Adaptive Batch Size Image Merging Steganography and Quantized Gaussian Image Steganography

Mehdi Sharifzadeh, *Member, IEEE*, Mohammed Aloraini, *Member, IEEE*, and Dan Schonfeld, *Fellow, IEEE*

***Abstract*— In digital image steganography, the statistical model of an image is essential for hiding data in less detectable regions and achieving better security. This has been addressed in the literature where different cost-based and statistical model-based approaches were proposed. However, due to the usage of heuristically defined distortions and non-constrained message models, resulting in numerically solvable equations, there is no closed-form expression for security as a function of payload. The closed-form expression is crucial for a better insight into image steganography problem and also improving performance of batch steganography algorithms. Here, we develop a statistical framework for image steganography in which the cover and the stego messages are modeled as multivariate Gaussian random variables. We propose a novel Gaussian embedding model by maximizing the detection error of the most common optimal detectors within the adopted statistical model. Furthermore, we extend the formulation to cost-based steganography, resulting in a universal embedding scheme that improves empirical results of current cost-based and statistical model-based approaches. This methodology and its presented solution, by reason of assuming a continuous hidden message, remains the same for any embedding scenario. Afterward, the closed-form detection error is derived within the adopted model for image steganography and it is extended to batch steganography. Thus, we introduce Adaptive Batch size Image Merging steganographer, *AdaBIM*, and mathematically prove it outperforms the state-of-the-art batch steganography method and further verify its superiority by experiments.**

***Index Terms*— Steganography, optimal detector, hypothesis testing, Gaussian embedding, batch steganography.**

I. Introduction

STEGANOGRAPHY problem is formulated by the prisoner's problem where Alice and Bob want to communicate through a cover medium without raising any suspicion from Wendy, the warden [1]. In this paper, we focus on the most popular and studied cover medium, digital images. Non-adaptive image steganography approaches [2], [3] are easily detectable as they neglect pixel to pixel dependencies [4]. Therefore, in order to achieve a better security, hidden message should be embedded in textured or noisy areas rather than smooth regions. This has led to a group of content adaptive spatial image steganography methods which we call cost based methods. In these methods, message embedding is done while minimizing the caused distortion and it is formulated as a source coding problem with a fidelity criterion [5]. These methods include two main steps, first is calculating cost of embedding in each pixel using a heuristically defined distortion function, and second is embedding the message according to the costs. The second step is solved for a general distortion function using syndrome trellis codes and Gibbs measure [6], [7]. Examples of such steganography methods are **S**patial **UNI**versal **WA**velet **R**elative **D**istortion (SUNIWARD) [8] and **HI**gh-pass, **L**ow-pass, and **L**ow-pass (HILL) [9]. Although, these methods achieve superior results, there is no theoretical relation between statistical security measures and these derived distortion functions [10]. Thus, the security of these methods can be measured only empirically. This issue has been resolved in the other category of steganography methods which we call statistical based methods. They rely on a cover model and aim to minimize statistical distortion while embedding.

The first successful example of such a steganography method is **H**ighly **U**ndetectable ste**GO** (HUGO) which tries to preserve SPAM feature vector [11] of the cover while embedding [12]. HUGO has low security against steganalysis with more complete feature space, since it is over fit to SPAM features [13]. To avoid this drawback, embedding can be done while minimizing statistical detectability instead of preserving an empirical feature space. This has been addressed in a revolutionary work by Fridrich et al., where a general Gaussian model was developed for cover image and embedding was done by minimizing its statistical distortion modeled as Kullback-Leibler (KL) divergence [14]. The results were improved using a generalized Gaussian model and measuring statistical distortion as performance of a likelihood ratio testing detector [15]. By assuming Gaussian cover model and utilizing a better pixel variance estimator, security of [15] was enhanced in **Mi**nimizing the **P**ower of **O**ptimal **D**etector (MiPOD) [16].

In all the mentioned statistical model based methods, as a result of a non-constrained message probability distribution, embedding probabilities are calculated using numerically solvable equations. Therefore, their performances are not expressed as closed-form functions of payload. Having a closed-form detection error plays a critical role in understanding image steganography and also batch steganography in which the payload is spread across multiple objects.

Manuscript received November 5, 2018; revised April 8, 2019 and June 23, 2019; accepted June 27, 2019. Date of publication July 17, 2019; date of current version October 8, 2019. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Jiwu Huang. *(Corresponding author: Mehdi Sharifzadeh.)*

The authors are with the Department of Electrical and Computer Engineering, University of Illinois at Chicago, Chicago, IL 60607 USA (e-mail: mshari5@uic.edu).

Digital Object Identifier 10.1109/TIFS.2019.2929441

Batch steganography and pool steganalysis are the extensions of steganography and steganalysis where the message is spread in multiple objects and the detector jointly analyzes objects. These two concepts were introduced in [17] and highlighted as important open problems in [18]. Non-adaptive message spreading batch steganography was studied in [19]–[21]. Batch steganography for content-adaptive methods were introduced in [22] where a more suitable sub-bath of images are chosen for embedding. The results were further improved by spreading the payload among all the images of a batch in [23]. In all the proposed methods, the batch size is assumed to be infinity. In other words, the whole data-set is grouped into one batch. To the best knowledge of the authors, smaller batch sizes have never been studied in the literature.

In this work, our contribution is threefold:

1) For the first time, we model the hidden message as continuous Gaussian random variable and propose a novel Gaussian embedding technique by minimizing the detection error of three most common optimal hypothesis detectors simultaneously. Subsequently, the closed-form detection error as a function of payload is derived for such an embedder. The explained formulation is also extended to distortion minimization framework. As a result, the proposed embedding model can be applied not only utilizing residual variances estimated by any variance estimator used in model-based approaches such as MiPOD [16] and [15] but also using embedding costs calculated by any cost-based image steganography methods, such as HILL [9] and SUNIWARD [8]. In all the cases, the proposed method results in a better security comparing to the original embedding schemes.
2) Employing continuous hidden message in the formulation allows us to do $(2q + 1)$-ary embedding for any q by only changing the quantization levels. Therefore, we effortlessly investigate the effect of maximum pixel change (q) on security of image steganography within the adopted model. We conclude that the higher the q is the better the security will be, which is contrary to the common belief of executing small changes or altering only the least significant bit of pixels.
3) We obtain the closed-form detection error for image merging batch steganography with batch size M. Consequently, we prove that using higher batch size results in higher detection error in small payloads. However, for large enough payloads, using lower batch size is more secure. Based on this, we introduce a novel **Ada**ptive **B**atch size **I**mage **M**erging steganographer (*AdaBIM*) that merges images in batches with size M, where M depends on the payload. It outperforms the state-of-the-art batch steganography method based on empirical evaluations.

This paper includes the extended version of our preliminary work [24] with more novel experiments and comparisons, in addition to introducing a novel batch steganography method and mathematically proving its superiority, and it is organized as follows. Related works are provided in Sec. II. The statistical model for the cover and stego images are presented in Sec. III. Using the statistical model, a framework is developed for a hypothesis testing detector in Sec. IV-A. Three optimal decision strategies for such a detector are investigated in Sec. IV-B. Based on all these strategies, a novel Gaussian embedding model is proposed in Sec. V-A. In Sec. V-B, the impact of batch size is studied, and a new batching strategy, *AdaBIM*, is proposed and proven to be superior. Then, the results are further extended to distortion steganography framework in Sec. V-C which makes the Gaussian embedding model applicable to cost-based methods. The experimental results and conclusions are provided in Sec. VI and VII respectively.

II. Related Works

The state-of-the-art image steganography algorithms fall into two main categories: cost based and statistical model based methods. S-UNIWARD [8] and HILL [9] are two famous algorithms for cost based methods. In S-UNIWARD, the embedding distortions are calculated through directional filter banks [8]. HILL uses a high-pass filter to find noisy parts, followed by two low-pass filters for smoothing.

The first statistical model based steganography is HUGO [12] which defines distortion as a weighted sum of difference between SPAM feature vectors of a cover image and its stego version [11]. Another approach is proposed in [14] which models the cover image pixels by independent normally distributed variables, where the variances are computed using a proposed variance estimator. Then, the message is embedded in a ternary scheme in each pixel while minimizing the KL divergence between the cover and the stego message. Using a similar framework but with a generalized Gaussian statistical model for cover images, a better variance estimator, embedding quinary message in each pixel, and minimizing the detection error of an optimal hypothesis testing detector better results were achieved in [15]. Building upon the result of these two works, MiPOD [16] was proposed outperforming state-of-the-art cost based image steganography methods. In MiPOD, the cover is modeled as independent Gaussian random variables and the stego message is the result of embedding a ternary message in each cover pixel. The embedding is done in a way to minimize the power of a hypothesis testing detector. In contrast to the methods utilizing the KL divergence, this method does not require the assumption of small payload.

Batch steganography for non-adaptive message spreading techniques was studied in [19]–[21] showing that the message should be distributed evenly or concentrated in the fewest possible number of cover mediums depending on the payload. However, for content adaptive methods Zhao *et al.* showed that choosing a more suitable sub-batch of images to carry the whole message significantly improves security comparing to randomly choosing a sub-batch [22]. Further studies improved the performance by spreading the payload among all the images of a batch using three message spreading techniques, distortion limited sender (DiLS), detectability limited sender (DeLS), and image merging sender (IMS) [23]. Assuming only one batch containing all the images of a dataset, DiLS and DeLS spread the payload among them in a way to have the same distortion and KL divergence respectively, according to an adopted cover model. However, IMS, the

best performing technique, merges all the images together while the embedding algorithm distributes the payload among them. In other words, IMS treats all the pixels in a batch as though they belonged to one image similar to the approach we proposed in [25].

III. Statistical Models

In this section, the statistical models for the cover and the stego messages are described. Cover image pixels are modeled by independent Gaussian random variables. Subsequently, the distribution of the stego image pixels are derived by embedding a Gaussian message in each cover pixel.

