What Makes the Stego Image Undetectable?

Songtao Wu, Yan Liu
Department of Computing
The Hong Kong Polytechnic University
Hong Kong, P. R. China
{csstwu, csyliu}@comp.polyu.edu.hk

Shenghua Zhong
College of Computer Science and Software Engineering
Shenzhen University
Shenzhen, P. R. China
csshzhong@szu.edu.cn

Yang Liu
Department of Computer Science
Hong Kong Baptist University
Hong Kong, P. R. China
csygliu@comp.hkbu.edu.hk

ABSTRACT

Steganography is the art of hiding information in ways that prevents the detection of hidden messages. Image steganography, which hides messages into a cover image for secret transmission, attracts increasing attention in social media era. Currently, most works focus on designing message embedding algorithms to avoid the stego images being distinguished from normal ones via visual observation or statistical analysis. This paper aims to make the detection of the stego images more difficult by selecting the suitable cover images. We propose a new measure to evaluate the hiding ability of the cover image based on Fisher Information Matrix and Gaussian Mixture Model. Experiments on standard dataset validate that the cover image with good hiding ability can improve the performance of various steganography algorithms obviously. Moreover, the proposed measure provides a statistical explanation of the existing cover image selection techniques and shows better performance against steganalysis.

Categories and Subject Descriptors

I.4 [**Image Processing and Computer Vision**]: Applications; K.6.m [**Management of Computing and Information Systems**]: Miscellaneous—*Security*

Keywords

Steganography, cover image selection, Fisher information, Gaussian mixture model

1. INTRODUCTION

Steganography, derived from the Ancient Greek words "steganos" and "graphein", refers to the technique of covered writing [27, 36]. It includes a large number of hidden communication methods that conceal the existence of secret message, such as invisible inks, microdots, etc [14]. Unlike cryptography which emphasizes protecting the information security by making messages illegible, steganography intends to conceal the fact that a secret message is being sent and thus will not raise an opponent's suspicion [21]. Owing to this benefit, steganography plays a crucial role in many important applications such as military and commercial communications.

ICIMCS '15, August 19-21, 2015, Zhangjiajie, Hunan, China

DOI: http://dx.doi.org/10.1145/2808492.2808539

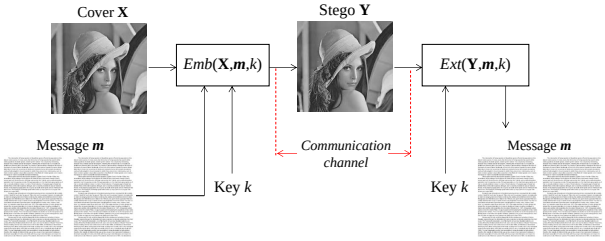


Figure 1: Illustration of the idea of image steganography.

Image steganography, which aims to hide messages into a cover image for secret transmission, attracts increasing interests in recent years [14, 27]. This is because that the rapid development of Internet and digital technologies have resulted in a huge amount of image data in our daily lives [13, 32], which provides extreme convenience for applying steganography. For example, as reported in a white paper from Facebook in 2013, its users are uploading 350 million photos each day [1]. Figure 1 shows the general idea of image steganography. The sender hides the message **m** in the cover image $\mathbf{X}$. By applying the message embedding algorithm Emb($\mathbf{X}$, **m**, k) and the key k on $\mathbf{X}$, the stego image $\mathbf{Y}$ is generated and then passed to the receiver. By applying the message extraction algorithm Ext($\mathbf{Y}$, **m**, k) and key k on $\mathbf{Y}$, the receiver can extract the secret message **m**. Here the stego image and cover image denote the images with and without hidden information, respectively. The objective is to make the stego image and cover image as similar as possible, so that the secret message will not be detected by any observers.

Currently, the research of image steganography focuses on designing the data embedding algorithms to achieve high security. One of the most classical data embedding methods is the least significant bit (LSB) based steganography [2], which replaces the LSBs of randomly selected pixels in the cover image with the secret message bits. Since LSB based steganography does not bring too much changes to the pixel values of the image, it is capable of hiding secret message in the cover without introducing many perceptible distortions. According to the design principles, the later image steganography techniques can be roughly divided into two categories: the model preserving (MP) steganography and the distortion minimization (DM) steganography [7]. The MP steganography builds a model of the source of cover images and then designs the embedding method to preserve the model [31, 33], while the DM

[1]https:fbcdn-dragon-a.akamaihd.net/hphotos-ak-ash3/851560_196423357203561_929747697_n.pdf

steganography aims to minimize a heuristically defined embedding distortion between the stego and the cover [12].

