Minimizing Distortion in Data Embedding Using LDGM Codes and the Cavity Method

Masoumeh Alinia and David G. M. Mitchell
Klipsch School of Electrical and Computer Engineering, New Mexico State University, Las Cruces, NM 88003
e-mail: {aliniama,dgmm}@nmsu.edu

***Abstract*—In this paper, we propose a lossy source coding approach to improve embedding efficiency in steganography. A higher embedding efficiency (decreasing the distortion function) is desirable since it leads to better security. We propose to use a soft-hard belief propagation guided decimation (BPGD) algorithm for the encoding problem with low-density generator matrix (LDGM) codes. However, for good distortion performance, the parameters of the soft or soft-hard BPGD need to be tuned. To achieve this, we apply the cavity method to predict a value called the dynamical phase transition, which can minimize the distortion function for the soft-hard BPGD. This approach facilitates secure steganography by finding optimal parameters for the distortion function without the need for exhaustive search and simulation. Our method is shown to outperform related works in terms of embedding efficiency, performance, and complexity.**

I. Introduction

Steganography and cryptography both hide secret messages, but steganography aims to conceal the message's existence by embedding the message in media without detection. Alice and Bob may use steganography to communicate their escape plan, embedding the message in an image called the *cover image*. Wendy, the warden, is unable to distinguish between cover and *stego images*. Alice can embed the message in the cover image in various ways, using cover selection, cover synthesis, or cover modification [1].

A common problem with empirical cover objects is their difficulty in accurate modeling. Attackers can exploit the mismatch to create sensitive detection schemes [2]. Additionally, oversimplified models [3] can introduce security weaknesses. One solution is to use more complex models, but this is often difficult, and the majority of existing steganographic constructions are tailored to a specific model and can not readily adjust to more intricate models [4]. A common approach is to minimize embedding distortion through heuristics, such as matrix embedding [5], wet paper codes [6], and minimal embedding distortion steganography [7]. The principle of minimum embedding distortion has produced the most secure steganographic methods for digital media, although current schemes are limited by additive distortion functions that cannot capture interactions among embedding changes [8].

Practical coding theory methods can improve steganographic schemes by increasing their embedding efficiency, defined as the expected number of random message bits [10]. In [7], a framework is proposed to achieve a minimum embedding distortion (impact) using low-density generator matrix (LDGM) and syndrome codes with the Survey Propagation (SP) message-passing algorithm. The problem of optimally encoding a message with the smallest embedding distortion requires a binary quantizer performing near the rate-distortion (RD) bound. It was shown in [9] that LDGM codes can be used with a proper encoding algorithm to achieve such performance.

The approach of [7] considers an encoding algorithm for LDGM codes utilizing hard decimation [11]. Decimation (pruning the code graph and reducing the solution space) is an effective technique to force the convergence of the belief propagation (BP) algorithm. Such an approach works well for lossy source coding with LDGM codes; however, the computational complexity of the proposed method is $\mathcal{O}(n^2)$. Soft BPGD was proposed in [14], where an indicator function is introduced to approximate the hard decimation, and was shown to have a very good distortion performance for optimized irregular LDGM codes. Since the new algorithm incorporates the decimation step into the BP update equations with just one more addition and multiplication per edge, the overall computational complexity is $\mathcal{O}(n)$ instead of $\mathcal{O}(n^2)$. A variation called soft-hard decimation [15] was later shown to further improve performance with an additional complexity for various classes of LDGM codes. However, one drawback of these approaches is that they have algorithmic parameters that must be optimized to achieve good RD performance.

In this work, we use binary quantization based on belief propagation guided decimation (BPGD) with LDGM codes for lossy source encoding to compute the distortion function. Specifically, we consider soft and soft-hard versions of BPGD. We measure the impact of embedding modifications, where the sender aims to minimize the distortion function while embedding the payload. To achieve good distortion results, the BPGD algorithm parameters should be carefully chosen, which is conventionally done with expensive and exhaustive Monte Carlo Simulation. Here, we provide a framework based on the cavity method, extending our results in [12], to compute a critical threshold for the BPGD parameters in an interval where the phase transition changes. Parameters equal to or close to the threshold value achieve superior rate-distortion performance and higher embedding efficiency compared to the binary quantizer [7]. The proposed method is shown to outperform related works in terms of embedding efficiency, performance, and complexity.

II. Background

In this section, we start by giving some basic definitions related to the distortion function in steganography. We then proceed to discuss matrix embedding methods and how LDGM codes can be used in this context. Finally, we discuss how the Gibbs distribution can be applied for this problem.

