}^r [36]. For a Markov process of order r , the \mathcal{G} -types are $(r+1)$ -th order types, and perfectly secure steganographic codes can be constructed from CCC(\mathcal{G}) codes with order-1 security using randomization over \mathcal{G} .

C. Isotropic Coverttexts

Let the alphabet \mathcal{S} be the real line, \mathcal{G} the rotation group over \mathbb{R}^N and $d(\mathbf{s}, \mathbf{x}) = \|\mathbf{s} - \mathbf{x}\|^2$ the squared Euclidean distance. Assume the distribution of \mathbf{S} is isotropic – in particular, \mathbf{S} could be i.i.d. Gaussian. If $p_{\mathbf{S}}$ is isotropic, the invariant sets T_v are centered spheres with radius equal to v . Let the prototype (f_N, ϕ_N) be a nested lattice code in \mathbb{R}^N [39], where the encoder output is scaled so as to satisfy the order-1 security property:

$$\|\mathbf{x}\| = \|f_N(\mathbf{s}, m)\| = \|\mathbf{s}\| = v, \quad \forall \mathbf{s} \in T_v, \quad v \geq 0.$$

¹Recall that “order-1 security” just means that the \mathcal{G} -type of the coverttext sequence is preserved; for a Markov process, the \mathcal{G} -type happens to be a second-order type.

The code (f_N, ϕ_N) randomized over the full rotation group \mathcal{G} satisfies the perfect-security property of Proposition 6.

D. Signal Transformations

Assume the following generative model for the covertext: $\mathbf{S} = h\tilde{\mathbf{S}}$ is the output of an injective mapping h applied to a length- N i.i.d. sequence $\tilde{\mathbf{S}}$ with finite alphabet $\tilde{\mathcal{S}}$ and PMF $p_{\tilde{s}}$. Denote by h^{-1} the inverse mapping (from $h\tilde{\mathcal{S}}^N$ to $\tilde{\mathcal{S}}^N$). For a perfectly secure steganographic code, the stegotext must satisfy the same generative model: $\mathbf{X} = h\tilde{\mathbf{X}}$, where $\tilde{\mathbf{X}}$ is i.i.d. $p_{\tilde{s}}$. Assume the distortion function takes the form $d^N(\mathbf{s}, \mathbf{x}) = \tilde{d}^N(\tilde{\mathbf{s}}, \tilde{\mathbf{x}})$, where $\tilde{d} : \tilde{\mathcal{S}} \times \tilde{\mathcal{S}} \rightarrow \mathbb{R}^+ \cup \{0\}$. Clearly any perfectly secure steganographic code for $\tilde{\mathbf{X}}^N$ induces a perfectly secure steganographic code for \mathbf{X}^N .

Finally, assume that Willie extracts $\tilde{\mathbf{X}} = h^{-1}\mathbf{X}$, passes it through a discrete memoryless channel $p_{\tilde{Y}|\tilde{X}}$, and outputs $\mathbf{Y} = h\tilde{\mathbf{Y}}$:

$$p_{\mathbf{Y}|\mathbf{X}}(\mathbf{y}|\mathbf{x}) = p_{\tilde{Y}|\tilde{X}}^N(\tilde{\mathbf{y}}|\tilde{\mathbf{x}}) \quad \text{where} \quad \mathbf{y} = h\tilde{\mathbf{y}}, \mathbf{x} = h\tilde{\mathbf{x}}.$$

Owing to this channel model, by application of Proposition 1 we conclude that a perfectly secure steganographic code for $\tilde{\mathbf{X}}^N$ can be constructed by randomized modulation of a prototype CCC code with order-1 security, and that the error probability of the randomized code is equal to that of the prototype code.

This generative model has a few interesting applications.

- *Filtered Processes.* Assume that \mathcal{S} is a finite field and \mathbf{S} is given by

$$S_i = (h\tilde{\mathbf{S}})_i \triangleq \sum_{j \geq 0} h_j \tilde{S}_{i-j \bmod N}, \quad 1 \leq i \leq N,$$

(circular convolution) where $\tilde{\mathcal{S}}$ is a subfield of \mathcal{S} , and h is an invertible filter with coefficients in \mathcal{S} . Since the samples \tilde{S}_i , $1 \leq i \leq N$, are i.i.d., the inverse filter h^{-1} may be viewed as a whitening filter. Moreover, if \tilde{S} is uniformly distributed over $\tilde{\mathcal{S}} = \{0, 1\}$ and $\tilde{d}(\cdot, \cdot)$ is Hamming distance, the desired perfectly secure steganographic code can be obtained using the randomized nested lattice construction of Section IV.

- *Timing Channels.* Let S_i , $i \in \mathbb{N}$, be a temporal point process with i.i.d. interarrival times $S_i - S_{i-1} = \tilde{S}_i$ for $1 \leq i \leq N$. This could be a simplified model for the timing of packets sent out by a computer. A pirate can modify the timing, resulting in a new time sequence X_i , $i \in \mathbb{N}$, that contains the stolen data. To make this information leakage perfectly undetectable, the distribution of the sequence \mathbf{X} should be the same as that of \mathbf{S} — hence the pirate needs a perfectly secure steganographic code. He may do so using the technique proposed in this section. Giles and Hajek [5] showed that the pirate can still reliably communicate even when the network tries to jam packet timings. It follows from our results that the pirate can communicate reliably at a positive rate, using perfectly secure steganographic codes.

E. Computational Security

This paper has focused on the interplay between communication performance and information-theoretic security, where security is achieved using a private key that is uniformly distributed over a group \mathcal{G}^{sub} . A more practical setup

would involve a public-key system, in which a reduced set of representers of \mathcal{G}^{sub} is selected, each corresponding to a value of the key. Assume the uniform distribution over this reduced set is computationally indistinguishable (in a sense to be precisely defined) from the uniform distribution over \mathcal{G}^{sub} . The resulting steganographic code is no longer perfectly secure but inherits the computational security of the key generation mechanism. Thus the framework analyzed in this paper can form the basis for constructing computationally secure steganographic codes that have near-optimal communication performance.