The motivation of using a continuous random variable to model the discrete message arises because of the difficulty in solving this problem in the discrete space. We therefore propose to work in a continuous framework in which both the cover and the message are modeled by continuous random variables. Once the problem is solved in the continuous space, we discretize the derived solution to the original discrete model to obtain the desired results. We note that the discrete model could potentially be solved directly to provide the same (and possibly even superior) results. However, a direct closed-form solution for the discrete model is currently unknown and remains an open problem. Furthermore, we would like to have a unified probability framework where the cover and message distributions are consistent and remain unchanged once the message has been added to the cover in a spatial steganography scenario; i.e., we are limited to stable distributions, also known as Levy alpha-stable distributions, that are closed under linear transformation. Our interest is further focused on a random variable model among the stable distributions that is symmetric. It is known that a symmetric alpha-stable distribution can be viewed as a transform of zero-mean Gaussian random variables whose variance is drawn from a stable distribution (see, e.g., Section 3.2.2. in [26]). We therefore assume a Gaussian cover model as well as a Gaussian message model, which as a result of the central limit theorem has the added advantage of robustness to channel and noise degradation as well as hostile attacks (see, e.g., Section 1.2.1 in [26]).

A. Cover Model

Cover images are shown by $\mathbf{c} = [c_1, \ldots, c_n] \in \mathcal{P} = \{0, \ldots, 255\}^n$, where $\mathcal{P}$ is the set of all vector representation of 8-bit gray-scale images of size $n_1 \times n_2 = n$. Each c_i is modeled as an independent Gaussian variable, $\mathcal{N}(\mu_i, \omega_i^2)$, quantized to $\mathcal{P}$. Suppose $\hat{\mu}_i$ is an unbiased estimation of μ_i based on the rest of the image. Thus, the residual of the estimation, defined as $x_i = c_i - \hat{\mu}_i$, has a Gaussian distribution, $\mathcal{N}(0, \sigma_i^2)$, where σ_i^2 is greater than ω_i^2 as it includes both the pixel's variance (ω_i^2) and the estimation error. Assuming $\sigma_i \gg \Delta$, where Δ is the quantization step size equal to 1, the probability distribution of the i^{th} cover pixel residual is

$$p_{x_i}(k) \propto \frac{1}{\sigma_i \sqrt{2\pi}} \exp\left(\frac{-k^2}{2\sigma_i^2}\right). \tag{1}$$

Refer to [16] for more information regarding this model. This statistical model is violated in practice in smooth or saturated regions because of assuming unbounded pixels and $\sigma_i \gg \Delta$. However, our proposed method will avoid embedding in those regions anyway which is covered thoroughly in Sec. V-A.

B. Stego Model

Unlike the previous works which only considered discrete hidden message elements, we model them, m_i, as Gaussian random variables with variance β_i distributed according to

$$p_{m_i}(k) = \frac{1}{\beta_i \sqrt{2\pi}} \exp\left(\frac{-k^2}{2\beta_i^2}\right). \tag{2}$$

The stego image is the summation of the cover image with the stego message elements, i.e. $\mathbf{s} = \mathbf{c} + \mathbf{m}$. Hence, the i^{th} stego pixel residual is $y_i = x_i + m_i$, and based on (1) and (2), its probability distribution is derived as

$$p_{y_i}(k) \propto \frac{1}{\sqrt{2\pi(\sigma_i^2 + \beta_i^2)}} \exp\left(\frac{-k^2}{2(\sigma_i^2 + \beta_i^2)}\right), \tag{3}$$

with the assumption of unbounded quantization levels and $\sqrt{\sigma_i^2 + \beta_i^2} \gg \Delta$. The next section is devoted to find the proper β_is for achieving the best security for a payload limited sender.

IV. Hypothesis Testing

The problem of steganography in a single image with a fixed payload can be formulated as constraint maximization of detection error of the warden [15], [16] given by

$$\begin{cases} \underset{(\beta_1, \ldots, \beta_n)}{\arg\max}\, \mathrm{P_E}(\beta_1, \ldots, \beta_n) \\ \sum_{i=1}^{n} \mathrm{H}(p_{m_i}) = np \end{cases}, \tag{4}$$

where $\mathrm{P_E}$ is the detection error derived in the following section, $\mathrm{H}(p_{m_i})$ is the entropy of a random variable with probability distribution p_{m_i} in natural unit of information (nats) and p is the relative payload in nats per pixel.

A. Likelihood Ratio Test Framework

To derive the detection error of the steganalyzer which is a function of the message variances, i.e. $\mathrm{P_E}(\beta_1, \ldots, \beta_n)$, we assume that the steganalyzer utilizes a likelihood ratio test (LRT) to do a binary hypothesis testing between $\mathcal{H}_0$ and $\mathcal{H}_1$, representing the cases of receiving a cover or a stego image respectively. We assume the worst case scenario of an omniscience steganalyzer who knows all the β_is and σ_is. Lets assume that $\mathbf{r} = [r_1, \ldots, r_n]$ are the residuals of the received image's pixels and they are statistically independent. As a consequence, the likelihood ratio for the whole image can be written as $\prod_{i=1}^{n} \Lambda_i$ in which Λ_i, the likelihood ratio for the i^{th} pixel, can be written based on (1) and (3) as follows

$$\Lambda_i = \frac{p_{y_i}(r_i)}{p_{x_i}(r_i)} = \sqrt{\frac{\sigma_i^2}{\sigma_i^2 + \beta_i^2}} \exp\left(\frac{-r_i^2}{2} \frac{-\beta_i^2}{\sigma_i^2(\sigma_i^2 + \beta_i^2)}\right). \tag{5}$$

As a result the natural logarithm of the likelihood ratio is

$$\ln \Lambda_i = \ln \sqrt{\frac{\sigma_i^2}{\sigma_i^2 + \beta_i^2}} + \frac{\beta_i^2}{2\sigma_i^2(\sigma_i^2 + \beta_i^2)} r_i^2, \tag{6}$$

where r_i has a normal distribution. Hence, r_i^2 multiplied by a constant term results in a Gamma distribution. Therefore, the natural logarithm of the likelihood ratio, $\ln \Lambda_i$, is a constant term plus a random variable with $\Gamma(k_i, \theta_i)$ distribution, where k_i and θ_i are the shape and scale parameters respectively. Parameter θ_i depends on the variance of r_i, in other words, whether r_i is distributed according to (1) or (3). In order to derive k_i and θ_i for both hypotheses, we employ Taylor series expansion of $\ln(1+x)$ where $x = \beta_i^2/\sigma_i^2$, assuming $x < 1$

$$\ln\left(\frac{\sigma_i^2}{\sigma_i^2+\beta_i^2}\right) = -\ln\left(1+\frac{\beta_i^2}{\sigma_i^2}\right) \approx -\frac{\beta_i^2}{\sigma_i^2} + \frac{1}{2}\left(\frac{\beta_i^2}{\sigma_i^2}\right)^2. \quad (7)$$

If $x = -\beta_i^2/(\sigma_i^2+\beta_i^2)$, the approximation is

$$\ln\left(\frac{\sigma_i^2}{\sigma_i^2+\beta_i^2}\right) \approx -\frac{\beta_i^2}{\sigma_i^2+\beta_i^2} - \frac{1}{2}\left(\frac{\beta_i^2}{\sigma_i^2+\beta_i^2}\right)^2, \quad (8)$$

which can be further simplified using Taylor series of $\frac{x}{1+x}$

$$\frac{\beta_i^2}{\sigma_i^2+\beta_i^2} \approx \frac{\beta_i^2}{\sigma_i^2} \quad (9)$$

Given $\mathcal{H}_0$, the Gamma distribution parameters are $k = 0.5$ and $\theta_i = \beta_i^2/(\sigma_i^2+\beta_i^2)$. The resulted mean and variance of the natural logarithm of the likelihood ratio are:

$$\begin{cases} \mathrm{E}^{\mathcal{H}_0}_{r_i|\sigma_i,\beta_i}[\ln \Lambda_i] = \ln\left(\sqrt{\dfrac{\sigma_i^2}{\sigma_i^2+\beta_i^2}}\right) + k\theta_i \\ \qquad\qquad \approx \dfrac{-1}{4}\left(\dfrac{\beta_i^2}{\sigma_i^2+\beta_i^2}\right)^2 \approx \dfrac{-1}{4}\left(\dfrac{\beta_i^2}{\sigma_i^2}\right)^2, \\ \mathrm{Var}^{\mathcal{H}_0}_{r_i|\sigma_i,\beta_i}[\ln \Lambda_i] = k\theta_i^2 \approx \dfrac{1}{2}\left(\dfrac{\beta_i^2}{\sigma_i^2}\right)^2 \end{cases} \quad (10)$$

where the approximations are based on (8) and (9). However, for $\mathcal{H}_1$, $k = 0.5$, $\theta_i = \beta_i^2/\sigma_i^2$ and the mean and variance are

$$\begin{cases} \mathrm{E}^{\mathcal{H}_1}_{r_i|\sigma_i,\beta_i}[\ln \Lambda_i] = \ln\left(\sqrt{\dfrac{\sigma_i^2}{\sigma_i^2+\beta_i^2}}\right) + k\theta_i \\ \qquad\qquad \approx \dfrac{1}{4}\left(\dfrac{\beta_i^2}{\sigma_i^2}\right)^2 \\ \mathrm{Var}^{\mathcal{H}_1}_{r_i|\sigma_i,\beta_i}[\ln \Lambda_i] = k\theta_i^2 = \dfrac{1}{2}\left(\dfrac{\beta_i^2}{\sigma_i^2}\right)^2 \end{cases}, \quad (11)$$

where the approximation is based on (7). For large enough number of pixels (n), the following theorem can be used to approximate the probability distribution of $\sum_{i=1}^n \ln(\Lambda_i)$.