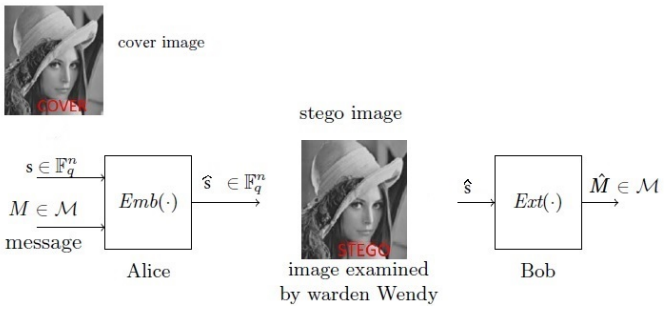

Fig. 1. Model of the steganographic scheme.

A. Distortion Function in Steganography

When embedding message M using some steganographic scheme, we take the *cover image* represented using a symbol assignment function as a sequence $\mathbf{s} \in \mathbb{F}_q^n$ and we change this sequence to the *stego image* represented as a sequence $\hat{\mathbf{s}} \in \mathbb{F}_q^n$. Further, we assume that our message M can be represented as a sequence $m \in \mathbb{F}_q^m$. A steganographic scheme is a pair of embedding and extraction mappings $\mathrm{Emb}(\cdot) : \mathbb{F}_q^n \times \mathcal{M} \to \mathbb{F}_q^n$ and $\mathrm{Ext}(\cdot) : \mathbb{F}_q^n \to \mathcal{M}$, satisfying

$$\mathrm{Ext}(\mathrm{Emb}(s, M)) = M, \forall \mathbf{s} \in \mathbb{F}_q^n, \forall M \in \mathcal{M}, \qquad (1)$$

where $\mathcal{M}$ refers to the set of all possible messages that can be communicated. The embedding capacity of the scheme is $\log |\mathcal{M}|$ and we will use the binary case $\mathbb{F}_q = GF(2)$ for our approach. The system diagram of the steganographic scheme is shown in Fig. 1.

The impact of embedding modifications will be measured using a distortion function D. The cost of making an embedding change at pixel s_i is $\rho_i \geq 0$. The total embedding impact is defined as $D(\mathbf{s}, \hat{\mathbf{s}}) = \|\mathbf{s} - \hat{\mathbf{s}}\|_D = \sum_{i=1}^n \rho_i |s_i - \hat{s}_i|$. The expected value $\mathbb{E}[D(\mathbf{s}, \hat{\mathbf{s}})]$ is calculated for all cover objects $\mathbf{s}$ and messages of length m. Suppose we want to communicate m bits on a test channel using n bits. For $\mathbf{s}$, $\hat{\mathbf{s}} \in \{0,1\}^n$, we define error pattern $\mathbf{z} \in \{0,1\}^n$ as $z_i = \delta(s_i, \hat{s}_i)$, where $\delta(x, y) = 1$ when $x = y$ and $\delta(x, y) = 0$, otherwise. Additionally, we define $D(\mathbf{z}) = D(\mathbf{s}, \hat{\mathbf{s}})$ as the distortion impact of making an error . Assume that we make an error pattern $\mathbf{z}$ with probability $p(\mathbf{z})$, the amount of communicated information is the entropy of $p(\mathbf{z})$

$$H(p) = -\sum_{\mathbf{z}} p(\mathbf{z}) \log_2 p(\mathbf{z}).$$

In order to to find the probability distribution $p(\mathbf{z})$ on the space of all possible flipping patterns $\mathbf{z}$ which minimizes the expected value of distortion $\sum_{\mathbf{z}} D(\mathbf{z}) p(\mathbf{z})$ subject to the condition

$$H(p) = \sum_{\mathbf{z}} p(\mathbf{z}) \log_2 p(\mathbf{z}) = m, \sum_{\mathbf{z}} p(\mathbf{z}) = 1,$$

we solve the Lagrange multipliers equation. Let

$$L(p(\mathbf{z})) = \sum_{\mathbf{z}} p(\mathbf{z}) D(\mathbf{z}) + c_1 \left(m - \sum_{\mathbf{z}} p(\mathbf{z}) \log_2 p(\mathbf{z}) \right) + c_2 \left(\sum_{\mathbf{z}} p(\mathbf{z}) - 1 \right),$$

then

$$\frac{\partial L}{\partial p(\mathbf{z})} = D(\mathbf{z}) - c_1 \left(\log_2 p(\mathbf{z}) + 1/\ln(2) \right) + c_2 = 0$$

if and only if $p(\mathbf{z}) = A e^{-\gamma D(\mathbf{z})}$, where $A^{-1} = \sum_{\mathbf{z}} e^{-\gamma D(\mathbf{z})}$ and γ is determined from