XI. CONCLUSION

A strict definition of perfect security has been adopted in this paper, implying that even a warden with unlimited computational resources is unable to reliably detect the presence of a hidden message. We have studied the Shannon-theoretic limits of communication performance under this perfect-security requirement and studied the structure of codes that asymptotically achieve those limits. The main results are summarized below.

- Perfectly secure steganography is closely related to the public watermarking problem of [31], [34]. Positive capacity and random-coding exponents are achieved using stacked-binning codes and an MPMI decoder.
- Randomized codes are generally needed to achieve perfect security. The common randomness is provided by a secret key shared between the encoder and decoder. For i.i.d. covertexts, Proposition 1 shows that perfectly secure steganographic codes can be constructed using randomized permutations of a prototype CCC watermarking code that merely has an order-1 security property, i.e., the prototype code matches the first-order marginals of the covertext and stegotext, but not the full N -dimensional statistics.
- The cost of perfect security in terms of communication performance is the same as the cost of order-1 security. However, if the covertext distribution is uniform and the distortion metric is cyclically symmetric, the security constraint does not cause any loss of performance.
- A generalization of the basic framework has been proposed, in which the covertext process and the distortion function are invariant relative to a group \mathcal{G} . To this end we have introduced the notion of \mathcal{G} -types and constructed perfectly secure steganographic codes using randomization (over the group \mathcal{G}) of a prototype $\text{CCC}(\mathcal{G})$ watermarking code with order-1 security. Some applications of this framework have been proposed.

As indicated, our basic framework could be used to analyze complex problems involving covertexts with elaborate statistical dependencies, covertexts defined over continuous alphabets, and computational security. While such extensions are technically challenging, we hope that the mathematical structure of optimal codes identified in this paper under simplifying assumptions will shed some light on the development of practical codes with high communication performance.

APPENDIX I

CONVERSE PROOF OF THEOREM 1

The converse is an extension of the proof in [34, Section 7]. Our upper bound on achievable rates is derived by

- replacing the perfect-security constraint with a weaker order-1 security constraint on the encoder:

$$p_{\mathbf{x}} = p_{\mathbf{s}} \quad \forall m, \mathbf{s}, \mathbf{x} = f_N(\mathbf{s}, m) \quad (46)$$

(matching the types of input \mathbf{s} and output $\mathbf{x} = f_N(\mathbf{s}, m)$ of the encoder f_N),

- replacing the almost-sure distortion constraint with an expected distortion constraint on the encoder:

$$\frac{1}{|\mathcal{M}|} \sum_{\mathbf{s} \in \mathcal{S}^N} p_S^N(\mathbf{s}) d^N(\mathbf{s}, f_N(\mathbf{s}, m)), \quad (47)$$

- and providing the decoder with knowledge of the attack channel $p_{Y|X}$.

Clearly any upper bound we derive under these assumptions is an upper bound on capacity as well.

For any rate- R code (f_N, ϕ_N) and DMC $p_{Y|X} \in \mathcal{A}(p_X, D_2)$, we have

$$\begin{aligned} NR = H(M) &= H(M|\mathbf{Y}) + I(M; \mathbf{Y}) \\ &\leq 1 + P_e(f_N, \phi_N, p_{Y|X}^N) NR + I(M; \mathbf{Y}), \end{aligned}$$

where the inequality is due to Fano's inequality. In order for P_e not to be bounded away from 0, rate R needs to satisfy

$$NR - 1 \leq \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} I(M; \mathbf{Y}). \quad (48)$$

The joint PMF of $(M, \mathbf{S}, \mathbf{X}, \mathbf{Y})$ is given by

$$p_{M\mathbf{S}\mathbf{X}\mathbf{Y}|f_N} = p_M p_S^N p_{Y|X}^N \mathbf{1}_{\{\mathbf{x}=f_N(\mathbf{s}, M)\}}. \quad (49)$$

Owing to (49), for any $1 \leq i \leq N$, $(M, \mathbf{S}, \{Y_j\}_{j \neq i}) \rightarrow X_i \rightarrow Y_i$ forms a Markov chain and so does

$$(W_i, S_i) \rightarrow X_i \rightarrow Y_i, \quad (50)$$

where the random variable W_i is defined as

$$W_i = (M, S_{i+1}, \dots, S_N, Y_1, \dots, Y_{i-1}). \quad (51)$$

Using the same set of inequalities as in [30, Lemma 4], we obtain

$$I(M; \mathbf{Y}) \leq \sum_{i=1}^N [I(W_i; Y_i) - I(W_i; S_i)]. \quad (52)$$

We define a time sharing random variable T , which is uniformly distributed over $\{1, \dots, N\}$ and independent of all other random variables, and define the quadruple of random variables (W, S, X, Y) as (W_T, S_T, X_T, Y_T) . With this definition, the order-1 security constraint (46) becomes $p_X = p_S$, and the expected distortion constraint (47) becomes $\sum_{s,x} p_S(s) p_{X|S}(x|s) d(s, x) \leq D_1$. Therefore $p_{X|S} \in \mathcal{Q}_1^{\text{Ste}g}(p_S, D_1)$.

By (51), the random variable W is defined over an alphabet of cardinality $\exp_2 \{N [R + \log |S|]\}$. Moreover $(W, S) \rightarrow X \rightarrow Y$ forms a Markov chain. Combining (48) and (52), we further derive

$$\begin{aligned}
R &\leq \frac{1}{N} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} I(M; \mathbf{Y}) \\
&\leq \frac{1}{N} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} \sum_{i=1}^N [I(W_i; Y_i) - I(W_i; S_i)] \\
&= \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} [I(W; Y|T) - I(W; S|T)] \\
&= \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} [I(W, T; Y) - I(W, T; S) - I(T; Y) + I(T; S)] \\
&\leq \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} [I(U; Y) - I(U; S)], \tag{53}
\end{aligned}$$

where $U = (W, T)$ is defined over an alphabet of cardinality

$$L(N) = N \exp_2 \{N [R + \log |S|]\}, \tag{54}$$

and the last inequality is due to $I(T; Y) \geq 0$ and $I(T; S) = 0$ (since T is independent of S). Since $p_{X|S} \in \mathcal{Q}_1^{Steg}(p_S, D_1)$, we have $p_{XU|S} \in \mathcal{Q}^{Steg}(L(N), p_S, D_1)$.