Theorem 1: Asymptotic Sum of Gamma Random Variables Suppose $X_1, \cdots, X_n$ are all independently distributed by Gamma with shape k, but with scaling parameters $\theta_1, \cdots \theta_n$ respectively. If all θ's are bounded, the probability distribution of the following summation, where $a_1, \ldots, a_n$ are some constants, converges to normal distribution as shown below.

$$\sum_{i=1}^n (X_i + a_i) \xrightarrow{d} \mathcal{N}\Big(\sum_{i=1}^n (k\theta_i + a_i), k\sum_{i=1}^n \theta_i^2\Big) \quad (12)$$

See Appendix A for the proof. Thus, the probability distribution of $\sum_{i=1}^n \ln(\Lambda_i)$, for large enough n, can be approximated with the following distributions, based on (10) and (11):

$$\begin{cases} \mathcal{N}(\dfrac{-1}{4}\alpha,\ \dfrac{1}{2}\alpha) & \text{if } \mathcal{H}_0 \text{ is true,} \\ \mathcal{N}(\dfrac{+1}{4}\alpha,\ \dfrac{1}{2}\alpha) & \text{if } \mathcal{H}_1 \text{ is true,} \end{cases} \quad (13)$$

where α is as follows

$$\alpha = \sum_{i=1}^n \left(\frac{\beta_i^2}{\sigma_i^2}\right)^2. \quad (14)$$

The result shown in (13), is also consistent with the shift hypothesis, which states embedding only affects the mean of the detector's output [17]. Here is the logarithm of the LRT

$$\sum_{i=1}^n \ln(\Lambda_i) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma, \quad (15)$$

where γ is the decision threshold. In the next section, we will discuss three different optimal decision criteria for deriving the decision boundary, γ, and consequently the detection error of the warden $\mathrm{P_E}(\beta_1, \ldots, \beta_n)$.

B. Optimal Decision Strategies

To derive the detection error of steganalyzer, $\mathrm{P_E}$, we employ the most common optimality criteria for hypothesis testing, Bayes, minimax, and Neyman-Pearson. All these strategies utilize a likelihood ratio test (LRT), but with different decision boundaries. In this section, we show that they all result in the same simplification of $\mathrm{P_E}(\beta_1, \ldots, \beta_n)$.

1) Bayes Criterion: Let's denote the prior probabilities of $\mathcal{H}_0$, and $\mathcal{H}_1$ with P_0, and P_1 respectively. The event and the cost associated with the decision $\mathcal{H}_i$ given that the true hypothesis is $\mathcal{H}_j$ are shown with D_{ij} and C_{ij} respectively. The risk function is defined as

$$R = \sum_{j=0}^{1}\sum_{j=0}^{1} P_i C_{ji}\ p(D_{ji}). \quad (16)$$

The Bayes decision boundary, γ_{Bayes}, which minimizes the risk defined in (16), is given by

$$\gamma_{\text{Bayes}} = \ln\left(\frac{P_0(C_{10}-C_{00})}{P_1(C_{01}-C_{11})}\right). \quad (17)$$

Consequently, the expected value of the detection error (summation of false alarm and missed detection) is given by

$$\mathrm{P_{E_{Bayes}}} = \phi\left(\frac{\gamma - \frac{\alpha}{4}}{\sqrt{\frac{\alpha}{2}}}\right)P_1 + \phi\left(\frac{-\gamma - \frac{\alpha}{4}}{\sqrt{\frac{\alpha}{2}}}\right)P_0, \quad (18)$$

where ϕ is the cumulative distribution of standard normal distribution, i.e. $\phi(x) = (2\pi)^{-0.5}\int_{-\infty}^{x} \mathrm{e}^{-x^2/2}dx$. If $P_0 = P_1$, which is frequently used for evaluating the security in practical steganalysis, derivative of (18) with respect to α is negative. This shows that regardless of the γ's value in (17), $\mathrm{P_{E_{Bayes}}}$ is a monotonic decreasing function of α in case of equal priors. As a result, a steganographer can minimize α instead of maximizing the $\mathrm{P_{E_{Bayes}}}$.

2) Minimax Criterion: In a minimax criterion, the decision rule is the same as the Bayes' rule but for the least favorable priors. The least favorable prior probability of $\mathcal{H}_1$, P_1^L, is defined as the prior probability that maximizes the risk function in (16). In case of having differentiable R, it is proven that P_1^L can be 0, 1, or the solution of $R_0 = R_1$. The first two cases will result in $\gamma = \pm\infty$. Therefore, we will consider the third case, which is called an equalizer rule. To find the threshold of the equalizer rule, we need to solve the following equation

$$C_{11}\Big(1-\phi\Big(\frac{\gamma-\alpha/4}{\sqrt{\alpha/2}}\Big)\Big)+C_{01}\phi\Big(\frac{\gamma-\alpha/4}{\sqrt{\alpha/2}}\Big) = C_{00}\Big(1-\phi\Big(\frac{-\gamma-\alpha/4}{\sqrt{\alpha/2}}\Big)\Big)+C_{10}\phi\Big(\frac{-\gamma-\alpha/4}{\sqrt{\alpha/2}}\Big). \quad (19)$$

By assuming symmetric costs, $C_{00} = C_{11}$ and $C_{01} = C_{10}$, $\gamma = 0$ is the solution that has the minimum expected risk over all possible prior distributions, and its error is given by

$$\mathrm{P_{E_{minimax}}} = \phi\Big(\frac{-\alpha/4}{\sqrt{\alpha/2}}\Big) = \phi\Big(-\sqrt{\frac{\alpha}{8}}\Big), \quad (20)$$

which is a monotonically decreasing function of α.

3) Neyman-Pearson Criterion: In Bayesian formulation, the overall expected cost is minimized to find the optimal strategy. In minimax criterion, the case where the prior probabilities are unknown is discussed and the optimal decision is found based on the cost of each decision and the calculated least favorable priors. However, in practice, there might not be any cost defined for each decision. Therefore, we utilize a Neyman-Pearson formulation to find the optimal decision and its corresponding error. In this framework, the detector maximizes the probability of detection, $p(D_{11})$, while keeping the probability of false alarm bounded, $p(D_{10}) \leq l$, where l is the significance level of the test. According to the Neyman-Pearson Lemma, an optimal decision rule exists for any $p(D_{10}) = l$. As a consequence, the decision threshold for such an optimal decision rule can be calculated as

$$\gamma_{\text{Neyman-Pearson}} = -\sqrt{\frac{\alpha}{2}}\phi^{-1}(l) - \frac{\alpha}{4}. \quad (21)$$

This results in the following total probability of error:

$$\mathrm{P_{E_{Neyman\text{-}Pearson}}} = \phi\left(-\phi^{-1}(l) - \sqrt{\frac{\alpha}{2}}\right)P_1 + lP_0. \quad (22)$$

The same as the two previously discussed criteria, this criterion also results in an error which is a monotonically decreasing function of α. Based on this behavior, the problem formulation in (4) can be simplified and will be discussed in the next section. From now on, for simplicity's sake, we employ the minimax error calculated in this section for the warden's detection error, $\mathrm{P_E}(\beta_1, \ldots, \beta_n)$, as it does not depend on any variable other than α.

V. Gaussian Embedding Model

In this section, a novel image steganography method is introduced based on maximizing the detection error of three optimal detectors shown in previous section. First, the methodology is derived for embedding in a single image, then it is extended to batch steganography. Subsequently, based on the theoretical findings for batch steganography, a new algorithm, *AdaBIM*, is proposed. Last but not least, the formulation is extended to distortion image steganography framework which makes the algorithm applicable in case of having cost of embedding in each pixel instead of the residual variance.

A. Single Image Steganography

The detection error, $\mathrm{P_E}(\beta_1, \ldots, \beta_n)$, is shown to be a monotonic decreasing function of α. Thus, in the proposed Gaussian embedding scenario, the problem of optimal embedding for a fixed payload, shown in (4), can be written as

$$\begin{cases} \underset{(\beta_1,\ldots,\beta_n)}{\arg\min}\ \alpha \equiv \underset{(\beta_1,\ldots,\beta_n)}{\arg\min} \sum_{i=1}^{n} \left(\frac{\beta_i^2}{\sigma_i^2}\right)^2 \\ \sum_{i=1}^{n} \mathrm{H}(p_{m_i}) = np \end{cases} \quad (23)$$

where p is the relative payload per pixel in nats. Shannon entropy of the hidden message elements (m_i), a Gaussian random variable with variance β_i^2, can be written as:

$$\mathrm{H}(p_{m_i}) = \frac{1}{2}\ln(2\pi\,\mathrm{e}\beta_i^2) \quad (24)$$

The solution of (23) using Lagrangian multipliers is the solution of the following equation:

$$\frac{\partial}{\partial\beta_i}\left(\sum_{j=1}^{n}\left(\frac{\beta_j^2}{\sigma_j^2}\right)^2 + \lambda\Big(np - \frac{1}{2}\sum_{j=1}^{n}\ln(2\pi\,\mathrm{e}\beta_j^2)\Big)\right) = 0, \quad (25)$$

for $i = 1, \ldots, n$, where λ is the Lagrangian multiplier that is calculated using the payload constraint in (23), and thus will be shown as a function of the payload, p. The solution of (23) is as follows

$$\beta_i^* = \frac{\sqrt[4]{\lambda(p)}}{\sqrt{2}}\sigma_i \quad \text{for } i = 1, \ldots, n \quad (26)$$

To achieve optimal security, the message's variance, β_i^2, should be proportional to the pixel's residual variance, σ_i^2. In other words, in a noisy or textured region where residual variances are high, embedding variances will be high as well. On the other hand, if a pixel's residual variance is zero, which means it belongs to a smooth region, no embedding takes place. Now that the distribution of the continuous hidden message is determined, the actual message is computed by quantizing the Gaussian distributed message to $\mathcal{Q} = \{-q, \ldots, -1, 0, 1, \ldots, +q\}$, for any natural number q.