Most of the steganographic algorithms are able to hide the secret message into a cover image that makes the difference between the cover image and stego image undetectable by human eyes. In order to detect the hidden message effectively, image steganalysis, which refers to the technologies for distinguishing images containing a secret message from those not containing any secret message, has been investigated [21]. According to the application fields, the image steganalysis technologies can be divided into specific methods and universal methods. Specific steganalysis methods are designed for the targeted steganographic techniques directly, and make full use of the knowledge of the corresponding steganographic techniques [4]. The universal steganalysis method do not require the knowledge of the details of the embedding methods, and can be used to detect several kinds of steganography [9, 11].

Several interesting works reported that if an appropriate cover image is selected, it will be more difficult to detect the existence of secret image and thus the security of steganography can be largely improved. [15] observed that complex cover images, which consist of many noisy, textured and cluttered regions, are generally securer for steganography than those smooth and flat images. [37] validated that the texture information is of great importance in evaluating the hiding ability of the cover image. [19] discussed how the texture, spatial frequency and the quality of cover images influence the steganographic security. [29] proposed to use steganalytic features to evaluate the embedding capacity of a cover image. [18, 30] investigated whether the steganographic security can be improved by selecting cover images based on the image quality, the number of pixel changes, the Mean Square Error (MSE), etc. Although several kinds of image features have been reported to be related to the hiding ability of the corresponding image, what properties that intrinsically determine the hiding ability of an image and make the steganography undetectable remain unclear. In this paper, we propose a unified measure to evaluate the hiding ability of the cover image. By representing images using the Gaussian mixture model (GMM), the proposed measure is formulated in terms of the Fisher information matrix. Based on the proposed measure, we can rank the given images and select the best one as the cover for steganography. Experimental results show that the performance of modern steganographic algorithms can be significantly improved if they utilize the cover image selected by the proposed measure.

The rest of the paper is organized as follows. In section 2, we review the use of Fisher information in steganography. In section 3, we introduce the proposed measure to evaluate the hiding ability of a given image. Extensive experimental results are reported and discussed in Section 4 to validate the effectiveness of the proposed measure. The paper is concluded in Section 5.

2. FISHER INFORMATION IN STEGANOGRAPHY

We are motivated to propose a measure with Fisher information because it is shown to be a perfect descriptor for steganographic security [6]. For example, [17] presented an empirical estimator for Fisher information and validated its effectiveness for comparing the security of message embedding algorithms. [6] derived a close form of Fisher information under assumptions that the steganographic embedding is mutually independent and the cover image is a Markov source. This close form was used to characterize perfectly secure stego-systems [5] and optimize message embedding algorithms [35]. Except for evaluating and optimizing message embedding algorithms, Fisher information also shows important roles in theoretic analysis of steganographic security. [20] and [8] used Fisher information to derive scaling laws, which theoretically answered how image operations, such as quantization and resizing, affect the security of message embedding algorithms. Unlike these works focusing on evaluating the security of message embedding algorithms, we choose to investigate the hiding ability of cover images with Fisher information.

3. THE PROPOSED MEASURE

This section presents the proposed measure. We use $\mathcal{N}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ to represent a multivariate Gaussian function with the mean vector $\boldsymbol{\mu}$ and the covariance matrix $\boldsymbol{\Sigma}$. The uppercase bold symbols $\mathbf{X}$ and $\mathbf{Y}$ represent the grayscale cover image and its stego version. $\mathbf{x} = (x_{ij})^{m\times n}$ and $\mathbf{y} = (y_{ij})^{m\times n}$, where $x_{ij} \in \mathbf{X}$ and $y_{ij} \in \mathbf{Y}$, denote image patches with size $m \times n$ extracted from $\mathbf{X}$ and $\mathbf{Y}$, respectively. In this paper, all the $m \times n$ image patches are represented as $mn \times 1$ dimensional vectors.

3.1 Problem Formulation

Assume $P(\mathbf{X}|\boldsymbol{\Theta})$ and $Q(\mathbf{Y}|\boldsymbol{\Theta}')$ represent the probability distribution of a cover image $\mathbf{X}$ and its stego image $\mathbf{Y}$, where $\boldsymbol{\Theta}$ and $\boldsymbol{\Theta}'$ are the parameters. The steganographic security is defined as the KL divergence between two distributions [3]:

$$D_{KL}\left(P||Q\right) = \int_{\mathbf{X}} P\, ln\left(\frac{P}{Q}\right) d\mathbf{X} \tag{1}$$