Recall that $J_L(p_S, p_{XU|S}, p_{Y|X}) \triangleq I(U; Y) - I(U; S)$ when $|\mathcal{U}| = L$, and that

$$C_L^{Steg} \triangleq \max_{p_{XU|S} \in \mathcal{Q}^{Steg}(L, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} J_L(p_S, p_{XU|S}, p_{Y|X}).$$

Following the same arguments as in [34], the sequence C_L^{Steg} is nondecreasing and converges to a finite limit

$$C^{Steg} \triangleq \lim_{L \rightarrow \infty} C_L^{Steg} = \lim_{L \rightarrow \infty} \max_{p_{XU|S} \in \mathcal{Q}^{Steg}(L, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} J_L(p_S, p_{XU|S}, p_{Y|X}).$$

Therefore, continuing with (53), R is bounded by

$$\begin{aligned}
R &\leq \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} [I(U; Y) - I(U; S)] \\
&= \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} J_L(N)(p_X, p_{XU|S}, p_{Y|X}) \\
&\leq \sup_L \max_{p_{XU|S} \in \mathcal{Q}^{Steg}(L, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} J_L(p_S, p_{XU|S}, p_{Y|X}) \\
&= \lim_{L \rightarrow \infty} \max_{p_{XU|S} \in \mathcal{Q}^{Steg}(L, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} J_L(p_S, p_{XU|S}, p_{Y|X}) \\
&= C^{Steg}. \tag{55}
\end{aligned}$$

This proves the converse part of Theorem 1.

APPENDIX II

PROOF OF PROPOSITION 2

We have

$$E_{r,L}^{Steg}(R) \leq E_{r,L}^{PubWM}(R).$$

Recall from [34, Lemma 3.1] that the sequence $E_{r,L}^{PubWM}(R)$ is nondecreasing and converges to a finite limit $E_r^{PubWM}(R)$ as $L \rightarrow \infty$. Using the same arguments as in [34, Lemma 3.1], it follows that the sequence $E_{r,L}^{Steg}(R)$

is nondecreasing and converges to a finite limit $E_r^{Steg}(R)$ as $L \rightarrow \infty$. Hence for any $\epsilon > 0$ and R , there exists $L(\epsilon)$ such that

$$E_{r,L}^{Steg}(R) \geq E_r^{Steg}(R) - \epsilon, \quad \forall L \geq L(\epsilon).$$

We next prove that for any L , a sequence of *deterministic* codes (f_N, ϕ_N) with order-1 steganographic security exist with the property that

$$\lim_{N \rightarrow \infty} \left[-\frac{1}{N} \log \max_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} P_e(f_N, \phi_N, p_{Y|X}) \right] = E_{r,L}^{Steg}(R).$$

To prove the existence of such a code, we construct a random ensemble \mathcal{C} of binning codes (f_N, ϕ_N) with auxiliary alphabet $\mathcal{U} \triangleq \{1, 2, \dots, L\}$ and show that the error probability averaged over \mathcal{C} vanishes at rate $E_{r,L}^{Steg}(R)$ as N goes to infinity. The proof is based on that of [34, Theorem 3.2] with special treatment on the encoder construction for perfect security.

Assume that $R < C_L^{Steg} - \epsilon$. For any covertext type p_s and conditional type $p_{\mathbf{x}|\mathbf{s}}$, define the function

$$E_{L,N}(R, p_s, p_{\mathbf{x}|\mathbf{s}}) \triangleq \min_{p_{\mathbf{y}|\mathbf{x}\mathbf{s}}} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} \left[D(p_s p_{\mathbf{x}|\mathbf{s}} p_{\mathbf{y}|\mathbf{x}\mathbf{s}} \| p_s p_{\mathbf{x}|\mathbf{s}} p_{Y|X}) + |I(\mathbf{u}; \mathbf{y}) - I(\mathbf{u}; \mathbf{s}) - \epsilon - R|^+ \right]. \quad (56)$$

Define $\mathcal{Q}^{Steg}(N, L, p_s, D_1)$ as the set of conditional types $p_{\mathbf{x}|\mathbf{s}}$ that also belong to the set $\mathcal{Q}^{Steg}(L, p_s, D_1)$ of feasible steganographic channels. If $p_{\mathbf{x}|\mathbf{s}} \in \mathcal{Q}^{Steg}(N, L, p_s, D_1)$ then

- (1) $p_{\mathbf{x}} = p_s$, i.e., the stegotext sequence has the same type as the covertext sequence and the order-1 security condition is satisfied;
- (2) $d^N(\mathbf{x}, \mathbf{s}) \leq D_1$, i.e., distortion is no greater than D_1 for any choice of \mathbf{s} and m .

The set $\mathcal{Q}^{Steg}(N, L, p_s, D_1)$ includes $p_{\mathbf{x}|\mathbf{s}} = \mathbb{1}_{\{\mathbf{x}=\mathbf{s}\}}$ and is therefore nonempty.

Now denote by $p_{\mathbf{x}|\mathbf{s}}$ the maximizer of (56) over the set $\mathcal{Q}^{Steg}(N, L, p_s, D_1)$. As a result of this optimization, we may associate

- to any covertext type p_s , a type class $T_U^*(p_s) \triangleq T_{\mathbf{u}}$ and a mutual information $I_{US}^*(p_s) \triangleq I(\mathbf{u}; \mathbf{s})$;
- to any covertext sequence \mathbf{s} , a conditional type class $T_{U|S}^*(\mathbf{s}) \triangleq T_{\mathbf{u}|\mathbf{s}}$;
- to any sequences \mathbf{s} and $\mathbf{u} \in T_{US}^*(p_s)$, a conditional type class $T_{X|US}^*(\mathbf{u}, \mathbf{s}) \triangleq T_{\mathbf{x}|\mathbf{u}\mathbf{s}}$.