$$-\sum_{\mathbf{z}} p(\mathbf{z}) \log_2 p(\mathbf{z}) = m.$$

B. Matrix Embedding

In the steganography scheme known as matrix embedding [7], the receiver has knowledge of the relative message length, denoted as $\alpha = m/n$, and the number of secret message bits, m. This information can be pre-agreed upon, or a small portion of the cover can be reserved to convey α using a few quantized bits dependent on a cryptographic key. We consider a binary linear code, denoted as $\mathcal{C}$, with dimensions $[n, n-m]$, consisting of an $n \times (n-m)$ generator matrix $\mathbf{G}$ and an $m \times n$ parity check matrix $\mathbf{H}$. These matrices are shared between the sender and recipient. The coset $\mathbf{C}(\mathbf{m})$ is defined as $\mathbf{C}(\mathbf{m}) = \{\mathbf{u} \in \{0,1\}^n \mid \mathbf{H}\mathbf{u} = \mathbf{m}\}$, where $\mathbf{m}$ represents the secret message and corresponds to the syndrome $\mathbf{m} \in \{0,1\}^m$. The following embedding scheme [7] communicates m bits in an n-element cover

$$\hat{\mathbf{s}} = \mathrm{Emb}(\mathbf{s}, \mathbf{m}) \triangleq \arg \min_{\mathbf{u} \in \mathcal{C}(\mathbf{m})} \|\mathbf{s} - \mathbf{u}\|_D$$
$$\mathrm{Ext}(\hat{\mathbf{s}}) = \mathbf{H}\hat{\mathbf{s}} = \mathbf{m}.$$

Here, $\hat{\mathbf{s}}$ are the bits assigned to the stego image. To minimize the embedding impact, the sender should select the member $\hat{\mathbf{s}}$ of the coset $\mathbf{C}(\mathbf{m})$ that is closest to $\mathbf{s}$ (closest in metric $\|\cdot\|_D$). Let $\mathbf{v}_\mathbf{m} \in \mathbf{C}(\mathbf{m})$ be selected arbitrarily, then since $\mathcal{C}$ is linear,

$$\begin{aligned} \min_{\mathbf{u} \in \mathcal{C}(\mathbf{m})} \|\mathbf{s} - \mathbf{u}\|_D &= \min_{\mathbf{c} \in \mathcal{C}} \|\mathbf{s} - (\mathbf{v}_\mathbf{m} + \mathbf{c})\|_D \\ &= \min_{\mathbf{w} \in \{0,1\}^{n-m}} \|\mathbf{s} - \mathbf{v}_\mathbf{m} - \mathbf{G}\mathbf{w}\|_D . \end{aligned} \qquad (2)$$

The equation (2) represents the embedding as a binary quantization problem. The sender needs to find $\mathbf{w} \in \{0,1\}^{n-m}$ such that $\mathbf{G}\mathbf{w}$ is closest to $\mathbf{s} - \mathbf{v}_\mathbf{m}$. In other words, the sender is compressing the source bit sequence $\mathbf{z} = \mathbf{s} - \mathbf{v}_\mathbf{m}$ to $n-m$ information bits $\mathbf{w}$ so that the reconstructed vector $\mathbf{G}\mathbf{w}$ is as close to the source sequence as possible. In order to process a secure embedding scheme, we need to be careful to generate a code with proper encoding and decoding algorithms to find $\mathbf{v}_\mathbf{m}$, with minimal distortion. According to rate-distortion theory, the rate of any source encoding algorithm that compresses n bits into $n-m$ bits is bounded by $R = 1 - m/n \leq 1 - H(d)$, where $d = D/n$ is the average distortion per bit. Therefore, the maximal embedding efficiency e of any matrix embedding scheme is bounded above by $e \leq \frac{\alpha}{H^{-1}(\alpha)}$, where $\alpha = m/n$ is the relative message length and $e = m/D$ is the average number of message bits embedded per unit distortion.