By following the shifting hypothesis [16], where message embedding only causes a parameter shift to the distribution of the cover signal, we assume that two distributions have the following relationship:

$$Q(\mathbf{Y}|\boldsymbol{\Theta}') \approx P(\mathbf{X}|\boldsymbol{\Theta} + \delta\boldsymbol{\Theta}) \tag{2}$$

where $\delta\boldsymbol{\Theta}$ represents a small variation to $\boldsymbol{\Theta}$. Combining Eq.(1) and Eq.(2), the KL divergence between two distributions can be expanded as a quadratic form using Taylor expansion:

$$D_{KL}\left(P||Q\right) \approx \left(\delta\boldsymbol{\Theta}\right)^T \boldsymbol{\mathcal{I}}\left(\boldsymbol{\Theta}\right)\left(\delta\boldsymbol{\Theta}\right) \tag{3}$$

where $\boldsymbol{\mathcal{I}}(\boldsymbol{\Theta})$ represents the Fisher information matrix [34]:

$$\boldsymbol{\mathcal{I}}(\boldsymbol{\Theta}) = E\left[\left(\frac{\partial\, lnP(\mathbf{X}|\boldsymbol{\Theta})}{\partial\boldsymbol{\Theta}}\right)\left(\frac{\partial\, lnP(\mathbf{X}|\boldsymbol{\Theta})}{\partial\boldsymbol{\Theta}}\right)^T\right] \tag{4}$$

where $E(\cdot)$ represents the expectation in terms of $P(\mathbf{X}|\boldsymbol{\Theta})$. In this paper, we propose the following measure to evaluate the security of $\mathbf{X}$:

$$\mathcal{M} = f\left(\boldsymbol{\mathcal{I}}(\boldsymbol{\Theta})\right) \tag{5}$$

where f is a function that maps Fisher information matrix $\boldsymbol{\mathcal{I}}(\boldsymbol{\Theta})$ into a real value.

3.2 Modeling Image with Gaussian Mixture

Directly modeling natural images is prohibitively hard due to their high dimensionality nature [38]. As a result, modern works approach this problem by learning models over image patches. Fortunately, the structure can be captured effectively by many statistical tools, such as Gaussian Mixture Model (GMM) [39], student t mixture [25] . Consequently, we use the distribution of patches to represent the distribution of the whole image. Assume $\{\mathbf{x}_k\}_{k=1}^N$ are N patches sampled from $\mathbf{X}$, we choose GMM to model their distribution:

$$\mathbf{x}_k \sim p(\mathbf{x}|\boldsymbol{\theta}) = \sum_{i=1}^{L} \pi_i \mathcal{N}(\mathbf{x}; \boldsymbol{\mu}_i, \boldsymbol{\Sigma}_i) \tag{6}$$

where $(\pi_i, \boldsymbol{\mu}_i, \boldsymbol{\Sigma}_i)$ are parameters of the i-th component of GMM, $\boldsymbol{\theta} = \{(\pi_i, \boldsymbol{\mu}_i, \boldsymbol{\Sigma}_i)\}_{i=1}^{L}$, $\pi_i \geq 0$, $\sum_{i=1}^{L} \pi_i = 1$. We use GMM because of its appealing advantages. First, GMM can approximate any probability distribution [28]. Second, GMM shows good performance in modeling image statistics [39]. Third, sampling from GMM is very easy, so that statistics can be effectively estimated [39].

Before learning the parameters $\boldsymbol{\theta}$, each patch $\mathbf{x}_k$ is centralized by subtracting its mean $\overline{\mathbf{x}}_k$. In this case, each component in GMM is assumed to share a zero expectation, i.e., $\boldsymbol{\mu}_i = \mathbf{0}$, thus:

$$p(\mathbf{x}|\boldsymbol{\theta}) = \sum_{i=1}^{L} \pi_i \mathcal{N}(\mathbf{x}; \mathbf{0}, \boldsymbol{\Sigma}_i) \tag{7}$$

By modeling $\mathbf{X}$ with GMM, $P(\mathbf{X}|\boldsymbol{\Theta})$ is equivalent to $p(\mathbf{x}|\boldsymbol{\theta})$, $\boldsymbol{\mathcal{I}}(\boldsymbol{\Theta})$ is equivalent to $\boldsymbol{\mathcal{I}}(\boldsymbol{\theta})$. In the following sections, $\boldsymbol{\theta}$ is viewed as a vector. It is formed by concatenating $\{\pi_i,\ vec(\boldsymbol{\Sigma}_i)\}$ into a long vector, where $vec(\cdot)$ represents the vectorization operator. Since steganographic embedding results in very small changes, we believe that only $\boldsymbol{\Sigma}_i$ are perturbed.