Here is the explanation of the proposed algorithm steps. First, in order to calculate the message variances, β_i, the pixel's residual variance, σ_i, is calculated using any variance estimator such as the methods proposed in [15], [16]. Then, by assuming a $(2q+1)$-ary embedding scenario where the message is a Gaussian random variable with variance β_i quantized to $\mathcal{Q} = \{-q, \ldots, +q\}$, the following system of equations with $n+1$ equations and variables, $\beta_1, \ldots, \beta_n$ and λ,

is solved using Newton–Raphson method.

$$\begin{cases} \beta_i^* = \dfrac{\sqrt[4]{\lambda(p)}}{\sqrt{2}}\sigma_i \quad \text{for } i = 1, \ldots, n \\ -\displaystyle\sum_{i=1}^{n}\sum_{k=-q}^{q}(p_{m_i}(k)\ln p_{m_i}(k)) = np \end{cases} \tag{27}$$

where p is the relative payload in nats per pixel and p_{m_i}, the probability distribution of m_i, is given by

$$p_{m_i}(k) = \frac{\phi(\frac{k+0.5}{\beta_i}) - \phi(\frac{k-0.5}{\beta_i})}{\phi(\frac{q+0.5}{\beta_i}) - \phi(\frac{-q-0.5}{\beta_i})}, \quad \forall k \in \{-q, \ldots, +q\}, \tag{28}$$

which is a quantized truncated Gaussian. In other words, $p_{m_i}(k)$ is the probability of changing the i^{th} pixel by k. For implementing the proposed embedding technique by syndrome-trellis codes [6], we need to find the embedding costs for all the pixels. Embedding cost, $\rho_i(k)$, is defined as the amount of distortion added to image by changing the i^{th} pixel by k. These costs are calculated by solving the following system of equations, having Gibbs form [7] for all pixels.

$$p_{m_i}(k) = \mathrm{e}^{-\rho_i(k)} / \sum_{d=-q}^{q} \mathrm{e}^{-\rho_i(d)}, \tag{29}$$

for $\forall i \in \{1, \ldots, n\}, \forall k \in \{-q, \ldots, q\}$. There are $n \times q$ equations and variables by assuming symmetric costs, and $\rho_i(0) = 0, \ \forall i \in \{1, \ldots, n\}$. Note that finding the costs using Eq. (29) guarantees that by increasing the computational complexity, the coding loss can become arbitrarily small. To avoid rapid increase of complexity and any loss of performance for q values higher than 1, the actual embedding can be done using multi-layered STCs schemes which employs a layered-construction to decompose the non-binary case into several binary cases [6]. Refer to the mentioned work for more information regarding the time complexity and the coding loss of such coding scheme. However in this study, the same as all the other conceptual studies, the coding process is disregarded and the embedding process is simulated by altering the image according to the probabilities shown in (28). The pseudo-code of the proposed embedding model is shown in Fig. 1.

The steganalyzer detection error for such an embedder can be computed based on (20) and (26). In order to get that, the closed-form expression of the Lagrangian multiplier, $\lambda(p)$, is needed. By substituting (26) in the payload constraint of (23) and utilizing (24), the Lagrangian multiplier is given by

$$\lambda(p) = \frac{\mathrm{e}^{4p}}{\left(\pi \mathrm{e} \sqrt[n]{\prod_{i=1}^{n} \sigma_i^2}\right)^2}, \tag{30}$$

which is a monotonically increasing function of payload as expected. As a result, all the message variances, β, are monotonically increasing functions of the payload as well. Note that based on the assumption of all residual variances being much greater than 1, $\sigma \gg 1$, for very small payloads, $p \ll 1$, lambda is very small, $\lambda \ll 1$. In addition, for large payloads, $p \to \infty$, lambda also approaches infinity. In the following section, based on these asymptotic behaviors, we compare the security of different batch sizes in various payloads.

Input: $\mathbf{c}$ = Cover Image, p = Payload, q, Hidden Message
Output: $\mathbf{s}$ = Stego Image

1: Compute all the pixel residual variances σ_i or embedding costs ρ_i for each cover pixel c_i.
2: **if** using residual variances, σ_i, for embedding **then**
3: Solve (27) using Newton-Raphson method to find λ.
4: Calculate all β_i values by (26).
5: **else if** using embedding costs, ρ_i, for embedding **then**
6: Substitute the first equation in (27) with (41), then solve it using Newton-Raphson method to find λ.
7: Calculate all β_i values by (41).
8: **end if**
9: Determine all $p_{m_i}(k)$ values for all k and i by (28).
10: Encode the hidden message according to the computed change probabilities, p_{m_i}, to get $\mathbf{m} = [m_1, \ldots, m_n]$.
11: Generate the stego image by $\mathbf{s} = \mathbf{c} + \mathbf{m}$.

Fig. 1. Pseudo-code for gaussian embedding model.

Based on (26) and the definition of α in (14), α is given by

$$\alpha^* = \sum_{i=1}^{n}\left(\frac{\beta_i^{*2}}{\sigma_i^2}\right)^2 = \frac{n\lambda(p)}{4}, \tag{31}$$

which results in the following error in detection for the whole image using (20) and (30),

$$\mathrm{P_E} = \phi\left(-\sqrt{\frac{n\lambda(p)}{32}}\right) = \phi\left(-\sqrt{\frac{n}{32}} \cdot \frac{\mathrm{e}^{2p}}{\pi \mathrm{e} \sqrt[n]{\prod_{i=1}^{n} \sigma_i^2}}\right). \tag{32}$$

It can be concluded that the geometric mean of residual variances, $\sqrt[n]{\prod_{i=1}^{n} \sigma_i^2}$, is a suitability measure of the image for steganography since for a fixed payload, the greater it is the higher the detection error is. In addition, an image with higher residual variances (having noisier regions) has a higher suitability measure as expected.

To calculate the average detection error for N images, we assume all the images have the same number of pixels, n, for simplicity. Thereby, the closed-form expression for average detection error of the Gaussian embedding scheme is

$$\mathrm{P_E}(M = 1, N, p) = \frac{1}{N}\sum_{l=1}^{N}\phi\left(-\sqrt{\frac{n\lambda_l(p)}{32}}\right), \tag{33}$$

where $\lambda_l(p)$ is the Lagrangian multiplier shown in (30) for the l^{th} image and M is the batch size which is 1 as no batching took place. In the next section, we discuss greater batch sizes.

B. Adaptive Batch Size Image Steganography

The problem of optimizing the distribution of a fixed size message among pixels of a single image is discussed in the previous section and the closed-form expression for detection error is derived. In this section, the results are extended to batch steganography in which the message is spread in multiple images. The state-of-the-art batch steganography method, image merging sender (IMS), batches all the images of a

dataset into one group [23]. In this section, we investigate the case when images are batched in groups of size M. Therefore, there are N/M batches of images in a dataset with N images. Without loss of generality, we assume the l^{th} batch contains images with indexes $(l-1)M, \ldots, lM-1$. We use IMS for spreading $n \cdot M \cdot p$ nats among M images in each batch [23], [25]. This means that all the images in each batch are merged together and treated as one image. Thus, formulation is the same as (23) except that the number of pixels is $n \cdot M$ instead of n. Therefore, the solution is similar to the solution of (23) shown in (26) and it is given by

$$\beta_{ij}^{*} = \frac{\sqrt[4]{\lambda_l^{(M)}(p)}}{\sqrt{2}}\sigma_{ij}, \quad \forall i \in \{1, \ldots, n\} \tag{34}$$

and $\forall j \in \{(l-1)M, \ldots, lM-1\}$, where σ_{ij} is the variance of the i^{th} pixel of j^{th} image, and $\lambda_l^{(M)}$ is the Lagrangian multiplier for the l^{th} batch derived similar to (30) as

$$\lambda_l^{(M)}(p) = \frac{\mathrm{e}^{4p}}{\left(\pi \mathrm{e} \sqrt[M]{\prod_{j=(l-1)M}^{lM-1} \sqrt[n]{\prod_{i=1}^{n} \sigma_{ij}^2}}\right)^2}. \tag{35}$$

Based on (35) and (24), payload of the j^{th} image is

$$p_j = np + \frac{n}{2} \ln\left(\frac{\sqrt[n]{\prod_{i=1}^{n} \sigma_{ij}^2}}{\sqrt[M]{\prod_{k=(l-1)M}^{lM-1} \sqrt[n]{\prod_{i=1}^{n} \sigma_{ik}^2}}}\right), \tag{36}$$

which shows that in an image with suitability measure, geometric mean of residual variances, greater than the suitability measure of the whole batch, more information than the average payload, $n \cdot p$ nats per image, is embedded. Similarly, the payload of an image with suitability measure smaller than the batch's is smaller than the average payload. This results in all the images in the same batch having equal detection error.

Based on (33) and (35), the average detection error for the whole database for the proposed embedding can be written as:

$$\begin{aligned} \mathrm{P_E}(M, N, p) &= \frac{1}{N} \sum_{l=1}^{N/M} \sum_{j=(l-1)M}^{lM-1} \phi\left(-\sqrt{n\lambda_l^{(M)}(p)/32}\right) \\ &= \frac{M}{N} \sum_{l=1}^{N/M} \phi\left(-\sqrt{n\lambda_l^{(M)}(p)/32}\right) \end{aligned} \tag{37}$$

In other words, equation (37) is the security measure of the algorithm for batch size M and payload p. The following theorem is needed to compare the security of various M's.

Theorem 2: Given any powers of two, M and N, where $2M$ *is less or equal than N, the following statements are true.*

(i) $P_E(M, N, p) < P_E(2M, N, p) \quad p \ll 1$
(ii) $P_E(M, N, p) > P_E(2M, N, p) \quad p \to \infty$

See Appendix B for the proof. Based on this theorem, for payloads much smaller than 1, sorted batch sizes according to their detection error in an ascending order are $1, 2, 4, 8, \ldots, N$. However, for large enough payloads this ranking is totally flipped and $M = 1$ has the highest detection error. Theorem 2 is consistent with the experiments, not only for the Gaussian version of HILL, MiPOD, and SUNIWARD but also their original versions. This flip happens in payloads between 0.75 and 1.5 bits per pixel depending on the embedding algorithm.

Based on theorem 2, we propose employing different batch sizes in different payloads. This results in a novel **Ada**ptive **B**atch size **I**mage **M**erging steganographer (*AdaBIM*). In *AdaBIM*, the batch size is N for payloads close to zero, then it gradually decreases as the payload increases until it reaches 1. This is done based on empirical results. Based on (36), it is observed that *AdaBIM* spreads the payload non-uniformly among all the images according to their suitability measure (more payload in images with more textured regions) for payloads near zero. However, for large payloads where the batch size is 1, the payload is spread uniformly among images.

The state-of-the-art batch steganography method (IMS) uses $M = N$ for all the payloads. Therefore, *AdaBIM* performs as well as IMS in payloads near zero. However, as the payload increases, we proved *AdaBIM* outperforms IMS. We also demonstrate this by comparing their empirical performances against the state-of-the-art steganalysis method in Sec. VI.