A random codebook \mathcal{C} is the union of codeword arrays $\mathcal{C}(p_s)$ indexed by the covertext sequence type p_s . Let $\rho(p_s) \triangleq I_{US}^*(p_s) + \epsilon$. The codeword array $\mathcal{C}(p_s)$ is obtained by drawing $2^{N(R+\rho(p_s))}$ random vectors independently and uniformly from the corresponding type class $T_U^*(p_s)$, and arranging them in an array with $2^{N\rho(p_s)}$ rows and 2^{NR} columns indexed by messages.

A. Encoder f_N

Given a codebook \mathcal{C} , a covertext sequence \mathbf{s} , and a message m , the encoder finds in $\mathcal{C}(p_s)$ an l such that $\mathbf{u}(l, m) \in T_{U|S}^*(\mathbf{s})$. If more than one such l exists, pick one of them randomly (with uniform distribution). Let $\mathbf{u} = \mathbf{u}(l, m)$. If no such l is available, the encoder declares an error and draws \mathbf{u} from the uniform distribution over

the conditional type class $T_{U|S}^*(\mathbf{s})$. Then \mathbf{x} is drawn from the uniform distribution over the conditional type class $T_{X|US}^*(\mathbf{u}, \mathbf{s})$. Recalling the discussion below (56), f_N satisfies both the order-1 steganographic security constraint and the maximum distortion constraint.

B. Decoder ϕ_N

Given \mathbf{y} and the same codebook \mathcal{C} used by the encoder, the decoder first seeks a covert text type p_s and $\hat{\mathbf{u}} \in \mathcal{C}(p_s)$ that maximizes the *penalized mutual information* criterion

$$\max_{p_s} \max_{\mathbf{u} \in \mathcal{C}(p_s)} [I(\mathbf{u}; \mathbf{y}) - \rho(p_s)]. \quad (57)$$

The decoder then outputs the column index \hat{m} that corresponds to $\hat{\mathbf{u}}$. If there exist maximizers with more than one column index, the decoder declares an error.

C. Error Probability Analysis

The probability of error is given by

$$P_{e,N} \triangleq \max_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} Pr(M \neq \hat{M}) = \max_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} P_e(f_N, \phi_N, p_{Y|X}).$$

Following the steps in [34, Section 5], the encoding error vanishes double-exponentially and only the decoding error contributes to $P_{e,N}$ on the exponential scale:

$$P_{e,N} \stackrel{\cdot}{\leq} \exp_2 \left\{ -N \min_{p_s} \max_{p_{\mathbf{x}|\mathbf{u}|\mathbf{s}}} E_{L,N}(R, p_s, p_{\mathbf{x}|\mathbf{u}|\mathbf{s}}) \right\}. \quad (58)$$

As $N \rightarrow \infty$, by [34, Lemma 2.2], the above error exponent converges to

$$E_{r,L}^{Steg}(R) = \min_{\tilde{p}_S \in \mathcal{P}_S} \max_{p_{XU|S} \in \mathcal{Q}^{Steg}(L, \tilde{p}_S, D_1)} \min_{\tilde{p}_{Y|XUS} \in \mathcal{P}_{Y|XUS}} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} \left[D(\tilde{p}_S p_{XU|S} \tilde{p}_{Y|XUS} \| p_S p_{XU|S} p_{Y|X}) + |J_L(\tilde{p}_S, p_{XU|S}, \tilde{p}_{Y|XUS}) - R|^+ \right]. \quad (59)$$

Clearly, $E_{r,L}^{Steg}(R) \geq 0$, with equality if and only if the following conditions are met:

- the minimizing PMF \tilde{p}_S is equal to p_S ;
- the minimizing conditional PMF $\tilde{p}_{Y|XUS}$ is equal to $p_{Y|X}$; and
- $R \geq \max_{p_{XU|S} \in \mathcal{Q}^{Steg}(L, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} J_L(p_S, p_{XU|S}, p_{Y|X}) = C_L^{Steg}$.

Therefore, $E_{r,L}^{Steg}(R) > 0$ and the error probability vanishes for any $R < C_L^{Steg}(D_1, D_2)$. This implies that the capacity is lower-bounded by

$$\lim_{L \rightarrow \infty} C_L^{Steg}(D_1, D_2).$$

D. Perfect Security

Having established the achievability of $E_{r,L}^{Steg}(R)$ and C_L^{Steg} for a deterministic code (f_N, ϕ_N) with order-1 security and maximum distortion D_1 , we invoke Proposition 1 to claim that the randomly modulated code with prototype (f_N, ϕ_N) achieves the same error probability (hence error exponent) and distortion as the prototype.

APPENDIX III
PROOF OF PROPOSITION 5

We prove Proposition 5 in two parts. We first establish that the right-hand side of (39) is an upper bound on the public watermarking capacity C^{PubWM} . Then we prove that the right-hand side of (39) is at the same time a lower bound on the perfectly secure steganographic capacity C^{Steg} .

We start with the following lemma on the properties of $p_{XU|S} \in \mathcal{Q}_{cyc}^{Steg}(qL, p_S, D_1)$, which are used throughout this proof.