3.3 Measure Estimation

In our formulation, we choose f as the trace $tr(\cdot)$ for its simplicity:

$$f\left(\boldsymbol{\mathcal{I}}(\boldsymbol{\theta})\right) = tr\left(\boldsymbol{\mathcal{I}}(\boldsymbol{\theta})\right) \tag{8}$$

In this case, only the diagonal elements in Eq.(4) need to be calculated, which can be written as:

$$\mathcal{I}(\boldsymbol{\theta})_{kk} = E\left[\left(\frac{\partial\, lnp(\mathbf{x}|\boldsymbol{\theta})}{\partial \boldsymbol{\theta}_k}\right)^2\right] \tag{9}$$

For GMM, the derivative to the covariance matrix $\boldsymbol{\Sigma}_i$, for $i = \{1, ..., L\}$, is:

$$\mathbf{P}_{\boldsymbol{\Sigma}_i} = \frac{\partial\, ln\, p(\mathbf{x}|\boldsymbol{\theta})}{\partial \boldsymbol{\Sigma}_i} = \frac{\gamma_i}{2}\left(\boldsymbol{\Sigma}_i^{-T}\mathbf{x}\mathbf{x}^T\boldsymbol{\Sigma}_i^{-T} - \boldsymbol{\Sigma}_i^{-T}\right) \tag{10}$$

where $\boldsymbol{\Sigma}_i^{-T} = \left(\boldsymbol{\Sigma}_i^{-1}\right)^T$, γ_i represents the weight of the i-th component:

$$\gamma_i = \frac{\pi_i \mathcal{N}(\mathbf{x}; \mathbf{0}, \boldsymbol{\Sigma}_i)}{\sum_{j=1}^{L} \pi_i \mathcal{N}(\mathbf{x}; \mathbf{0}, \boldsymbol{\Sigma}_j)} \tag{11}$$

By rewriting Eq.(10) into its vectorized form, we can obtain the measure by combining it with Eq.(8) and Eq.(9):

$$\mathcal{M} = \sum_{i=1}^{L} E\left(vec\left(\mathbf{P}_{\boldsymbol{\Sigma}_i}\right)^T vec\left(\mathbf{P}_{\boldsymbol{\Sigma}_i}\right)\right) \tag{12}$$

Although Eq.(12) gives the definition of $\mathcal{M}$, it can not be calculated directly due to no analytic expression for the measure. To handle this difficulty, we estimate $\mathcal{M}$ by calculating its empirical expectation $\widetilde{\mathcal{M}}$ to approximate its true value:

$$\widetilde{\mathcal{M}} = \sum_{i=1}^{L} \frac{1}{K}\left(\sum_{k=1}^{K} vec\left(\mathbf{P}_{\boldsymbol{\Sigma}_i}(\mathbf{x}_k)\right)^T vec\left(\mathbf{P}_{\boldsymbol{\Sigma}_i}(\mathbf{x}_k)\right)\right) \tag{13}$$

where $\mathbf{x}_k$ is an instance sampled from GMM, which can be efficiently generated by a two step procedure [39]. $\mathbf{P}_{\boldsymbol{\Sigma}_i}(\mathbf{x}_k)$ is calculated based on Eq.(10):

$$\mathbf{P}_{\boldsymbol{\Sigma}_i}(\mathbf{x}_k) = \frac{\gamma_i}{2}\left(\boldsymbol{\Sigma}_i^{-T}\mathbf{x}_k\mathbf{x}_k^T\boldsymbol{\Sigma}_i^{-T} - \boldsymbol{\Sigma}_i^{-T}\right) \tag{14}$$

4. EXPERIMENTS

In this section, we evaluate the effectiveness of the proposed measure on standard dataset BOSSbase ver 1.01 [1]. The dataset consists of 10,000 grayscale natural images with the size of 512×512. Figure 2 shows several sample images of the dataset. For parameters, we set L, i.e. the number of components, as 100. Parameters in GMM are learned by efficient online Expectation Minimization method [24]. For the size of image patches, we set $m = 5$, $n = 5$. $N = 10000$ image patches are uniformly sampled from a given image for GMM training. Before learning the parameters of GMM, all patches are centralized. The number of random samples K used for measure estimation is set as 10000.

Figure 2: Sample images in BOSSbase ver 1.01.

4.1 Cover Image Selection for Steganography in Spatial Domain

In this experiment, we conduct the proposed measure in spatial domain. For steganography, we use four state-of-the-art algorithms for performance evaluation: Least Significant Bit Matching revisiting (LSBM-r) [23], Edge Adaptive steganography (EA) [22], Highly Undetectable steGanOgraphy (HUGO) [26] and the Spatial UNIversal WAvelet Relative Distortion (S-UNIWARD) [12]. For steganalysis, the Spatial Rich Model (SRM) [9] based steganalysis is selected for its excellent performances in attacking many steganographic algorithms, including LSBM, EA and HUGO. In our implementation, 5000 randomly selected images in BOSSbase are used for training SRM based ensemble classifier and the rest 5000 images are for testing. The security performance is evaluated by the detection error P_E:

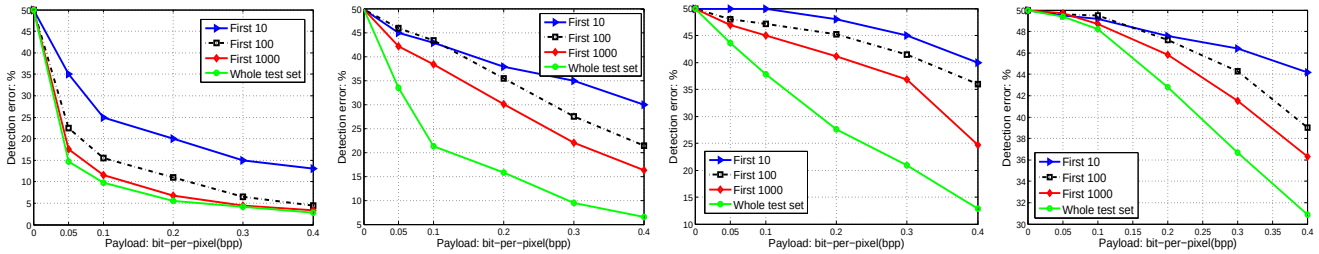
$$P_E = \frac{1}{2}(P_{MD} + P_{FA}) \tag{15}$$

where P_{MD} is the miss detection probability and P_{FA} represents the false alert probability. We use this evaluation standard because it is widely used in modern steganalysis [9].

Before evaluation, the proposed measure $\mathcal{M}$ for each image in the test set is calculated according to Eq.(13). Then all these images are sorted in an ascending manner. To prove the effectiveness of the proposed measure, we select the top M cover images with high hiding ability, where M is chosen as 10, 100, 1000 and 5000 (whole test set). The prediction error is the average of ten times running based on Eq.(15).

For the experiment, we evaluate security performances of four different steganographic algorithms based on the SRM steganalysis. The purpose is to investigate how the detection error P_E changes if top secure images are selected as the covers. Higher detection error indicates securer cover images and the vice versa. The experiment is conducted on different payloads, where the payload is defined as the division between the length of hidden messages and the dimension of the cover image, bit-per-pixel (bpp). We follow the general settings [9] to the payload in image steganography. Figure 3 shows the detection errors. Experimental results show that, when the top 10 secure images are selected as covers, the detection errors are high for four steganographic algorithms at five different payloads.

We also compare the proposed measure with several other cover image selection methods. Three measures, the mean square error



(a) LSBM-r **(b)** EA **(c)** HUGO **(d)** S-UNIWARD

Figure 3: Average detection errors P_E for LSBM, EA, HUGO and S-UNIWARD using SRM features. Four different settings are investigated: top 10 images, top 100 images, top 1000 images the whole test dataset. Here, top M represent M highest ranked images according to the proposed measure.

based cover selection (MSE-sel), number of pixel changes based cover selection (Change-sel) and the local prediction error based cover selection (Local-sel), are chosen for comparison. Details about these algorithms are introduced in [18, 30]. We choose these methods because they achieve promising performances in improving steganographic security. Table 1 shows detection errors for HUGO steganography at 0.1 bpp. The results prove that the proposed measure outperforms all other three measures.

Table 1: Performance comparison with other measures: MSE-sel, Change-sel and Local-sel. All schemes select top 100 secure images according to their measures. The payload is chosen as 0.4 bpp.

Algorithms	MSE-sel	Change-sel	Local-sel	$\mathcal{M}$
LSBM-r	3.6%	3.8%	6%	**8.5%**
EA	15.6%	14.8%	28.5%	**33%**
HUGO	23%	21%	35%	**38%**
S-UNI	28%	27.5%	40%	**45%**

4.2 Cover Image Selection for Steganography in Compressed Domain

In this experiment, we conduct the proposed measure in the compressed domain. The steganography we evaluate is nsF5 [10] for its wide use. For steganalysis, the recently proposed Discrete Cosine Transform Residual (DCTR) [11] based steganalysis is used for detection. Before evaluation, all images in BOSSbased are transformed to JPEG format with different Quality Factors (QF). QF is a number in [0,100], high QF indicates less degradation. In our experiment, general settings of QF: 75, 85 and 95, are used. Similar to the settings as the first experiment, 5000 randomly selected images are used for training the DCTR based steganalysis and the rest images are for testing. Table 2 shows the results, which prove the effectiveness of the proposed measure.

Table 2: Average detection error for nsF5 JPEG steganography. nsF5 is used for hiding messages, with payload 0.1 bpp. The detection error rate is calculated based on DCTR.

QF	10	100	1000	5000
75	28%	19.4%	16.5%	15.5%
85	30%	22.6%	20.0%	19.6%
95	34%	25.8%	23.6%	21.7%

4.3 Discussions

In this section, we discuss the properties of selected cover images. Figure 4 demonstrates several sample images evaluated by the proposed measure, including high hiding ability, middle hiding ability and low hiding ability images. By calculation, we find an interesting phenomenon that, the entropy of GMM's coefficients $S_{\boldsymbol{\pi}}$ has a monotonous relationship with the proposed measure as Table 3, where $S_{\boldsymbol{\pi}}$ is defined as:

$$S_{\boldsymbol{\pi}} = -\sum_{i=1}^{L} \pi_i ln \pi_i \tag{16}$$

Table 3: Average $S_{\boldsymbol{\pi}}$ and $\mathcal{M}$ on ranked images.

