Adaptive Payload Distribution in Multiple Images Steganography Based on Image Texture Features

Xin Liao, *Member, IEEE*, Jiaojiao Yin, Mingliang Chen, and Zheng Qin

Abstract—With the coming era of cloud technology, cloud storage is an emerging technology to store massive digital images, which provides steganography a new fashion to embed secret information into massive images. Specifically, a resourceful steganographer could embed a set of secret information into multiple images adaptively, and share these images in cloud storage with the receiver, instead of traditional single image steganography. Nevertheless, it is still an open issue how to allocate embedding payload among a sequence of images for security performance enhancement. This article formulates adaptive payload distribution in multiple images steganography based on image texture features and provides the theoretical security analysis from the steganalyst's point of view. Two payload distribution strategies based on image texture complexity and distortion distribution are designed and discussed, respectively. The proposed strategies can be employed together with these state-of-the-art single image steganographic algorithms. The comparisons of the security performance against the modern universal pooled steganalysis are given. Furthermore, this article compares the per image detectability of these multiple images steganographic schemes against the modern single image steganalyzer. Extensive experimental results show that the proposed payload distribution strategies could obtain better security performance.

Index Terms—Image steganography, multiple images, payload distribution, image texture features

1 Introduction

Steganography is a technique which takes advantage of the content redundancy in digital media to conceal secret information, to achieve covert communication through the common channel [1], [2]. A great number of data hiding methods have been proposed, and widely used for secret data transmission [3], privacy preserve [4], access control [5] and so on.

In decades, many effective single image steganographic schemes have been proposed, and the most important requirement in steganography is statistical undetectability. There are two mainstream frameworks to minimize the statistical detectability in empirical covers [6]. In the embedding distortion minimizing framework, general steganographic schemes can be formulated as a source coding problem that minimizes embedding distortion [7], [8], [9], [10], [11]. Model-based framework starts with adopting a cover model that the embedding algorithm is forced to preserve [12], [13], [14], [15], [16].

With the rapid development of could technology, cloud storage can provide a platform to store and share massive images with others. It also provides us a new possible approach for image steganography, i.e., multiple images steganography. The payload can be spread strategically into multiple images adaptively, which would be difficult for steganalyst to identify stegos from a sequence of images. Thus, multiple images steganography could obtain better empirical steganographic security than traditional single image steganography. In a cloud service scenario, a sender can embed the secret messages into a set of his own images before uploading them to the cloud server for storage and sharing. Due to the difficulty of steganalysis among a large number of images, only the receiver can extract covert messages from the cloud server easily.

In the pioneering work, Ker first introduced the concept of multiple images steganography [17], and then utilized game theory and Kullback-Leibler (KL) divergence to measure the security of multiple images steganography in [18] and [19], respectively. With respect to a natural definition of secure capacity, the study in [20] showed explicitly how the security steganographic capacity is influenced by the number of cover images. Apart from theoretical security analysis on multiple images steganography, how to spread the embedding payload among a group of images is a significant issue in the practical implementation of multiple images steganography. Researchers have extended single image stego methods to multiple image steganography and proposed payload distribution strategies [21], [22], [23],

- *X. Liao is with the College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China , and also with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China. E-mail: xinliao@hnu.edu.cn.*
- *J. Yin and Z. Qin are with the College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China. E-mail: {jjy, zqin}@hnu.edu.cn.*
- *M. Chen is with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA. E-mail: mchen126@terpmail.umd.edu.*

Manuscript received 6 Sept. 2019; revised 15 Apr. 2020; accepted 20 June 2020. Date of publication 24 June 2020; date of current version 14 Mar. 2022. (Corresponding author: Xin Liao.) Digital Object Identifier no. 10.1109/TDSC.2020.3004708

[24], [25], [26]. One intuitive embedding strategy is based on uniform payload distribution (ES-UPD), i.e., evenly distributing the total payload into each cover image. However, the study in [21], [22] pointed out that a steganographer should cluster the embedding in a small number of cover objects, instead of spreading the embedding across all covers. Our experiments also show the unsatisfactory results of the ES-UPD strategy. Besides, the image merging sender (IMS) strategy [24] were designed for payload distribution in massive images steganography. However, IMS treats multiple images steganography as single image steganography by concatenating all cover images into one large-scale image, which requires large memory and is hard to implement with the cover images of different sizes.