C. LDGM code ensembles for steganography

LDGM codes, as duals of LDPC codes, can be represented by generator matrix $\mathbf{G} \in \{0,1\}^{n\times k}$. We define the factor graph of this code as $\mathcal{G} = (V, C, E)$, where $V = \{1, \ldots, k\}$, $C = \{1, \ldots, n\}$, and $E = \{\ldots, (a, i), \ldots\}$ denote the code bit nodes, the generator nodes, and the edges connecting them, respectively. The vector (a, i) denotes an edge between generator node a and code bit node i, which occurs iff $\mathbf{G}_{a,i} = 1$. We will use indices $a, b, c \in C$ to denote generator nodes and indices $i, j, k \in V$ to denote code bit nodes. We define the sets $C(i) = \{a \in C \mid (a, i) \in E\}$ and $V(a) = \{i \in V \mid (a, i) \in E\}$. In this paper, we follow the construction of [13], where each edge emanating from a regular check node with degree l is connected uniformly at random to one of the bit nodes. The degree of bit nodes is a random variable with Binomial distribution $Bi(ln, 1/k)$. In the asymptotic regime of large n, k, the bit node degrees have i.i.d. Poisson distribution with an average degree l/R. For an LDGM code $\mathcal{C}$, defined by the generator matrix $\mathbf{G}$, and for a codeword $\mathbf{w}$, the reconstructed source sequence is given by $\hat{\mathbf{s}} = \mathbf{G}\mathbf{w}$.

In this paper, we quantize a sequence $\mathbf{s} = (s_1, s_2, \ldots, s_n)$ consisting of n independent and identically distributed Bernoulli random variables to the nearest codeword $\mathbf{w} = (w_1, w_2, \ldots, w_k)$, giving a *compression rate* of $R = \frac{k}{n}$. The codeword $\mathbf{w}$ is used to reconstruct the source sequence as $\hat{\mathbf{s}}$, where the mapping $\mathbf{w} \to \hat{\mathbf{s}}(\mathbf{w})$ depends on the LDGM code. The measure of binary quantization is the Hamming metric $d(\mathbf{s}, \hat{\mathbf{s}}) = \frac{1}{n}\sum_{i=1}^{n} |\mathbf{s}_i - \hat{\mathbf{s}}_i|$. The final goal is to minimize the average distortion $D = \mathbb{E}[d(\mathbf{s}, \hat{\mathbf{s}})]$, where $\mathbb{E}[\cdot]$ is the expectation taken over all possible source sequences $\mathbf{s}$. The rate-distortion function is in the form $R(D) = 1 - H(D)$ for $D \in [0, 0.5]$ and 0 otherwise, where H is the binary entropy function.

D. Gibbs distribution

The probability $p(\mathbf{z})$ from the distortion function described in Section II-A follows an exponential Gibbs distribution with respect to distortion $D(\mathbf{z})$. In statistical mechanics, the Gibbs distribution is a probability measure that gives the probability of finding a system in a particular state [16]. It is a function of the state's energy and the temperature of the system. BPGD encoding can be understood as examining the scenario where the temperature approaches zero in the Gibbs distribution with a Hamiltonian. We can therefore utilize the features of the Gibbs distribution to minimize the distortion function using the cavity method adopted for our soft BPGD algorithm, resulting in a method to determine bounds on optimal algorithm parameters. In other words, we search to minimize the expected embedding impact $E[D(\mathbf{s}, \hat{\mathbf{s}})]$ with proper selection of parameters for covers of length n, embedding capacity m, and destructibility measure $\rho_i = 1$.

Let us equip the solution space $\{0,1\}^{nR}$ of the equation $\hat{\mathbf{s}} = \mathbf{G}\mathbf{w}$ with a conditional probability which is linked to spin glass theory in statistical mechanics. We consider the general class of Gibbs distribution of the form

$$P_\gamma(\mathbf{w} \mid \mathbf{s}) = \frac{1}{Z_\gamma} \prod_{a\in C} e^{-2\gamma N d(\mathbf{s}, \hat{\mathbf{s}}(\mathbf{w}))}. \tag{3}$$

The term $2Nd(\mathbf{s}, \hat{\mathbf{s}}(\mathbf{w}))$ is called random Hamiltonian function which a cost-function for assignments of variables $w_i \in \{0, 1\}$. Here, the different source bits and different graph ensembles of LDGM codes give different cost functions. The parameter γ is the inverse temperature, and the normalizing factor Z_γ is the partition function. From a statistical mechanics point of view, finding the most reliable code word $\mathbf{w}^* = \arg\max_{\mathbf{w}} P_\gamma(\mathbf{w} \mid \mathbf{s})$ is to find the minimum energy configuration [13]. The minimum energy per node is equal to $2d_{N,\min}$, in which $d_{N,\min} = \min_{\mathbf{w}} d(\mathbf{s}, \hat{\mathbf{s}}(\mathbf{w}))$. In the cavity method, the one-step replica symmetry breaking (1RSB) gives the exact value for the internal energy. This can allow the computation of the optimal distortion numerically by the population dynamics method known as Monte Carlo in channel coding.