C. Extension to Cost Based Methods

Cost based steganography methods calculate embedding cost instead of residual variances [8], [9], [12]. In these methods, the steganographer tries to minimize the expected value of a distortion function, $\mathrm{D}(\mathbf{s}, \mathbf{c})$, where $\mathbf{s}$ and $\mathbf{c}$ are the stego and cover images respectively. To adapt our framework to be applicable for these methods and boost their performance, we define the distortion to be the expected value of the absolute difference between the pixel intensities the same as prior arts. As a result, the steganography problem for a payload limited sender can be written as:

$$\begin{cases} \underset{(\beta_1,\ldots,\beta_n)}{\arg\min}\ \mathrm{E}[\mathrm{D}(\mathbf{s}, \mathbf{c})] = \underset{(\beta_1,\ldots,\beta_n)}{\arg\min} \sum_{i=1}^{n} \mathrm{E}_{m_i|\beta_i}\left[\rho_i |s_i - c_i|\right] \\ \sum_{i=1}^{n} \mathrm{H}(p_{m_i}) = np, \end{cases} \tag{38}$$

where ρ_i is the cost of embedding ± 1 in the i^{th} pixel which can be calculated by any of the mentioned algorithms [8], [9], [12]. Assuming the same Gaussian embedding scenario where $m_i \sim \mathcal{N}(0, \beta_i^2)$, the expected value of the distortion is

$$\mathrm{E}_{m_i|\beta_i}\left[\rho_i |s_i - c_i|\right] = \mathrm{E}_{m_i|\beta_i}\left[\rho_i |m_i|\right] = \rho_i \beta_i \sqrt{\frac{2}{\pi}}. \tag{39}$$

Using Lagrangian multipliers approach, the problem is translated to

$$\frac{\partial}{\partial \beta_i}\left(\sum_{j=1}^{n}\left(\rho_j \beta_j \sqrt{\frac{2}{\pi}}\right) + \lambda\left(np - \frac{1}{2}\sum_{j=1}^{n} \ln(2\pi \mathrm{e} \beta_j^2)\right)\right) = 0. \tag{40}$$

The solution to (40) is

$$\beta_i^{*} = \frac{\lambda(p)}{\rho_i}\sqrt{\frac{\pi}{2}}, \tag{41}$$

where λ is the Lagrangian multiplier which can be calculated using the payload constraint in (38). The rest of the embedding

TABLE I

DETECTION ERROR COMPUTED BY STEGANALYSIS USING MAXSRMD2 FEATURES IN DIFFERENT PAYLOADS RANGING FROM 0 TO 1 BPP FOR THE PROPOSED GAUSSIAN VERSION OF THE HILL ALGORITHM WITH DIFFERENT q VALUES IN A $(2q+1)$-ary EMBEDDING SCENARIO

q	payload = **0.01**	**0.05**	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**	**0.75**	**1**
1	.499±.0025	.488±.0018	.464±.0031	.412±.0033	.351±.0026	.296±.0035	.240±.0029	.132±.0025	.064±.0028
2	.498±.0023	.488±.0018	.467±.0020	.415±.0025	.359±.0028	.303±.0034	.253±.0029	.150±.0035	.084±.0028
3	.499±.0033	.489±.0019	.469±.0025	.417±.0027	.361±.0035	.306±.0040	.256±.0044	.154±.0027	.091±.0034
4	.500±.0030	.489±.0018	.469±.0040	.418±.0027	.361±.0024	.307±.0036	.257±.0050	.155±.0024	.092±.0030
5	.500±.0017	.491±.0027	.469±.0033	.417±.0021	.364±.0036	.309±.0034	.256±.0023	.157±.0033	.094±.0032
6	.500±.0026	.490±.0027	.468±.0029	.418±.0023	.363±.0037	.309±.0034	.258±.0036	.158±.0032	.094±.0028

TABLE II

DETECTION ERROR COMPUTED BY STEGANALYSIS USING MAXSRMD2 FEATURES IN PAYLOADS RANGING FROM 0 TO 1 BPP FOR THREE IMAGE STEGANOGRAPHY METHODS AND THEIR PROPOSED GAUSSIAN VERSIONS WITH DIFFERENT q VALUES IN A $(2q+1)$-ary EMBEDDING SCENARIO

Embedding	q	payload = **0.01**	**0.05**	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**	**0.75**	**1**
G-HILL	3	**.499±.0033**	**.489±.0019**	**.469±.0025**	**.417±.0027**	**.361±.0035**	**.306±.0040**	**.256±.0044**	**.154±.0027**	**.091±.0034**
HILL	3	.496±.0014	.486±.0026	.461±.0032	.411±.0023	.353±.0036	.298±.0029	.243±.0030	.142±.0024	.082±.0023
G-HILL	1	.499±.0025	.488±.0018	.464±.0031	.412±.0033	.351±.0026	.296±.0035	.240±.0029	.132±.0025	.064±.0028
HILL	1	.499±.0030	.488±.0019	.464±.0023	.409±.0032	.346±.0029	.292±.0034	.234±.0023	.130±.0030	.062±.0024
G-MiPOD	3	.498±.0023	.483±.0017	.461±.0024	.407±.0023	.351±.0027	.295±.0036	.241±.0034	.145±.0026	.083±.0020
MiPOD	3	.497±.0028	.480±.0019	.453±.0024	.402±.0019	.347±.0030	.289±.0029	.241±.0019	.151±.0044	.092±.0020
G-MiPOD	1	.497±.0030	.482±.0024	.457±.0014	.401±.0023	.346±.0033	.287±.0032	.233±.0024	.124±.0032	.062±.0024
MiPOD	1	.498±.0026	.479±.0017	.451±.0030	.397±.0017	.339±.0018	.279±.0034	.229±.0026	.131±.0031	.066±.0024
G-SUNIWARD	3	.500±.0026	.484±.0036	.456±.0027	.392±.0038	.324±.0025	.263±.0036	.214±.0032	.123±.0030	.067±.0024
SUNIWARD	3	.500±.0025	.482±.0030	.448±.0024	.381±.0019	.313±.0040	.256±.0042	.205±.0033	.120±.0030	.068±.0023
G-SUNIWARD	1	.499±.0015	.485±.0011	.453±.0023	.386±.0025	.319±.0028	.256±.0027	.208±.0026	.109±.0023	.051±.0022
SUNIWARD	1	.499±.0031	.483±.0017	.444±.0023	.373±.0026	.298±.0033	.239±.0032	.187±.0036	.098±.0025	.042±.0018

approach is the same as it is explained in Sec. V-A. The proposed Gaussian steganography method can be applied in both cases of having pixel residual variances and embedding costs. This makes our approach a universal technique for improving all the recent spatial image steganography methods.

VI. EXPERIMENTS AND DISCUSSIONS

Throughout this paper, BOSSbase 1.01 database with $10k$ gray-scale 512×512 pixels images [27] is used. To show the performance of each method, the average detection error, defined as the average of false positive and negative rates, is reported. It is evaluated by an ensemble classifier steganalyzer [28] with a 10-fold cross validation, trained on maxSRMd2 feature vectors with $34,671$ elements [29]. 4096 and 4096 images are chosen randomly as training/validation and testing set respectively, since throughout this paper we assumed the size of dataset to be power of 2 and 4096 is the largest power of 2 less than $5k$ (half of the images in the dataset).

Three state-of-the-art content-adaptive image steganography methods: HILL [9], MiPOD [16], and SUNIWARD [8] are used for evaluations with settings that are shown in the original papers to achieve the best security. HILL algorithm is used with a 3×3 Ker-Bohme high-pass filter and a 3×3 and a 15×15 averaging filters as low-pass filters [9]. MiPOD method utilizes a two dimensional Wiener filter with width, $w = 2$, and medium blocks, which means $p = 9$ and $l = 9$ [16]. SUNIWARD algorithm is used with $\sigma = 1$ [30]. For the 7-ary version of HILL, and SUNIWARD, the cost of adding $\pm d$ to the i^{th} pixel is the distortion introduced by changing only the i^{th} pixel by $\pm d$ according to distortion function of the corresponding algorithm. For 7-ary version of MiPOD, the probability of changes are computed by employing a 3×3 Fisher information matrix following the same framework used in [15] for 5-ary embedding.

Embedding in saturated pixels are shown to drop the performance of steganography methods [31], therefore in all of the experiments, we avoid embedding in saturated pixels as well as the pixels that will be saturated after embedding. For example, in a 7-ary embedding scheme, all the pixels having the following intensities are avoided: $0, 1, 2, 253, 254, 255$.

In all the batch steganography experiments, the largest batch size tested is 128. The batch sizes greater than 128 are not tried due to computational limitations. We believe this batch size is enough to show sufficient proof for the claimed statements.

A. Determining Maximum Pixel Change (q)

The Gaussian embedding technique proposed in Sec. V-A has a controlling parameter q which represents the maximum changes of the cover pixels during embedding. To find the optimal q, we have evaluated the performance of HILL's Gaussian version derived in (41) with different settings, $q = 1, \ldots, 6$, for various payloads between 0 and 1 bits per pixel (bpp). The results are presented in Table I. It is observed that for the Gaussian embedding model, the larger the q is, the higher the security is. For example, comparing G-HILL with $q = 1$ and $q = 3$ shows that the former performs significantly better for payloads higher or equal than 0.1 bpp. Similar conclusion can be drawn from Table II for G-MiPOD and G-SUNIWARD. However, the complexity of the coding algorithm will increase

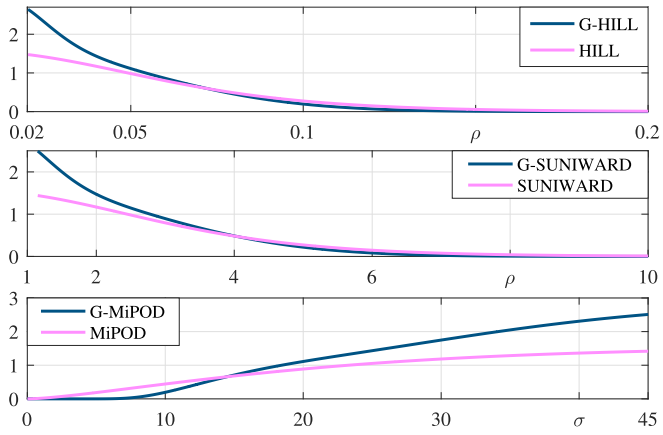

Fig. 2. Bits of information embedded in pixels of a single image (1.pgm) versus pixels embedding cost or residual variance for the proposed Gaussian versions and original versions of HILL (top), SUNIWARD (middle), and MiPOD (bottom) when embedding a payload of 0.3 bpp.

if q increases [6]. Furthermore, the results in Table I also suggest that q values greater than 3 do not result in considerably better security comparing to q equal to 3. Thus, we choose $q = 3$ for the rest of the experiments resulting in septenary (7-ary) embedding scenarios unless mentioned otherwise.