Lemma 1: Any $p_{XU|S} \in \mathcal{Q}_{cyc}^{Steg}(qL, p_S, D_1)$ generated by (34) from its corresponding $p_{XV|S} \in \mathcal{Q}(L, p_S, D_1)$ has the following properties:

- (i) $p_{S|U}(s|qv + i) = p_{S|V}(\underline{s-i}|v)$, $\forall i, s \in \mathcal{S}$ and $\forall v \in \mathcal{V}$;
- (ii) $p_{X|U}(x|qv + i) = p_{X|V}(\underline{x-i}|v)$, $\forall i, x \in \mathcal{S}$ and $\forall v \in \mathcal{V}$;
- (iii) $p_U(qv + i) = \frac{1}{q}p_V(v)$, $\forall i \in \mathcal{S}$, $v \in \mathcal{V}$, where p_U (resp. p_V) is the marginal PMF of U (resp. V) induced from $p_{XU|S}$ (resp. $p_{XV|S}$) and $p_S = \mathbb{U}(\mathcal{S})$; and
- (iv) $\hat{p}_X = \mathbb{U}(\mathcal{S})$, where \hat{p}_X is the marginal PMF of X induced from $p_{XU|S}$ and $p_S = \mathbb{U}(\mathcal{S})$.

It is straightforward to verify Lemma 1(i)-(iv) from (34).

A. Upper Bound

For the capacity of the public watermarking game,

$$\begin{aligned} C^{PubWM}(D_1, D_2) &= \lim_{L \rightarrow \infty} \max_{p_{XV|S} \in \mathcal{Q}(L, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} J_L(p_S, p_{XV|S}, p_{Y|X}) \\ &\leq \lim_{L \rightarrow \infty} \max_{p_{XV|S} \in \mathcal{Q}(L, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}_{cyc}(D_2)} J_L(p_S, p_{XV|S}, p_{Y|X}), \end{aligned} \quad (60)$$

since $\mathcal{A}_{cyc}(D_2) \subset \mathcal{A}(p_X, D_2)$ by (38).

Given any $p_{XV|S} \in \mathcal{Q}(L, p_S, D_1)$ and its associated $p_{XU|S} \in \mathcal{Q}_{cyc}^{Steg}(qL, p_S, D_1)$, we first verify that

$$I(S; U) = I(S; V). \quad (61)$$

From $p_S = \mathbb{U}(\mathcal{S})$ and $p_{XV|S}$, we obtain

$$H(S|V) = - \sum_{v=0}^{L-1} p_V(v) \sum_{s=0}^{q-1} p_{S|V}(s|v) \log p_{S|V}(s|v). \quad (62)$$

From $p_S = \mathbb{U}(\mathcal{S})$ and $p_{XU|S}$, we have

$$\begin{aligned} H(S|U) &= - \sum_{v=0}^{L-1} \sum_{i=0}^{q-1} \sum_{s=0}^{q-1} p_U(qv + i) p_{S|U}(s|qv + i) \log p_{S|U}(s|qv + i) \\ &= - \sum_{v=0}^{L-1} \sum_{i=0}^{q-1} \sum_{s=0}^{q-1} \frac{1}{q} p_V(v) p_{S|V}(\underline{s-i}|v) \log p_{S|V}(\underline{s-i}|v) \end{aligned} \quad (63)$$

$$= \frac{1}{q} \sum_{i=0}^{q-1} H(S|V) = H(S|V), \quad (64)$$

where (63) is obtained by using Lemma 1(i) and (iii). Since $I(S;U) = H(S) - H(S|U)$ and $I(S;V) = H(S) - H(S|V)$, (61) follows from (64).

For the pair $(p_{XV|S}, p_{Y|X}) \in \mathcal{Q}(L, p_S, D_1) \times \mathcal{A}_{cyc}(D_2)$ and its associated pair $(p_{XU|S}, p_{Y|X}) \in \mathcal{Q}_{cyc}^{Steg}(qL, p_S, D_1) \times \mathcal{A}_{cyc}(D_2)$, we have the following lemma that is proved in Appendix IV.

Lemma 2:

$$I_{p_S, p_{XV|S}, p_{Y|X}}(Y; V) \leq I_{p_S, p_{XU|S}, p_{Y|X}}(Y; U). \quad (65)$$

From (61), Lemma 2, and the definition of J_L in (14), we obtain

$$J_L(p_S, p_{XV|S}, p_{Y|X}) \leq J_{qL}(p_S, p_{XU|S}, p_{Y|X}), \quad (66)$$

which yields

$$\begin{aligned} & \lim_{L \rightarrow \infty} \max_{p_{XV|S} \in \mathcal{Q}(L, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}_{cyc}(D_2)} J_L(p_S, p_{XV|S}, p_{Y|X}) \\ & \leq \lim_{L \rightarrow \infty} \max_{p_{XU|S} \in \mathcal{Q}_{cyc}^{Steg}(qL, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}_{cyc}(D_2)} J_{qL}(p_S, p_{XU|S}, p_{Y|X}). \end{aligned} \quad (67)$$

Therefore, (60) and (67) yield

$$\begin{aligned} C^{Steg}(D_1, D_2) & \leq C^{PubWM}(D_1, D_2) \\ & \leq \lim_{L \rightarrow \infty} \max_{p_{XU|S} \in \mathcal{Q}_{cyc}^{Steg}(qL, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}_{cyc}(D_2)} J_L(p_S, p_{XU|S}, p_{Y|X}). \end{aligned} \quad (68)$$

B. Lower Bound

Using the same argument at the end of Appendix I for the sequence $\{C_L^{Steg}(D_1, D_2)\}$, we can argue that the sequence $\{C_L^{PubWM}(D_1, D_2)\}$ is also nondecreasing and bounded by $\log |S|$. Therefore, $\{C_L^{PubWM}(D_1, D_2)\}$ and any of its subsequences converge to the same limit. That is

$$\begin{aligned} C^{PubWM}(D_1, D_2) & = \lim_{L \rightarrow \infty} \max_{p_{XU|S} \in \mathcal{Q}(L, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} J_L(p_S, p_{XU|S}, p_{Y|X}) \\ & = \lim_{L \rightarrow \infty} \max_{p_{XU|S} \in \mathcal{Q}(qL, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} J_L(p_S, p_{XU|S}, p_{Y|X}). \end{aligned} \quad (69)$$