III. Soft-Hard BPGD

This section discusses the soft and soft-hard BPGD algorithms that we will use to construct an efficient embedding scheme with LDGM codes. The soft-decimation BP algorithm equations [14] are updated as follows

$$\eta_i^{(t+1)} = \sum_{a\in C(i)} \widehat{\eta}_{a\to i}^{(t)}, \quad \eta_{i\to a}^{(t+1)} = \sum_{b\in C(i)\setminus a} \widehat{\eta}_{b\to i}^{(t)} + \frac{1}{\mu}\eta_i^{(t)}, \tag{4}$$

$$\widehat{\eta}_{a\to i}^{(t+1)} = 2(-1)^{s_a+1} \tanh^{-1}\left(\beta \prod_{j\in V(a)\setminus i} B_{j\to a}^{(t)}\right), \tag{5}$$

$$B_i^{(t)} = \tanh\left(\frac{\eta_i^{(t)}}{2}\right), \quad B_{i\to a}^{(t)} = \tanh\left(\frac{\eta_{i\to a}^{(t)}}{2}\right), \tag{6}$$

where $\eta_{i\to a}^{(t)}, \widehat{\eta}_{a\to i}^{(t)}$, and $B_{i\to a}^{(t)}$ denote the message sent from code node i to check node node a, the message sent from check node a to code node i, and the bias associated with $\eta_{i\to a}^{(t)}$ at iteration t, respectively; $\eta_i^{(t)}$ and $B_i^{(t)}$ denote the likelihood ratio of code bit i and the bias associated with $\eta_i^{(t)}$, respectively; and $\beta = \tanh(\gamma)$ and μ are non-negative parameters. The γ parameter reflects the effort of the message-passing algorithm to find the resulting codeword $\hat{\mathbf{s}} = \mathbf{G}\mathbf{w}$ as close to $\mathbf{s}$ as possible. The larger the γ, the stronger is the effort. On the other hand, the structure of the code imposes a limit on how strong this effort can be.

The term $\frac{1}{\mu}\eta_{i\to a}^{(t)}$ is added to the plain BP equation to make the decimation softer. The soft indicator function $I_S(B_{i\to a}^{(t)}) = \frac{2}{\mu}\tanh^{-1}(B_{i\to a}^{(t)}) = \frac{1}{\mu}\eta_{i\to a}^{(t)}$ approximates the hard-indicator function [15], given as

$$I_H\left(B_{i\to a}^{(t)}\right) = \begin{cases} -\infty, & B_{i\to a}^{(t)} = -1, \\ 0, & -1 < B_{i\to a}^{(t)} < 1, \\ +\infty, & B_{i\to a}^{(t)} = 1, \end{cases}$$

where μ controls the softness of the approximation and is called the *softness parameter*. The soft-hard BPGD combines elements of both hard [11] and soft decimation [14]. Similar to soft decimation equations, our algorithm identifies a bit node with the maximum bias value after each iteration. Algorithm 1 describes the procedure, where t indicates the iteration

number, $\mathcal{G}^{(t)}$ is the LDGM code graph at iteration t, and w_i represents the binary value assigned to code node i. The initial information to check node node messages, $\eta_{i\to a}^{(0)}$, are set to ± 0.1 with $\mathbb{P}\left(\eta_{i\to a}^{(0)} = 0.1\right) = 0.5$, and reset to 0 at iteration number 1.

Algorithm 1 Soft-Hard Decimation Algorithm

Require: At iteration $t = 0$, initialize graph instance $\mathcal{G}^{(t=0)}$;
Generate a Bernoulli symmetric source word s;
while $V \neq \emptyset$ **do**
Update $\eta_{i\to a}^{(t+1)}$ according to (4) for all $(a, i) \in E$;
Update $\widehat{\eta}_{a\to i}^{(t)}$ according to (5) for all $(i, a) \in E$;
Compute bias $B_{i\to a}^{(t)}$ and $B_i^{(t)}$ according to (6);
Find $B^{(t)} = \max_i \left\{ \left| B_i^{(t)} \right| \mid \text{i not fixed} \right\}$;
if $B^{(t)} > 0$ **then**
$w_i \leftarrow '0'$;
else
$w_i \leftarrow '1'$;
end if
$\forall a \in C(i), s_a \leftarrow s_a \oplus w_i$ (update source);
Reduce the graph $\mathcal{G} \leftarrow \mathcal{G} \backslash \{i\}$;
$\mathcal{G}^{(t+1)} = \mathcal{G}^{(t)} \backslash \{i\}$ (remove code node i and all its edges);
end while

The primary benefit of this formulation lies in its capacity to restrict the belief of information bits in the direction of the current bit belief during each iteration, as opposed to limiting beliefs solely at the decimation step. This allows for a continuous refinement of information bit beliefs throughout each iteration. Consequently, all bits undergo decimation simultaneously, as opposed to a fixed number of information bits at each decimation step, as observed in [11]. In [7], there is no analytical way to tune the value of γ in order to give the best distortion performance. The best value of γ is conventionally found numerically by exhaustive and expensive code simulation. In the next section, we apply spin glass theory in the cavity method to carefully tune γ and the softness parameters μ or β in the soft-hard BPGD algorithm to ensure good RD performance.