B. Comparison of Gaussian Embedding With Prior Arts

In this section, we compare the security of three stat-of-the-art image steganography methods, HILL [9], MiPOD [16], and SUNIWARD [8], with their proposed Gaussian versions. We conduct experiments on all the methods with both ternary ($q = 1$) and septenary ($q = 3$) embedding for various payloads between 0 and 1 bpp. The results are presented in Table II. For the proposed Gaussian versions of these algorithms, we use a prefix of G, e.g. G-HILL. G-HILL and G-SUNIWARD use the embedding cost calculated by HILL and SUNIWARD respectively and they compute the message variances by (41). G-MiPOD uses the variance estimator of MiPOD to calculate pixel residual variances and computes the message variances by (26). It is observed that the statistically significant improvement of the Gaussian embedding scheme, assuming a significance level of 0.05, with $q = 1$ and $q = 3$ emerges in the range of 0.05-0.2 bpp and 0.05-0.1 bpp respectively depending on the algorithm. However, the advantages of the Gaussian embedding model becomes less significant for HILL algorithm with $q = 1$ in very high payloads of 0.75-1 bpp. MiPOD outperforms G-MiPOD in payloads of 0.75-1 bpp, regardless of the q value. For SUNIWARD with $q = 3$ and payload of 1 bpp, the improvement is not significant. The most secure embedding is G-HILL with $q = 3$ in all the payloads.

We believe that the improvement is due to the fact that the proposed Gaussian method embeds more bits in textured areas (pixels with low embedding costs or equivalently high residual variances) and less bits in smooth areas (pixels with high embedding costs or equivalently low residual variances). To confirm that, in Fig. 2, we have plotted the number of bits embedded in each pixel versus pixel's embedding cost computed by HILL and SUNIWARD, and also pixel's residual variances computed by MiPOD for a payload of 0.3 bpp in "1.pgm". It is observed that the proposed Gaussian embedding scheme embeds less bits in smooth regions and more in noisy regions comparing to the original methodologies.

C. Batch Steganography

In theorem 2, two statements are proven for the effect of batch size on detection error of batch steganography. To examine this theorem in practice, we evaluate the performance of G-HILL and HILL with various batch sizes (1, 2, 4, 8, 16, 128) for different payloads between 0 and 1 bpp. The results, depicted in Fig. 3, indicate that the performance improves by increasing the batch size for payloads from 0 to 0.2 bpp. This behavior is consistent with theorem 2 stating that the detection error is higher for larger batch sizes if payload is much lower than 1 nat per pixel (equivalently 1.44 bpp). Theorem 2 also states that when payload approaches infinity, the detection error is lower for larger batch sizes. In Fig. 3, this behavior starts to emerge for payloads greater than 0.3 bpp and in payload of 1 bpp, the greatest batch size (128) has the lowest security comparing to smaller batch sizes. By comparing the performances shown in Table II and III, similar behavior is observed for G-MiPOD, MiPOD, G-SUNIWARD, and SUNIWARD algorithms for batch sizes equal to 1 and 128. The beauty of theorem 2 is the fact that it is formulated based on the proposed Gaussian embedding scheme, however it also holds for the original algorithms as well (HILL, MiPOD, and SUNIWARD).

By taking advantage of this phenomenon, *AdaBIM* is proposed that has significantly higher performance, with p-value less than or equal to 0.05, for majority of the payloads between 0 and 1 bpp, compared to IMS. See Table III. Security improvement in *AdaBIM* rises in the range of 0.2-0.4 bpp depending on the steganography algorithm. Authors believe that advantages of *AdaBIM* could emerge in even lower payloads if IMS batch size (M) is equal to the total number of images in the database as it is defined in its original paper, instead of $M = 128$. However, due to computational limitations we could not utilize higher M.

The performance improvement of *AdaBIM* comparing to IMS is due to the fact that in *AdaBIM* the batch size gradually decreases as the payload increases. In low payloads, the highest batch size ($M = 128$) has the highest security. However as the payload increases the optimum M decreases until very high payloads (near 1) where the optimal option is $M = 2$. Note that, the optimal batch size in each payload varies for different methods. Thus, it needs to be calculated separately for each algorithm. It is needless to say that the larger the number of experimented M is, the more precise the optimal M will be. This time consuming step needs to be done once and the calculated optimal batch sizes can be used in practice. In other words, finding optimal batch sizes for each payload and algorithm can be seen as a training step whose results can be used in future practices without further calculations.

In this study, we do not impose any assumptions about the warden's knowledge of image' sources, and thus, we do not perform any pooled steganalysis experiments. However, we plan to investigate the pooled steganalysis problem in the future, where the derived closed-form expression of the

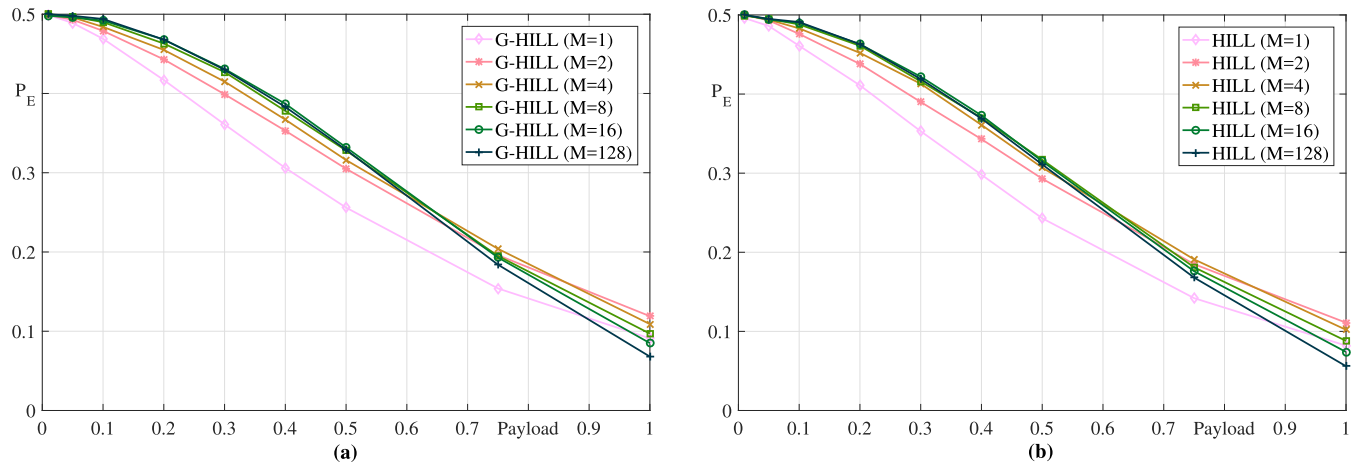

Fig. 3. Detection error computed by steganalysis using maxSRMd2 features in different payloads ranging from 0 to 1 bpp for (a) G-HILL (b) HILL algorithms with different batch sizes ($M = 1, 2, 4, 8, 16, 128$). It can be seen that the best performing batch size decreases as the payload increases.

TABLE III

DETECTION ERROR OF BATCH STEGANOGRAPHY USING THREE STEGANOGRAPHY METHODS AND THEIR PROPOSED GAUSSIAN VERSION WITH TWO DIFFERENT BATCHING STRATEGIES, IMS WITH BATCH SIZE 128 AND THE PROPOSED *AdaBIM* WITH ADAPTIVE BATCH SIZE, COMPUTED BY STEGANALYSIS USING MAXSRMD2 FEATURES IN DIFFERENT PAYLOADS RANGING FROM 0 TO 1 BPP

Embedding	Batching	payload = **0.01**	**0.05**	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**	**0.75**	**1**
G-HILL	*AdaBIM*	.500±.0022	.498±.0022	.494±.0021	.468±.0029	.431±.0037	.387±.0022	.332±.0033	.204±.0028	.119±.0036
	IMS	.500±.0022	.498±.0022	.494±.0021	.468±.0029	.430±.0014	.383±.0020	.329±.0031	.184±.0035	.068±.0018
HILL	*AdaBIM*	.500±.0024	.495±.0017	.491±.0026	.463±.0025	.422±.0025	.373±.0017	.317±.0027	.191±.0027	.111±.0023
	IMS	.500±.0024	.495±.0017	.491±.0026	.463±.0025	.419±.0027	.369±.0017	.311±.0017	.168±.0027	.056±.0023
G-MiPOD	*AdaBIM*	.499±.0022	.497±.0037	.488±.0020	.453±.0024	.396±.0020	.327±.0023	.256±.0022	.133±.0022	.072±.0024
	IMS	.499±.0022	.497±.0037	.488±.0020	.453±.0024	.392±.0028	.322±.0016	.243±.0024	.070±.0024	.023±.0017
MiPOD	*AdaBIM*	.499±.0032	.497±.0025	.485±.0032	.446±.0020	.383±.0017	.306±.0017	.232±.0035	.129±.0043	.070±.0033
	IMS	.499±.0032	.497±.0025	.485±.0032	.446±.0020	.379±.0011	.299±.0032	.214±.0021	.065±.0019	.018±.0012
G-SUNIWARD	*AdaBIM*	.499±.0024	.497±.0028	.491±.0027	.464±.0025	.429±.0023	.382±.0048	.336±.0036	.221±.0027	.139±.0022
	IMS	.499±.0024	.497±.0028	.491±.0027	.464±.0025	.429±.0023	.380±.0033	.332±.0049	.206±.0028	.101±.0019
SUNIWARD	*AdaBIM*	.500±.0027	.494±.0034	.487±.0022	.457±.0021	.418±.0023	.370±.0026	.324±.0030	.205±.0027	.135±.0013
	IMS	.500±.0027	.494±.0034	.487±.0022	.457±.0021	.417±.0029	.367±.0022	.317±.0021	.180±.0020	.067±.0010

TABLE IV

AVERAGE TIME IN SECONDS SPENT TO EMBED A CODED MESSAGE IN AN IMAGE USING THREE DIFFERENT STEGANOGRAPHY METHODS AND THEIR PROPOSED GAUSSIAN VERSIONS IN DIFFERENT $(2q+1)$-ARY EMBEDDING SCENARIOS WITH VARIOUS BATCH SIZES (M)

M	q	G-HILL	HILL	G-MiPOD	MiPOD	G-SUNIWARD	SUNIWARD
1	1	0.160	0.037	0.197	0.263	0.219	0.058
	3	0.372	0.074	0.425	0.799	0.457	0.107
128	1	0.097	0.022	0.111	0.206	0.129	0.051
	3	0.252	0.065	0.335	0.665	0.416	0.093

detection error could be utilized to improve the performance when the warden is assumed to know the image sources.