Similarly,

$$\begin{aligned} C^{Steg}(D_1, D_2) & = \lim_{L \rightarrow \infty} \max_{p_{XU|S} \in \mathcal{Q}^{Steg}(L, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} J_L(p_S, p_{XU|S}, p_{Y|X}) \\ & = \lim_{L \rightarrow \infty} \max_{p_{XU|S} \in \mathcal{Q}^{Steg}(qL, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} J_L(p_S, p_{XU|S}, p_{Y|X}). \end{aligned} \quad (70)$$

From (36),

$$\mathcal{Q}_{cyc}^{Steg}(qL, p_S, D_1) \subset \mathcal{Q}^{Steg}(qL, p_S, D_1) \subset \mathcal{Q}(qL, p_S, D_1).$$

Thus, we have

$$\begin{aligned} C^{PubWM}(D_1, D_2) & \geq C^{Steg}(D_1, D_2) \\ & \geq \lim_{L \rightarrow \infty} \max_{p_{XU|S} \in \mathcal{Q}_{cyc}^{Steg}(qL, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} J_L(p_S, p_{XU|S}, p_{Y|X}). \end{aligned} \quad (71)$$

Given $p_{Y|X} \in \mathcal{A}(p_X, D_2)$, we define q conditional PMFs:

$$p_{Y|X}^m(y|x) = p_{Y|X}(\underline{y-m}|\underline{x-m}), \quad \forall x, y \in \mathcal{S}, 0 \leq m < q. \quad (72)$$

Since the distortion matrix $\{d(i, j)\}_{i, j=0}^{q-1}$ is cyclic, it is easy to verify that all the q conditional PMFs $p_{Y|X}^m \in \mathcal{A}(p_X, D_2)$.

The conditional PMF $p_{Y|U}^m$ induced by $(p_{XU|S}, p_{Y|X}^m) \in \mathcal{Q}_{cyc}^{Steq}(qL, p_S, D_1) \times \mathcal{A}(p_X, D_2)$ is given by

$$\begin{aligned} p_{Y|U}^m(y|qv + i) &= \sum_{x=0}^{q-1} p_{X|U}(x|qv + i) p_{Y|X}^m(y|x) \\ &= \sum_{x=0}^{q-1} p_{X|U}(x|qv + i) p_{Y|X}(\underline{y-m}|\underline{x-m}) \end{aligned} \quad (73)$$

$$= \sum_{x=0}^{q-1} p_{X|V}(\underline{x-i}|\underline{v}) p_{Y|X}(\underline{y-m}|\underline{x-m}) \quad (74)$$

$$= \sum_{x=0}^{q-1} p_{X|U}(\underline{x-m}|\underline{qv + i - m}) p_{Y|X}(\underline{y-m}|\underline{x-m}) \quad (75)$$

$$= p_{Y|U}(\underline{y-m}|\underline{qv + i - m}), \quad \forall y, i \in \mathcal{S}, v \in \mathcal{V}, \quad (76)$$

where (73) follows from the definition (72), and both (74) and (75) follow by applying Lemma 1(ii). We also obtain the marginal PMF of Y as

$$\begin{aligned} p_Y^m(y) &= \sum_{v=0}^{L-1} \sum_{i=0}^{q-1} p_U(qv + i) p_{Y|U}^m(y|qv + i) \\ &= \sum_{v=0}^{L-1} \sum_{i=0}^{q-1} p_U(qv + \underline{i - m}) p_{Y|U}(\underline{y - m}|\underline{qv + i - m}) \end{aligned} \quad (77)$$

$$= p_Y(\underline{y - m}), \quad \forall y \in \mathcal{S}, \quad (78)$$

where (77) follows from Lemma 1(iii) and (76).

From (76) and (78), we obtain

$$I_{p_S, p_{XU|S}, p_{Y|X}}(Y; U) = I_{p_S, p_{XU|S}, p_{Y|X}^m}(Y; U) \quad (79)$$

and hence

$$J_L(p_S, p_{XU|S}, p_{Y|X}) = J_L(p_S, p_{XU|S}, p_{Y|X}^m), \quad (80)$$

for $0 \leq m < q$.

Let $\bar{p}_{Y|X} \triangleq \frac{1}{q} \sum_{m=0}^{q-1} p_{Y|X}^m$. It is easy to check that $\bar{p}_{Y|X} \in \mathcal{A}_{cyc}(D_2)$. Also,

$$J_L(p_S, p_{XU|S}, p_{Y|X}) = \frac{1}{q} \sum_{m=0}^{q-1} J_L(p_S, p_{XU|S}, p_{Y|X}^m) \quad (81)$$

$$\geq J_L\left(p_S, p_{XU|S}, \frac{1}{q} \sum_{m=0}^{q-1} p_{Y|X}^m\right) = J_L(p_S, p_{XU|S}, \bar{p}_{Y|X}), \quad (82)$$

where the inequality comes from the fact that for fixed p_S and $p_{XU|S}$, $J_L(p_S, p_{XU|S}, p_{Y|X})$ is convex in $p_{Y|X}$ [31, Proposition 4.1(iii)]. Therefore, from (82) we have

$$\begin{aligned} C^{PubWM}(D_1, D_2) &\geq C^{Steg}(D_1, D_2) \\ &\geq \lim_{L \rightarrow \infty} \max_{p_{XU|S} \in \mathcal{Q}_{cyc}^{Steg}(qL, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}(p_X, D_2)} J_L(p_S, p_{XU|S}, p_{Y|X}) \\ &\geq \lim_{L \rightarrow \infty} \max_{p_{XU|S} \in \mathcal{Q}_{cyc}^{Steg}(qL, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}_{cyc}(D_2)} J_L(p_S, p_{XU|S}, p_{Y|X}). \end{aligned} \quad (83)$$

Combining the upper bound inequality in (68) and the lower bound inequality in (83), we prove the claim

$$\begin{aligned} C^{PubWM}(D_1, D_2) &= C^{Steg}(D_1, D_2) \\ &= \lim_{L \rightarrow \infty} \max_{p_{XU|S} \in \mathcal{Q}_{cyc}^{Steg}(qL, p_S, D_1)} \min_{p_{Y|X} \in \mathcal{A}_{cyc}(D_2)} J_L(p_S, p_{XU|S}, p_{Y|X}), \end{aligned} \quad (84)$$

which means that the perfectly secure steganographic constraint does not cause any capacity loss.