IV. Cavity method to determine parameters for soft-hard BPGD

The best assignment for bit $\mathbf{w}^*$ is obtained from the corresponding bit marginal value. However here the cavity method assumes that (3) can be decomposed into a convex superposition of measures

$$P_\gamma(\mathbf{w} \mid \mathbf{s}) = \sum_{\lambda=1}^{\mathcal{N}} \omega_\lambda P_{\gamma,\lambda}(\mathbf{w} \mid \mathbf{s}). \tag{7}$$

The summation of weights $\omega_\lambda = e^{-\gamma N(f_\lambda - f)}$ should be one, where f_λ is the free energy. Therefore

$$e^{-\gamma N f} \approx \sum_{\lambda=1}^{\mathcal{N}} e^{-\gamma N f_\lambda} \approx e^{-\gamma N \min_\varphi \left(\varphi - \gamma^{-1}\Sigma(\varphi;\gamma)\right)}, \tag{8}$$

where $e^{N\Sigma(\varphi;\gamma)}$ counts the number of extremal states P_γ with free energy $f_\lambda \approx \varphi$. The cavity method seeks two thresholds, γ_d and γ_c, in which the nature of the decomposition (7) changes. For $\gamma < \gamma_d$ this measure is extremal and $\mathcal{N} = 1$. For $\gamma_d < \gamma < \gamma_c$, the measure is a convex superposition of an exponentially large number of extremal states. The exponent $\varphi - \gamma^{-1}\Sigma(\varphi;\gamma)$ in (8) is minimized at a value $\varphi_{\text{int}}(\gamma)$ such that $\Sigma\left(\varphi_{\text{int}}(\gamma);\gamma\right) > 0$. Then the complexity function

$$\Sigma(\gamma) \equiv \Sigma\left(\varphi_{\text{int}}(\gamma);\gamma\right) = \gamma\left(\varphi_{\text{int}}(\gamma) - f(\gamma)\right) \tag{9}$$

describes the growth rate of extremal states (7). The complexity function decreases as γ increases, becoming negative at γ_c, which is the point where it loses its meaning. At γ_d, there are no singularities in the free and internal energies, and their analytical expressions do not change in the range $0 < \gamma < \gamma_c$. The transition at γ_d is dynamic, and Markov chain Monte Carlo algorithms have an equilibration time that diverges when γ approaches γ_d. The cavity method uses the population dynamic approach to predict phase transitions by solving fixed point integral equations.

The cavity method [13] is applied to soft BPGD equations, and the BP formulation with a soft indicator function that we use will result in certain changes to the computation. We first derive the cavity equations needed to compute the complexity function (9) for our soft-hard BPGD algorithm. For BP equations (4) and (5), we need to replace $(-1)^{s_a} = J$ as well as express the bias in terms of variable to check node updates using (6), since the average field h_i in the cavity method must be defined as $\eta_{i\to a}^{(t)} = \gamma h_i$. To derive the fixed point equations, the cavity equations are written for an average ensemble of the graph and source word, which involve messages on the edges of the graph. For the integral fixed point equations and their relations, the interested reader may refer to appendices B and C of [13]. The derivations and adaptations to the present setting of soft-hard BPGD and the proper approach for finding γ_d follows [12] and are omitted due to space constraints.

V. Numerical Results

A. Determining γ

In order to obtain parameter thresholds for soft-hard BPGD, we now derive the corresponding values $\beta_d = (1-e^{-2\gamma_d})/(1+e^{-2\gamma_d})$ and $\mu_d = e^{4\gamma_d}$ following the procedure outlined in Section IV. Since decimated BP can correctly sample the Gibbs-Boltzmann measure up to γ_d, we can see that the optimal value for γ can be found near the dynamic phase γ_d. Therefore, the best value of μ for soft-hard BPGD can be found in the interval $\left(0, e^{4\gamma_d}\right)$. This can either be used to reduce the search space for an optimal value of μ, or the thresholds can be used directly in the BP equations. These techniques significantly reduce the complexity of exhaustive search techniques based on code simulation, such as [11], which need to be re-run for each code/code ensemble.