D. Computational Time

In this section, we compare the amount of time that each embedding algorithm and its Gaussian version spend to embed a $(2q+1)$-ary message in one image. In addition, we also compare their computation time in batch steganography scenario for $M = 128$. See Table IV. Each time is reported in seconds and calculated by taking the average of time spent per image when embedding payloads ranging from 0.01 to 1 bpp in the whole database. It is observed that all the proposed approaches (G-HILL, G-MiPOD, and G-SUNIWARD) are faster than MiPOD, the state-of-the-art model based method. G-HILL and G-SUNIWARD are 3 to 5 times slower than HILL and SUNIWARD respectively depending on q and M values, however given the superior security of the Gaussian versions, their computation time is still reasonable. In general, embedding a 7-ary message is 2 to 3 times slower than 3-ary message. For all the embedding methods, the batch steganography scenario with $M = 128$ is faster than $M = 1$ for similar q, which is expected since MATLAB performs vectorization faster than "for" loops.

VII. CONCLUSION

In this work, a statistical framework is developed for steganography problem in which the cover and the stego messages are modeled by independent Gaussian random variables. Subsequently, a novel Gaussian embedding model is proposed by simultaneously minimizing the detection error of three optimal hypothesis testing detectors. The proposed Gaussian embedding model can work with both pixel embedding costs and residual variances which makes it a universal embedding technique applicable to all the state-of-the-art image steganography methods, and it improves their security significantly.

Additionally, the closed-form detection error as a function of payload is derived within the adopted model for image steganography and it is extended to batch steganography as well. The availability of the closed-form detection error allowed us to investigate the effect of batch size on security of batch steganography. As a result, a new batching strategy, *AdaBIM*, is introduced, which is shown to outperform the state-of-the-art both mathematically and empirically.

In future, we plan investigate skewed statistical models such as generalized Gaussian distribution for cover and stego image pixels. This may lead to asymmetric embedding steganography method that can embed in saturated pixels and also outliers in smooth regions. Additionally, the derived closed-form expression of the detection error could be utilized to solve the pooled steganalysis problem as well as the batch steganography problem directly without utilizing the image merging sender. Moreover, it can be employed to investigate the design of embedding costs and residual variances.

APPENDIX A
ASYMPTOTIC SUM OF GAMMA RANDOM VARIABLES

Suppose $X_1, \cdots, X_n$ are all independently distributed by Gamma with shape k, but with scaling parameters $\theta_1, \cdots \theta_n$ respectively. Let Y be the sum of all these variables and Z be the normalized Y, i.e.

$$Z = \frac{Y - \mathrm{E}[Y]}{\mathrm{Var}[Y]} = \frac{\sum_{\ell=1}^{n}(X_\ell - k\theta_\ell)}{\sqrt{k\sum_{i=1}^{n}\theta_i^2}}. \tag{42}$$

Based on [32], probability distribution of Z converges to standard normal distribution, $\mathcal{N}(0,1)$, when $n \to \infty$ if the following conditions are met.

1) $0 < k\sum_{i=1}^{n}(\frac{\theta_i}{\sqrt{n}})^2 < \infty$
2) $\lim_{n\to\infty} k\sum_{i=1}^{n}(\frac{\theta_i}{\sqrt{n}})^r = 0 \quad$ for $\; r \geq 3$

These conditions are met as long the θ's are bounded. To show this, suppose that $0 < \theta_{\min} \leq \theta_i \leq \theta_{\max} < \infty$ for all i's. Then it can be easily shown that

$$kn\frac{\theta_{min}^r}{\sqrt{n^r}} < k\sum_{i=1}^{n}(\frac{\theta_i}{\sqrt{n}})^r < kn\frac{\theta_{max}^r}{\sqrt{n^r}}. \tag{43}$$

If $n \to \infty$, and $r = 2$, the lower and upper bounds are $k\theta_{min}^2$ and $k\theta_{max}^2$ respectively and they are both bounded. If $n \to \infty$, and $r \geq 3$, they both tend to zero.

Therefore, for large enough n, probability distribution of Y can be approximated with normal distribution, i.e.

$$Y \sim \mathcal{N}\Big(k\sum_{i=1}^{n}\theta_i,\; k\sum_{i=1}^{n}\theta_i^2\Big) \tag{44}$$

Now we are one step away from the complete proof of the theorem. Suppose $Y' = \sum_{i=1}^{n}(X_i + a_i)$ which is just a constant, $\sum_{i=1}^{n} a_i$, plus Y. As a result

$$Y' \sim \mathcal{N}\Big(\sum_{i=1}^{n}(k\theta_i + a_i),\; k\sum_{i=1}^{n}\theta_i^2\Big), \tag{45}$$

which proves the theorem.

APPENDIX B
PROOF OF THEOREM 2

In this section, the following lemma is proven first. Then, the result is extended to compare the detection error in case of using different batch sizes and prove Theorem 2.

Lemma 1: Given any $x, \alpha \geq 0$, the following statements for normal cumulative distribution function, ϕ, are true:

(i) $\frac{1}{2}\phi(-x) + \frac{1}{2}\phi(-\alpha x) \leq \phi(-\sqrt{\alpha}x) \qquad x, \alpha x \ll 1$

(ii) $\frac{1}{2}\phi(-x) + \frac{1}{2}\phi(-\alpha x) \geq \phi(-\sqrt{\alpha}x) \qquad x, \alpha x \to \infty$

Proof (i): The first part of the lemma states that when x tends to zero, the following inequality holds;

$$\frac{1}{2}\phi(-x) + \frac{1}{2}\phi(-\alpha x) \leq \phi(-\sqrt{\alpha}x) \quad x, \alpha x \ll 1. \tag{46}$$

To prove (46), we approximate ϕ with the first two terms of its Taylor series expansion given by

$$\phi(z) = \frac{1}{2} + \frac{1}{\sqrt{2\pi}}\sum_{n=0}^{\infty}\frac{(-1)^n z^{2n+1}}{(2n+1)2^n n!} \xrightarrow{z\ll 1} \frac{1}{2} + \frac{z}{\sqrt{2\pi}}. \tag{47}$$

Applying approximation shown in (47) to (46) results in

$$\frac{1}{2} + \frac{(-x)}{2\sqrt{2\pi}} + \frac{(-\alpha x)}{2\sqrt{2\pi}} \leq \frac{1}{2} + \frac{(-\sqrt{\alpha}x)}{\sqrt{2\pi}}. \tag{48}$$

Since x is positive, this in turn means

$$-\alpha - 1 \leq -2\sqrt{\alpha}, \tag{49}$$

which is true due to the fact that $0 \leq (\sqrt{\alpha} - 1)^2$. ■

Proof (ii): The second part of the lemma states that when x approaches infinity, the following inequality holds;

$$\frac{1}{2}\phi(-x) + \frac{1}{2}\phi(-\alpha x) \geq \phi(-\sqrt{\alpha}x) \quad x, \alpha x \to \infty. \tag{50}$$

To prove (50), we approximate ϕ with its asymptotic expansion. To derive this expansion, the asymptotic expansion of the error function, erf, is utilized which is given by

$$\mathrm{erf}(z) = \text{-}1 + \frac{\mathrm{e}^{-z^2}}{\sqrt{\pi}}\sum_{n=0}^{\infty}\frac{(\text{-}1)^n(2n\text{-}1)!!}{2^n\ (\text{-}z)^{n+1}} \quad \text{as } z \to -\infty, \tag{51}$$

where !! is the double factorial, i.e. $n!! = n \cdot (n-2)\cdots 1$. Given that $\mathrm{erf}(z) = 2\phi(\sqrt{2}z) - 1$ and using the first two terms of the asymptotic series in (51), it can be shown that

$$\phi(-z) \xrightarrow{z\to\infty} \frac{\mathrm{e}^{\frac{-z^2}{2}}}{\sqrt{2\pi}\,z}. \tag{52}$$

By applying (52), to (50), we get the following inequality,

$$\frac{\mathrm{e}^{\frac{-x^2}{2}}}{2\sqrt{2\pi}x} + \frac{\mathrm{e}^{\frac{-(\alpha x)^2}{2}}}{2\sqrt{2\pi}\alpha x} \geq \frac{\mathrm{e}^{\frac{-(\sqrt{\alpha}x)^2}{2}}}{\sqrt{2\pi}\alpha x}. \tag{53}$$

Since x and αx are positive as they approach infinity, inequality (53) can be simplified as

$$\alpha^{\frac{1}{2}}\mathrm{e}^{\frac{-(1-\alpha)x^2}{2}} + \alpha^{\frac{-1}{2}}\mathrm{e}^{\frac{-(\alpha^2-\alpha)x^2}{2}} \geq 2. \tag{54}$$

This is true for every positive α, since for every α other than one, one of the terms on the left hand side of this equation goes to infinity as x approaches infinity, and for α equal to one, the left hand side is exactly two and equality happens. ■