APPENDIX IV

PROOF OF LEMMA 2

For the pair $(p_{XV|S}, p_{Y|X}) \in \mathcal{Q}(L, p_S, D_1) \times \mathcal{A}_{cyc}(D_2)$, the conditional PMF of Y given V is

$$\begin{aligned} p_{Y|V}(y|v) &= \sum_{x=0}^{q-1} p_{X|V}(x|v) p_{Y|X}(y|x) \\ &= \sum_{x=0}^{q-1} p_{X|V}(x|v) p_{Y|X}(\underline{y-x}|0), \quad \forall y \in \mathcal{S}, v \in \mathcal{V}, \end{aligned} \quad (85)$$

where (85) follows from (37) in Definition 11 for $p_{Y|X} \in \mathcal{A}_{cyc}(D_2)$. The conditional entropy of Y given V is

$$H(Y|V) = - \sum_{v=0}^{L-1} p_V(v) \sum_{y=0}^{q-1} p_{Y|V}(y|v) \log p_{Y|V}(y|v). \quad (86)$$

For the associated pair $(p_{XU|S}, p_{Y|X}) \in \mathcal{Q}_{cyc}^{Steg}(qL, p_S, D_1) \times \mathcal{A}_{cyc}(D_2)$, the conditional PMF of Y given U is

$$\begin{aligned} p_{Y|U}(y|qv+i) &= \sum_{x=0}^{q-1} p_{X|U}(x|qv+i) p_{Y|X}(y|x) \\ &= \sum_{x=0}^{q-1} p_{X|V}(\underline{x-i}|v) p_{Y|X}(\underline{y-i-(x-i)}|0) \end{aligned} \quad (87)$$

$$= p_{Y|V}(\underline{y-i}|v), \quad \forall y, i \in \mathcal{S}, v \in \mathcal{V}, \quad (88)$$

where to obtain (87) we have used Lemma 1(ii) and (37) in Definition 11 for $p_{Y|X} \in \mathcal{A}_{cyc}(D_2)$; and (88) follows from (85). The marginal PMF of Y is given by

$$\begin{aligned} \hat{p}_Y(y) &= \sum_{v=0}^{L-1} \sum_{i=0}^{q-1} p_U(qv+i) p_{Y|U}(y|qv+i) \\ &= \sum_{v=0}^{L-1} \sum_{i=0}^{q-1} \frac{1}{q} p_V(v) p_{Y|V}(\underline{y-i}|v) \end{aligned} \quad (89)$$

$$= \frac{1}{q} \sum_{j=0}^{q-1} p_Y(\underline{j-i}) = \frac{1}{q}, \quad (90)$$

where (89) follows from Lemma 1(iii) and (88). The conditional entropy of Y given U is

$$\begin{aligned} H(Y|U) &= - \sum_{v=0}^{L-1} \sum_{i=0}^{q-1} p_U(qv+i) \sum_{y=0}^{q-1} p_{Y|U}(y|qv+i) \log p_{Y|U}(y|qv+i) \\ &= - \sum_{v=0}^{L-1} \sum_{i=0}^{q-1} \frac{1}{q} p_V(v) \sum_{y=0}^{q-1} p_{Y|V}(y-i|v) \log p_{Y|V}(y-i|v) \end{aligned} \quad (91)$$

$$= \frac{1}{q} \sum_{j=0}^{q-1} H(Y|V) = H(Y|V), \quad (92)$$

where (91) follows from Lemma 1(iii) and (88), and (92) follows from (86).

Since $\hat{p}_Y(y) = \frac{1}{q}$ for any $y \in \mathcal{S}$ as shown in (90), we have

$$H_{\hat{p}_Y}(Y) \geq H_{p_Y}(Y), \quad (93)$$

where \hat{p}_Y and p_Y are the marginal PMF of Y for $(p_S, p_{XU|S}, p_{Y|X})$ and $(p_S, p_{XV|S}, p_{Y|X})$, respectively. Therefore, from (92) and (93), we obtain

$$I(Y; U) = H_{\hat{p}_Y}(Y) - H(Y|U) \quad (94)$$

$$\geq H_{p_Y}(Y) - H(Y|V) \quad (95)$$

$$= I(Y; V). \quad (96)$$

Hence, Lemma 2 is proved.