Quantity	10	100	1000	5000
$\overline{S}_{\boldsymbol{\pi}}$	3.182	2.986	2.797	2.622
$\overline{\mathcal{M}}$	0.384	0.428	0.524	0.722

To validate the rationality of the proposed measure, we conduct an experiment to find the relationship between the proposed measure, $S_{\boldsymbol{\pi}}$ and the KL divergence between a cover image and its stego. KL divergences are estimated through their GMM models. We use LSBM-r as the steganographic algorithm, the payload is set as 0.4 bpp. The image with highest $\mathcal{M}$ and image with lowest $\mathcal{M}$ are chosen. Figure 5 and Table 4 show the images and their corresponding $\mathcal{M}$ and $S_{\boldsymbol{\pi}}$ respectively. The results demonstrate that $\mathcal{M}$ is consistent with the theoretical definition of steganographic security, the KL divergence.

Table 4: $\mathcal{M}$, KL divergence and $S_{\boldsymbol{\pi}}$ for two extreme cases.

Hiding ability	$\mathcal{M}$	KL divergence	$S_{\boldsymbol{\pi}}$
Highest	0.366	9.13×10^{-7}	3.09
Lowest	12.5	7.84×10^{-4}	1.69

(a) Lowest hiding ability **(b) highest hiding ability**

Figure 5: Image with highest hiding ability and the lowest hiding ability with the proposed measure.

To demonstrate what intrinsic properties of cover images determine steganographic security, we calculate $S_{\boldsymbol{\pi}}$ and $\mathcal{M}$ in three dif-

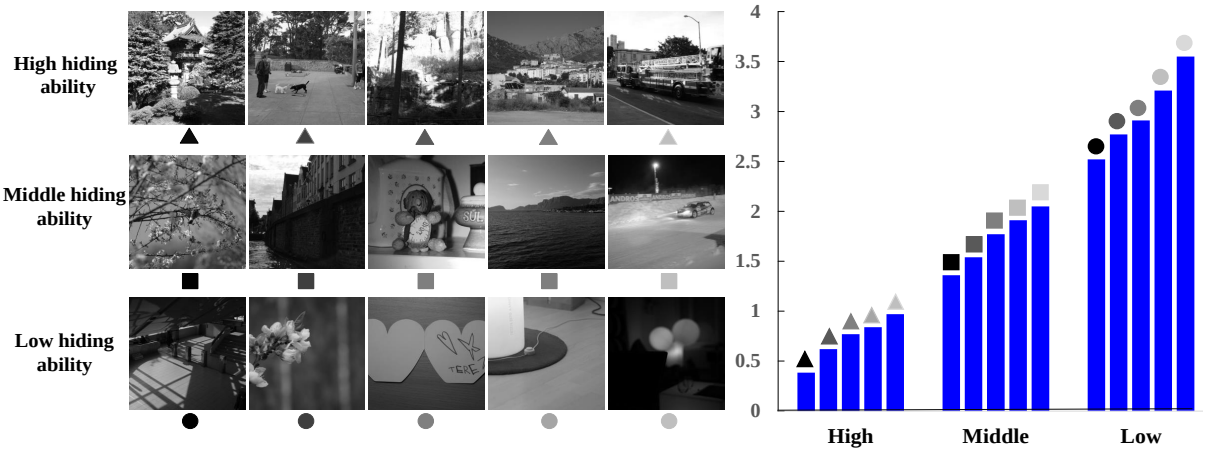
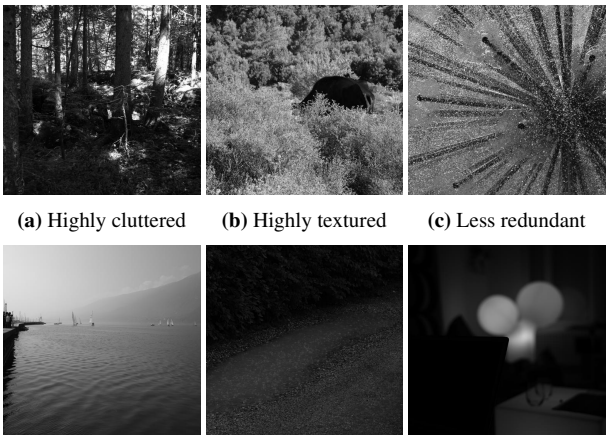


Figure 4: Demonstration for the images with high, middle and low hiding ability.

Table 5: $\mathcal{M}$ and S_{π} of cluttered, textured and redundant images.