Proof of Theorem 2: This theorem compares the error of detection for batch size of M and $2M$ for embedding p nats per pixel in a database of N images. Suppose M, and N are powers of two and $2M \leq N$. Without loss of generality, assume that the l^{th} batch includes these images: $(l-1)B, \ldots, lB-1$, where B is the batch size. As a result, the l^{th} batch when $B = 2M$, contains images of batches $2l-1$ and $2l$ of the case when $B = M$. Based on (33), the average detection error for these images $((l-1)2M, \ldots, 2lM-1)$, when $B = M$, is

$$\frac{1}{2}\phi\left(-\sqrt{n\lambda_{2l-1}^{(M)}(p)/32}\right)+\frac{1}{2}\phi\left(-\sqrt{n\lambda_{2l}^{(M)}(p)/32}\right), \quad (55)$$

and when $B = 2M$, is

$$\phi\Big(-\sqrt{n\lambda_{l}^{(2M)}(p)/32}\Big), \quad (56)$$

where $\lambda_l^{(M)}(p)$ is the Lagrangian multiplier for the l^{th} batch when the batch size and the payload are M, and p respectively. For using the lemma to compare these two average detection errors, (55) and (56), let us define x and α as

$$x = \sqrt{\frac{n\lambda_{2l-1}^{(M)}(p)}{32}}, \quad (57)$$

$$\alpha = \frac{\sqrt{\frac{n\lambda_{2l}^{(M)}(p)}{32}}}{\sqrt{\frac{n\lambda_{2l-1}^{(M)}(p)}{32}}} = \frac{\sqrt[M]{\prod_{j=(2l-2)M}^{(2l-1)M-1}\sqrt[n]{\prod_{i=1}^{n}\sigma_{ij}^2}}}{\sqrt[M]{\prod_{j=(2l-1)M}^{2lM-1}\sqrt[n]{\prod_{i=1}^{n}\sigma_{ij}^2}}}, \quad (58)$$

where the simplification is done based on (35). Note that, α, defined in (58), is constant for all the payloads, p, regardless of the value of x and l. Employing (35), it can be shown that

$$\lambda_l^{(2M)}(p) = \sqrt{\lambda_{2l}^{(M)}(p)\lambda_{2l-1}^{(M)}(p)}, \quad (59)$$

which results in

$$\sqrt{n\lambda_l^{(2M)}(p)/32} = \sqrt{\alpha}x. \quad (60)$$

Based on the variable definitions in (57), (58), and (60), and the first part of the lemma, (46), it can be shown that if $x, \alpha x \ll 1$, (55) is less or equal than (56). Therefore, the summation of (55) over all batches, $l \in \{1, \ldots \frac{N}{M}\}$, is less or equal than the summation of (56). In addition, as it was shown in Sec. V, for payloads much smaller than one, Lagrangian multiplier λ for all batches and consequently x and αx are much smaller than one. Therefore, based on (37), and the mentioned inequality, it is concluded that

$$\mathrm{P_E}(M, N, p) < \mathrm{P_E}(2M, N, p) \quad p \ll 1. \quad (61)$$

Following similar steps but using the second part of the lemma, (50), it can be shown that if x and αx, shown in (57) and (58), approach infinity, the summation of (55) over all batches, $l \in \{1, \ldots \frac{N}{M}\}$, is greater or equal than the summation of (56). In addition, as it was shown in Sec. V, for payloads approaching infinity, Lagrangian multiplier λ for all batches and consequently x and αx approach infinity. Thus, the following inequality holds

$$\mathrm{P_E}(M, N, p) > \mathrm{P_E}(2M, N, p) \quad p \to \infty, \quad (62)$$

which proves the second part of Theorem 2. ■

REFERENCES

[1] G. J. Simmons, "The prisoners' problem and the subliminal channel," *Adv. Cryptol.*, vol. 5, pp. 51–67, Feb. 1984.

[2] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, no. 3, pp. 727–752, Mar. 2010.

[3] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, Feb. 1998.

[4] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proc. Workshop Multimedia Secur., New Challenges*, Oct. 2001, pp. 27–30.

[5] C. E. Shannon, "Coding theorems for a discrete source with a fidelity criterion," *IRE Nat. Conv. Rec.*, vol. 4, no. 1, pp. 142–163, 1959.

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

[7] T. Filler and J. Fridrich, "Gibbs construction in steganography," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 705–720, Dec. 2010.

[8] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP J. Inf. Secur.*, vol. 1, pp. 1–13, Dec. 2014.

[9] B. Li, M. Wang, J. Huang, and X. Li, "A new cost function for spatial image steganography," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Oct. 2014, pp. 4206–4210.

[10] R. Böhme, *Advanced Statistical Steganalysis*. New York, NY, USA: Springer, 2010.

[11] T. Pevný, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 215–224, Jun. 2010.

[12] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Proc. Int. Workshop Inf. Hiding*, Jun. 2010, pp. 161–177.

[13] J. Kodovsky, J. Fridrich, and V. Holub, "On dangers of overtraining steganography to incomplete cover model," in *Proc. 13th ACM Multimedia Workshop Multimedia Secur.*, Sep. 2011, pp. 69–76.

[14] J. Fridrich and J. Kodovský, "Multivariate Gaussian model for designing additive distortion for steganography," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, May 2013, pp. 2949–2953.

[15] V. Sedighi, J. Fridrich, and R. Cogranne, "Content-adaptive pentary steganography using the multivariate generalized Gaussian cover model," *Proc. SPIE*, vol. 4, Mar. 2015, Art. no. 94090H.

[16] V. Sedighi, R. Cogranne, and J. Fridrich, "Content-adaptive steganography by minimizing statistical detectability," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 221–234, Feb. 2016.

[17] A. D. Ker, "Batch steganography and pooled steganalysis," in *Information Hiding* (Lecture Notes in Computer Science). New York, NY, USA: Springer-Verlag, 2007.

[18] A. D. Ker *et al.*, "Moving steganography and steganalysis from the laboratory into the real world," in *Proc. 1st ACM Workshop Inf. Hiding Multimedia Secur.*, Jun. 2013, pp. 45–58.

[19] A. D. Ker, "Batch steganography and the threshold game," *Proc. SPIE*, vol. 4, Mar. 2007, Art. no. 650504.

[20] A. D. Ker, "Perturbation hiding and the batch steganography problem," in *Proc. Int. Workshop Inf. Hiding*, May 2008, pp. 45–59.

[21] A. D. Ker and T. Pevny, "Batch steganography in the real world," in *Proc. Multimedia Secur.*, Sep. 2012, pp. 1–10.

[22] Z. Zhao, Q. Guan, X. Zhao, H. Yu, and C. Liu, "Embedding strategy for batch adaptive steganography," in *Proc. Int. Workshop Digit. Watermarking*, Feb. 2017, pp. 494–505.

[23] R. Cogranne, V. Sedighi, and J. Fridrich, "Practical strategies for content-adaptive batch steganography and pooled steganalysis," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Mar. 2017, pp. 2122–2126.

[24] M. Sharifzadeh, M. Aloraini, and D. Schonfeld, "Quantized Gaussian embedding steganography," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, May 2019, pp. 2637–2641.

[25] M. Sharifzadeh, C. Agarwal, M. Salarian, and D. Schonfeld, "A new parallel message-distribution technique for cost-based steganography," May 2017, *arXiv:1705.08616*. [Online]. Available: https://arxiv.org/abs/1705.08616

[26] W. H. Lee, "Continuous and discrete properties of stochastic processes," Ph.D. dissertation, Univ. Nottingham, U.K.: 2010.

[27] P. Bas, T. Filler, and T. Pevný, "Break our steganographic system': The ins and outs of organizing BOSS," in *Proc. Int. Workshop Inf. Hiding*, May 2011, pp. 59–70.

[28] J. Kodovský, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 432–444, Apr. 2012.
[29] T. Denemark, V. Sedighi, V. Holub, R. Cogranne, and J. Fridrich, "Selection-channel-aware rich model for steganalysis of digital images," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2014, pp. 48–53.
[30] T. Denemark, J. Fridrich, and V. Holub, "Further study on the security of S-UNIWARD," *Proc. SPIE*, vol. 19, Feb. 2014, Art. no. 902805.
[31] V. Sedighi and J. Fridrich, "Effect of saturated pixels on security of steganographic schemes for digital images," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Sep. 2016, pp. 2747–2751.
[32] A. M. Mathai, "Storage capacity of a dam with gamma type inputs," *Ann. Inst. Stat. Math.*, vol. 34, no. 1, pp. 591–597, 1982.

Mehdi Sharifzadeh received the B.S. degree in electrical engineering from the Sharif University of Technology in 2012. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Illinois at Chicago. He is currently a Researcher with the Department of Electrical and Computer Engineering, University of Illinois at Chicago. His current research interest includes image steganography. Along with his main research topic, he is involved in deep neural networks and problems in machine learning and computer vision.

Mohammed Aloraini received the B.S. degree in electrical engineering from Qassim University in 2011, and the M.S. degree in electrical and computer engineering from the University of Illinois at Chicago in 2014, where he is currently pursuing the Ph.D. degree in electrical and computer engineering. His current research interests include multimedia forensics and information security.

Dan Schonfeld (F'10) received the B.S. degree in electrical engineering and computer science from the University of California at Berkeley, in 1986, and the M.S. and Ph.D. degrees in electrical and computer engineering from The Johns Hopkins University, in 1988 and 1990, respectively. In 1990, he joined the University of Illinois at Chicago, where he is currently a Professor with the Departments of Electrical and Computer Engineering, Computer Science, and Bio-Engineering. His current research interests include signal processing, image and video analysis, video retrieval and communications, multimedia systems, computer vision, medical imaging, and genomic signal processing. He has been an elected University Scholar of the University of Illinois at Chicago and was a recipient of the Graduate Mentoring Award from the University of Illinois at Chicago. He has authored over 200 technical papers in various journals and conferences. He has been elevated to the rank of fellow of the SPIE. He has previously served as the Editor-in-Chief of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, and also an Area Editor for special issues of the *IEEE Signal Processing Magazine*.