REFERENCES

- [1] N. F. Johnson and S. Katzenbeisser, "A survey of steganographic techniques," in *Information Hiding*, S. Katzenbeisser and F. Petitcolas, Eds. Norwood, MA: Artech House, 2000, pp. 43–78.
- [2] N. F. Johnson, Z. Duric, and S. Jajodia, *Information Hiding: Steganography and Watermarking-Attacks and Countermeasures*. Boston: Kluwer Academic Publishers, 2000.
- [3] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Francisco: Morgan-Kaufmann, 2002.
- [4] P. Moulin and R. Köetter, "Data-hiding codes," *Proc. IEEE*, vol. 93, no. 12, pp. 2083–2126, Dec. 2005.
- [5] J. Giles and B. Hajek, "An information-theoretic and game-theoretic study of timing channels," *IEEE Trans. Inform. Theory*, vol. 48, no. 9, pp. 2455–2477, Sept. 2003.
- [6] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," *IEEE J. Select. Areas Commun.*, vol. 16, no. 4, pp. 474–481, May 1998.
- [7] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *IEEE Computer*, vol. 31, no. 2, pp. 26–34, Feb. 1998.
- [8] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Security and Privacy Magazine*, vol. 1, no. 3, pp. 32–44, May-June 2003.
- [9] G. J. Simmons, "The prisoner's problem and the subliminal channel," in *Proc. CRYPTO'83*, 1984, pp. 51–67.
- [10] C. Cachin, "An information-theoretic model for steganography," *Information and Computation*, vol. 192, no. 1, pp. 41–56, July 2004.
- [11] Y. Wang and P. Moulin, "Steganalysis of block-DCT steganography," in *Proc. IEEE Workshop on Statistical Signal Processing*, St. Louis, MO, Sept. 2003, pp. 339–342.
- [12] —, "Steganalysis of block-structured stegotext," in *Proc. of the SPIE, Security, Steganography, and Watermarking of Multimedia Contents VI*, San Jose, CA, Jan. 2004, pp. 477–488.
- [13] O. Dabeer, K. Sullivan, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, "Detection of hiding in the least significant bit," *IEEE Trans. Signal Processing*, vol. 52, no. 10, pp. 3046–3058, Oct. 2004.
- [14] P. Moulin and A. Briassouli, "A stochastic QIM algorithm for robust, undetectable image watermarking," in *Proc. Int. Conf. on Image Processing*, vol. 2, Singapore, Oct. 2004, pp. 1173–1176.
- [15] Y. Wang and P. Moulin, "Optimized feature extraction for learning-based image steganalysis," *IEEE Trans. Inform. Forensics and Security*, vol. 2, no. 1, Mar. 2007.
- [16] K. Sullivan, U. Madhow, S. Chandrasekaran, and B. Manjunath, "Steganalysis for Markov cover data with applications to images," *IEEE Trans. Inform. Forensics and Security*, vol. 1, no. 2, pp. 275–287, June 2006.
- [17] K. Solanki, K. Sullivan, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, "Provably secure steganography: Achieving zero K-L divergence using statistical restoration," in *Proc. IEEE Int. Conf. on Image Processing*, Atlanta, GA, Oct. 2006.
- [18] K. Sullivan, K. Solanki, B. Manjunath, U. Madhow, and S. Chandrasekaran, "Determining achievable rates for secure zero divergence steganography," in *Proc. IEEE Int. Conf. on Image Processing*, Atlanta, GA, Oct. 2006.
- [19] J. J. Harmsen and W. A. Pearlman, "Steganalysis of additive noise modelable information hiding," in *Proc. of the SPIE, Security, Steganography, and Watermarking of Multimedia Contents VI*, San Jose, CA, Jan. 2003, pp. 131–142.
- [20] L. M. Marvel, C. G. Bonchelet, and C. T. Retter, "Spread spectrum image steganography," *IEEE Trans. Image Processing*, vol. 8, no. 8, pp. 1075–1083, Aug. 1999.
- [21] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," *IEEE Trans. Inform. Forensics and Security*, vol. 1, no. 1, pp. 111–119, Mar. 2006.
- [22] M. Goljan, J. Fridrich, and T. Holtyak, "New blind steganalysis and its implications," in *Proc. of the SPIE, Security, Steganography, and Watermarking of Multimedia Contents VI*, San Jose, CA, Jan. 2006, pp. 1–13.
- [23] H. Farid, "Detecting hidden messages using higher-order statistical models," in *Proc. IEEE Int. Conf. on Image Processing*, New York, Sept. 2002, pp. 905–908.
- [24] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color and gray-scale images," *IEEE Multimedia*, vol. 8, no. 4, pp. 22–28, Oct. 2001.
- [25] J. Fridrich and M. Goljan, "Practical steganalysis of digital images—state of the art," in *Proc. of SPIE Photonics West*, vol. 4675, San Jose, CA, Jan. 2002, pp. 1–13.

- [26] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," *IEEE Trans. Signal Processing*, vol. 51, no. 7, pp. 1995–2007, July 2003.
- [27] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, "Writing on wet paper," *IEEE Trans. Signal Processing*, vol. 53, no. 10, pp. 3923–3935, Oct. 2005.
- [28] J. Fridrich, M. Goljan, and D. Soukal, "Wet paper codes with improved embedding efficiency," *IEEE Trans. Inform. Forensics and Security*, vol. 1, no. 1, pp. 102–110, Mar. 2006.
- [29] F. Galand and G. Kabatiansky, "Steganography via covering codes," in *Proc. Int. Sym. on Inform. Theory*, Yokohama, Japan, July 2003, p. 192.
- [30] S. I. Gel'fand and M. S. Pinsker, "Coding for channel with random parameters," *Prob. of Control and Inform. Theory*, vol. 9, no. 1, pp. 19–31, 1980.
- [31] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information hiding," *IEEE Trans. Inform. Theory*, vol. 49, no. 3, pp. 563–593, Mar. 2003.
- [32] A. Somekh-Baruch and N. Merhav, "On the error exponent and capacity games of private watermarking systems," *IEEE Trans. Inform. Theory*, vol. 49, no. 3, pp. 537–562, Mar. 2003.
- [33] —, "On the capacity game of public watermarking systems," *IEEE Trans. Inform. Theory*, vol. 50, no. 3, pp. 511–524, Mar. 2004.
- [34] P. Moulin and Y. Wang, "Capacity and random-coding exponents for channel coding with side information," *IEEE Trans. Inform. Theory*, to appear, April 2007. [Online]. Available: <http://arxiv.org/abs/cs.IT/0410003>
- [35] I. Csiszár and J. Körner, *Information Theory: Coding Theory for Discrete Memoryless Systems*. New York: Academic Press, 1981.
- [36] I. Csiszár, "The method of types," *IEEE Trans. Inform. Theory*, vol. 44, no. 6, pp. 2505–2523, Oct. 1998.
- [37] P. Moulin and Y. Wang, "New results on steganographic capacity," in *Proc. Conf. on Inform. Science and Systems*, Princeton, NJ, Mar. 2004, pp. 813–818.
- [38] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Trans. Inform. Theory*, vol. 6, no. 44, pp. 2148–2177, Oct. 1998.
- [39] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *IEEE Trans. Inform. Theory*, vol. 48, no. 6, pp. 1250–1276, June 2002.
- [40] R. J. Barron, B. Chen, and G. W. Wornell, "The duality between information embedding and source coding with side information and some applications," *IEEE Trans. Inform. Theory*, vol. 49, no. 5, pp. 1159–1180, May 2003.