Images	Highly cluttered	Less cluttered	Highly textured	Less textured	Less redundant	Highly redundant
$\mathcal{M}$	0.37	9.75	0.45	11.90	0.39	11.96
S_{π}	3.43	1.91	3.25	2.05	3.03	1.97



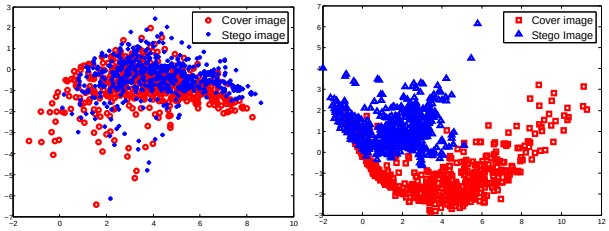
(a) Highly cluttered **(b)** Highly textured **(c)** Less redundant

(d) Less cluttered **(e)** Less textured **(f)** Highly redundant

Figure 6: Schematic illustration to cluttered, textured and redundant images.

ferent cases. For the first case, we choose two images for comparison: one is highly cluttered and the other is a less cluttered. The highly cluttered image shows extreme variability, its coefficient entropy S_{π} is higher than the less cluttered image. For the second case, a highly textured image and a less textured image are investigated. The entropy S_{π} for highly textured image is large than the less textured one. For the last case, we choose two images, one is lowly redundant image and the other is highly redundant. The entropy S_{π} for lowly redundant image is large than the highly redundant one. The selected images and their S_{π} and $\mathcal{M}$ values are demonstrated in Figure 6 and Table 5. The results show that cover images with good hiding ability w.r.t. $\mathcal{M}$ are the images that need more parameters to be modeled.

In feature space, images with excellent hiding ability are hard to be discriminated from their stego versions. In order to observe discriminability between cover images and their stegos in feature space, we extract SRM features of 500 best images and 500 worst images. Then Principle Component Analysis (PCA) is used to project high dimensional SRM features into 2 dimensional vectors.



(a) Top 500 **(b)** Low 500

Figure 7: PCA projection to top 500 and lowest 500 cover-stego images. HUGO with 0.4 bpp is used for schematic illustration.

The results are shown as Figure 7. Obviously, SRM features of best cover images and their stegos are mixed with each other, while they can be easily discriminated for the worst case.

5. CONCLUSIONS

This paper aims to improve steganography security by selecting the cover images with good hiding ability. We propose a novel measure based on Fisher Information Matrix to evaluate the hiding ability of the cover images, which are approximated by Gaussian Mixture Model. We demonstrate the effectiveness of the proposed measure by testing on various steganography and steganalysis techniques in both spatial domain and compressed domain. We conclude that:

(1) The cover images selected by the proposed measure improve the performance of steganography techniques obviously.

(2) The proposed measure outperforms other existing cover image selection techniques.

(3) The cover images selected by the proposed measure have the common statistic character that the entropy of the GMM coefficients is high. This observation explains why the cover images with complex texture, cluttered visual content, and low spatial redundancy, are recognized as the images with good hiding ability by the previous works. It also indicates that the proposed model could be considered as the generalization of the existing hiding ability measure.

The secret message considered in this work is simply the random

binary code. The structure of the secret message itself is not taken into account in the procedure of cover image selection. In the future work, we are going to investigate how to design the measure for cover image selection with highly structured secret message.

6. REFERENCES

[1] P. Bas, T. Filler, and T. Pevny. Boss (break our steganography system). *http://boss.gipsa-lab.grenoble-inp.fr*, 2009.

[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. Techniques for data hiding. *IBM System Journal*, 35(3):313–336, 1996.

[3] C. Cachin. An information theoretic model for steganography. *Information and Computation*, 192(1):41–56, 2004.

[4] S. Dumitrescu, X. Wu, and Z. Wang. Detection of lsb steganography via sample pair analysis. *IEEE Transactions on Signal Processing*, 51(7):1995–2007, 2003.

[5] T. Filler and J. Fridrich. Complete characterization of perfectly secure stegosystems with mutually independent embedding operation. In *ICASSP*, pages 1429–1432, 2009.

[6] T. Filler and J. Fridrich. Fisher information determines capacity of epsilon-secure steganography. In *Information Hiding Workshop*, pages 31–47, 2009.

[7] T. Filler and J. Fridrich. Gibbs construction in steganography. *IEEE Transactions on Information Forensics and Security*, 5(4):705–720, 2010.

[8] J. Fridrich. Effect of cover quantization on steganographic fisher information. *IEEE Transactions on Information Forensics and Security*, 8(2):261–373, 2013.

[9] J. Fridrich and J. Kodovsky. Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security*, 7(3):868–882, 2012.

[10] J. Fridrich, T. Pevny, and J. Kodovsky. Statistically undetectable jpeg steganography: dead ends, challenges, and opportunities. In *ACM Multimedia and Security Workshop*, pages 3–14, 2007.