In Fig. 2, we plot the distortion of an LDGM code as a function of γ with $n = 2000$, $R = 1/2$, and check node degree $l = 3$ for $0 < \gamma < 1.5$. From right to left, as the temperature increases (inverse of γ), we observe that the distortion curve

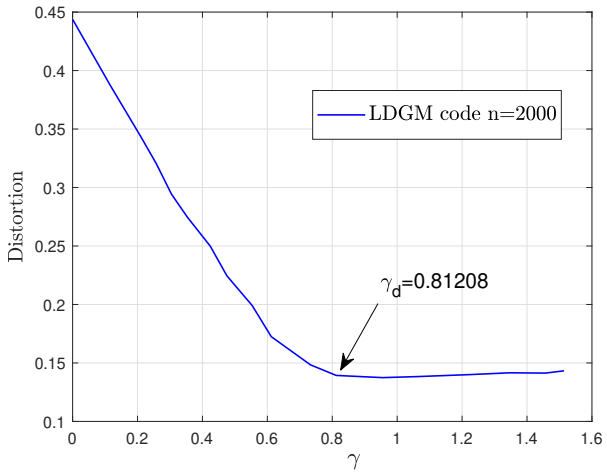

Fig. 2. The relation between distortion and γ.

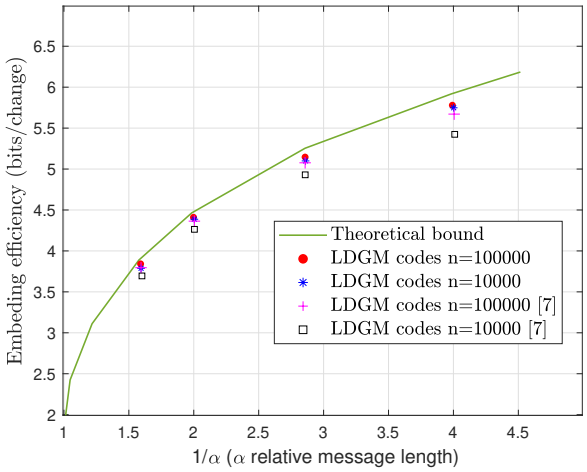

Fig. 3. Embedding efficiency over a range of α for long codes with BPGD and [7].

shows a slow decrease, followed by a sharp increase around the phase transition threshold. The lowest distortion occurs within the flat region and as long as γ is selected within this flat segment, the distortion does not vary much. We leverage this characteristic, calculating the distortion curve (embedding efficiency) of the BPGD at a pre-determined γ value ($\gamma_d = 0.81208$ in this example).

B. Simulation Results

We have implemented Algorithm 1 in C++ and run a Monte Carlo simulator for some constructed LDGM codes to compare the embedding efficiency against the proposed LDGM codes from [7]. For each code construction, we computed the value of γ with the cavity method. Codes were generated randomly with regular check nodes and irregular bit nodes degrees with a binomial distribution as described in Section II-C.

Fig. 3 displays a comparison of the embedding efficiency obtained from the LDGM codes [7] and soft-hard BPGD algorithm as a function of α for two different code lengths $n = 10000$ and $n = 100000$. Our LDGM codes are constructed randomly, as described in section II-C, with a constant check node degree $l = 5$. The proposed dynamic phase transition in the cavity method described in Section IV can be applied to determine different γ_d related to α. For example, the value of the γ_d for $\alpha = 1/2$ with cavity method is 0.832 without the need for exhaustive computation and search. The embedding efficiency is computed for fixed α and the empirical average is taken. Then, each embedding efficiency was obtained by averaging over 20 randomly generated messages. The comparison indicates the embedding efficiency of simulated codes using the BPGD algorithm outperforms codes simulated with the encoding scheme [7]. Note that the results are compared for the computed threshold and not numerically optimized.

Fig. 4 demonstrates the impact of code length on the embedding efficiency. The algorithm was run for 100 iterations of a randomly drawn LDGM code with a constant check node degree 9, $R = 1/2$, and different codeword lengths. The results were obtained by averaging over 100 trials. The dynamic phase transition in the cavity method for this degree distribution is $\gamma_d = 0.671$ for this simulation. We observe

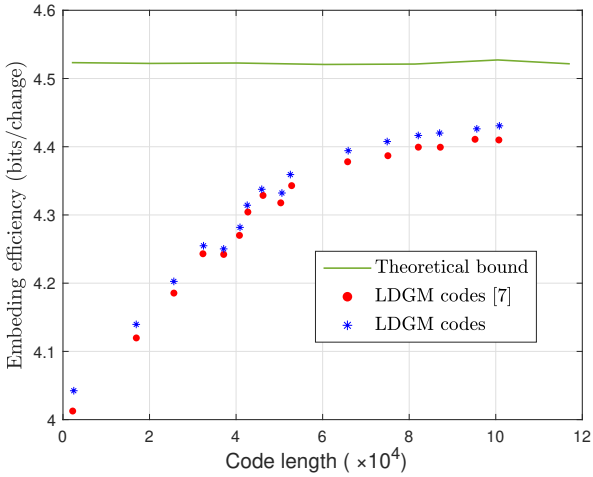

Fig. 4. Embeding efficiency using BPGD for LDGM codes with $R = 1/2$.

that the embedding efficiency approaches the upper bound as the code length grows. The final gap in embedding efficiency between the theoretical bound and codes based on the code length $n = 10^5$ is less than 0.07 bits per change, smaller than the gap for algorithm [7].

VI. Conclusions

This paper considered the problem of minimizing embedding efficiency in steganography using LDGM codes and soft-hard BPGD encoding. We presented a framework employing the cavity method to optimize distortion function parameters. Numerical simulation results confirm that optimized distortion performance is achieved when parameters are chosen at or near the threshold value, outperforming the hard BPGD algorithm. This strategy can mitigate the need for expensive computer searches and simulations to optimize parameters, while maintaining good rate-distortion performance and therefore better embedding efficiency.

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No. CCF-2145917.

REFERENCES

[1] M. Kharrazi, H.T. Sencar, and N. Memon, "Cover selection for steganographic embedding," *International Conference on Image Processing,* pp. 117-120, 2006.

[2] A. Westfeld and R. Böhme, "Exploiting preserved statistics for steganalysis," *6th International Workshop Information Hiding,* volume 3200 of Lecture Notes in Computer Science, pp. 82–96, 2004.

[3] J. Kodovsky and J. Fridrich, "On completeness of feature spaces in blind steganalysis," *10th ACM Multimedia and Security Workshop,* pp. 123–132, 2008.

[4] T. Filler and J. Fridrich, "Gibbs construction in steganography," *IEEE Transactions on Information Forensics and Security,* vol. 5, no. 4, pp.705-720, 2010.

[5] J. Fridrich and D. Skoal, "Matrix embedding for large payloads," *IEEE Transactions on Information Forensics and Security,* vol. 1, no. 3, pp.390-395, 2006.

[6] J. Fridrich, M. Goljan, D. Soukal, and P. Lisonek, "Writing on wet paper," *Electronic Imaging, Security, Steganography, and Watermarking of Multimedia* Contents VII, vol. 5681, pages 328–340, 2005.

[7] J. Fridrich and T. Filler, "Practical methods for minimizing embedding impact in steganography," *Security, Steganography, and Watermarking of Multimedia* Contents IX, vol. 6505, pp. 13-27, SPIE, 2007.

[8] T. Filler, J. Judas, and J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," *IEEE Transactions on Information Forensics and Security,* vol. 6, no. 3, pp.920-935, 2011.

[9] M. J. Wainwright and E. Maneva, "Lossy source encoding via message-passing and decimation over generalized codewords of LDGM codes," *International Symposium on Information Theory,* pp. 1493-1497, 2005.

[10] W. Zhang and S. Li, "Steganographic Codes, a New Problem of Coding Theory," arXiv preprint cs/0505072, 2005.

[11] T. Filler and J. Fridrich, "Binary quantization using belief propagation with decimation over factor graphs of LDGM codes," CoRR, vol.abs/0710.0192, 2007.

[12] M. Alinia and D. G. M. Mitchell, "Optimizing Parameters in Soft-hard BPGD for Lossy Source Coding," *12th International Symposium on Topics in Coding (ISTC)* pp. 1-5, 2023.

[13] V. Aref, N. Macris and M. Vuffray, "Approaching the Rate-Distortion Limit With Spatial Coupling, Belief Propagation, and Decimation," *IEEE Trans. Inf. Theory*, vol. 61, no. 7, pp. 3954-3979, 2015.

[14] D. Castanheira and A. Gameiro, "Lossy source coding using belief propagation and soft-decimation over LDGM codes," *21st Annual IEEE Int. Symp. on Personal, Indoor and Mobile Radio Comm.,* pp. 431-436, 2010.

[15] A. Golmohammadi, D. G. M. Mitchell, J. Kliewer and D. J. Costello, "Encoding of spatially coupled LDGM codes for lossy source compression," *IEEE Trans. Comm.*, vol. 66, no. 11, pp. 5691-5703, 2018.

[16] A. Montanari, F. Ricci-Tersenghi, G. Semerjian, "Clusters of solutions and replica symmetry breaking in random k-satisfiability," *Journal of Statistical Mechanics: Theory and Experiment,* p.P04004, 2008.