[11] V. Holub and J. Fridrich. Low-complexity features for jpeg steganalysis using undecimated dct. *IEEE Transactions on Information Forensics and Security*, 10(2):219–228, 2015.

[12] V. Holub, J. Fridrich, and T. Denemark. Universal distortion function for steganography in an arbitrary domain. *EURASIP Journal on Information Security*, 2014(1):1–13, 2014.

[13] S. Q. Jiang, C. S. Xu, Y. Rui, A. D. Bimbo, and H. X. Yao. Preface: internet multimedia computing and service. *Multimedia Tools and Applications*, 70(2):599–603, 2014.

[14] N. F. Johnson and S. Jajodia. Exploring steganography: Seeing the unseen. *IEEE Computer*, 31(2):26–34, 1998.

[15] E. Kawaguchi and R. O. Eason. Principle and applications of bpcs steganography. *Multimedia Systems and Applications*, 3528:464–473, 1998.

[16] A. D. Ker. A capacity result for batch steganography. *IEEE Signal Processing Letters*, 14(8):525–528, 2007.

[17] A. D. Ker. Estimating steganographic fisher information in real images. In *Information Hiding Workshop*, pages 73–88, 2009.

[18] M. Kharrazi, H. T. Sencar, and N. Memon. Cover selection for steganographic embedding. In *IEEE International Conference on Image Processing*, pages 117–120, 2006.

[19] J. Kodovsky and J. Fridrich. Influence of embedding strategies on security of steganographic methods in the jpeg domain. In *SPIE*, pages 1–12, 2008.

[20] J. Kodovsky and J. Fridrich. Steganalysis in resized images. In *ICASSP*, pages 2857–2861, 2013.

[21] B. Li, J. He, J. Huang, and Y. Q. Shi. A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing*, 2(2):142–172, 2011.

[22] W. Luo, F. Huang, and J. Huang. Edge adaptive image steganography based on lsb matching revisited. *IEEE Transactions on Information Forensics and Security*, 5(2):201–214, 2010.

[23] P. Mielikainen. Lsb matching revisited. *IEEE Signal Processing Letters*, 13(5):285–287, 2006.

[24] R. M. Neal and G. E. Hinton. A view of the em algorithm that justifies incremental, sparse, and other variants. *Learning in Graphical Models*, pages 355–368, 1998.

[25] A. V. D. Oord and B. Schrauwen. The student-t mixture as a natural image patch prior with application to image compression. *The Journal of Machine Learning Research*, 15:2061–2086, 2014.

[26] T. Pevny, T. Filler, and P. Bas. Using high-dimensional image models to perform highly undetectable steganography. In *Information Hiding Conference*, pages 161–177, 2010.

[27] N. Provos and P. Honey-man. Hide and seek: an introduction to steganography. *IEEE Security and Privacy Magazine*, 1(3):32–44, 2003.

[28] D. Reynolds. Gaussian mixture models. *Encyclopedia of Biometric Recognition*, pages 659–663, 2009.

[29] H. Sajedi and M. Jamzad. Secure cover selection steganography. *Advances in Information Security and Assurance*, 5576:317–326, 2009.

[30] H. Sajedi and M. Jamzad. Using contourlet transform and cover selection for secure steganography. *International Journal of Information Security*, 9(5):337–352, 2010.

[31] P. Sallee. Model-based methods for steganography and steganalysis. *International Journal of Image Graphics*, 5(1):167–190, 2005.

[32] J. T. Sang and C. S. Xu. Browse by chunks: Topic mining and organizing on web-scale social media. *ACM Transactions on Multimedia Computing, Communications and Applications*, 7(30):1–18, 2011.

[33] A. Sarkar, K. Solanki, U. Madhow, and B. S. Manjunath. Secure steganography: Statistical restoration of the second order dependencies for improved security. In *ICASSP*, pages 277–280, 2007.

[34] L. J. Savage. On rereading r. a. fisher. *The Annals of Statistics*, 4(3):441–500, 1976.

[35] Y. Sun, D. Niu, G. Tang, and Z. Gao. Optimized lsb matching steganography based on fisher information. *Journal of Multimedia*, 7(4):295–302, 2012.

[36] H. Wang and S. Wang. Cyber warfare: Steganography vs. steganalysis. *Communications of the ACM*, 47(10):76–82, 2004.

[37] M. J. Z. Kermani. A robust steganography algorithm based on texture similarity using gabor filter. In *IEEE Symposium on Signal processing and Information Technology*, pages 578–582, 2005.

[38] D. Zoran and Y. Weiss. From learning models of natural image patches to whole image restoration. In *ICCV*, pages 479–486, 2011.

[39] D. Zoran and Y. Weiss. Natural images, gaussian mixtures and dead leaves. In *NIPS*, pages 1745–1753, 2012.