To tackle the above disadvantages, we try to find out an indicator of the secure capacity of the individual cover image, so that the payload can be directly allocated into images according to the estimated secure capacity and each cover image can be embedded with the assigned payload independently. In steganalysis side, the image with low overall embedding distortion conceptually has better ability in resisting blind universal pooled steganalysis. Perceptually, complex texture features are less vulnerable to steganalysis than simple texture features, indicating the payload should be allocated more in the region with complex texture [27]. Therefore, we exploit the image texture features as an indicator of the secure capacity of the cover image to assign sub-payload adaptively in each cover image. The initial idea of image texture based payload allocation schemes were proposed in [28], and this paper explores and investigates the adaptive payload allocation strategies more thoroughly and systematically. In addition, we provide further discussions about how to ensure correct data extraction in the practical implementation of the proposed strategies, and the detailed analysis of the computational complexity.

We conduct several experimental evaluations on the proposed payload distribution strategies. It is shown that they could be incorporated into these state-of-the-art single image steganographic algorithms, and achieve better security performance against the modern universal pooled steganalysis. The comparisons of the per image detectability of these multiple images steganographic schemes against the modern single image steganalyzer are also provided.

The major contributions of this paper are as follows:

1) On the assumption that the receiver has knowledge of the payload allocation, we propose a framework of multiple images steganography with adaptive payload distribution strategy based on image texture features and analyze the steganalyst's knowledge, recoverability of payload distribution, and the security from the perspective of information theory.
2) We propose two payload distribution strategies based on image texture complexity and distortion distribution, and provide further discussions about the practical implementation and computational complexity. The adaptive payload distribution strategies are compatible with the state-of-the-art single image steganographic algorithms in the framework of multiple images steganography.
3) We conduct extensive experiments to show the better steganographic security performance of two proposed adaptive payload distribution strategies against the intuitive uniform payload distribution scheme and the state-of-the-art distribution method, which indicates the important role of the adaptive payload distribution strategy played in multiple images steganography.

The rest of the paper is organized as follows. Section 2 briefly reviews the related works. In Section 3, we propose a systematic framework for adaptive payload distribution in multiple images steganography based on image texture features and provide the theoretical security analysis. Section 4 first describes an intuitive uniform payload distribution strategy, and explicitly proposes two payload distribution strategies based on image texture complexity and distortion distribution. The computational complexity analysis is also given. Section 5 shows experimental comparisons to demonstrate the effectiveness of two proposed payload distribution strategies. The corresponding discussions are presented in Section 6. Section 7 concludes the paper.

2 Related Works

In this section, we briefly review the related works about state-of-the-art single image steganography, and multiple images steganography.

2.1 State-of-the-Art Single Image Steganography

In recent years, various popular single image steganographic schemes are designed to conceal information into a cover image without drawing suspicion. There are two general frameworks to minimize the statistical detectability in empirical covers: steganography minimizing a well-defined distortion function and steganography preserving a chosen cover model.

The first framework attempts to design content-adaptive steganography by embedding the secret messages while minimizing the defined costs of all changed pixels. Since the advanced syndrome-trellis codes (STCs) [29] and Gibbs construction [30] perform well in minimizing the distortion costs, scholars have been paying more attention to designing distortion costs. Wavelet obtained weights (WOW) assigns high costs to more predictable pixels and low costs to less predictable pixels by directional filters [7]. Compared to WOW, S-UNIWARD (spatial-universal wavelet relative distortion) utilizes the same bank of directional filters, but computes the cost as the sum of relative changes of wavelet coefficients over all subbands [8]. high-pass, low-pass, low-pass (HILL) overcomes the problem that the small embedding suitability of one direction causes strong effects on distortion values by utilizing one high-pass filter and two low-pass filters [9]. Later, Denemark *et al.* [10] and Li *et al.* [11] independently proposed the Synch (synchronize) strategy and clustering modification directions (CMD) strategy to preserve the correlation between neighboring pixels and synchronize the embedding modifications.

In statistical model-based framework, content-adaptive image steganographic schemes are typically realized by adopting a cover model that the embedding algorithm is forced to preserve. Highly undetectable stego (HUGO) [12]

attempts to preserve the subtractive pixel adjacency matrix (SPAM) feature [31] model and change pixels with the smallest impact on the empirical statistical distribution of pixel groups. It might become highly detectable if the steganalyst designs the detector "outside of the model" [32]. multivariate Gaussian (MG) [13] starts with the cover model as a sequence of independent quantized Gaussian, and computes the embedding change probabilities to minimize the Kullback-Leibler (KL) divergence between cover and stego objects. Multivariate generalized Gaussian model (MVGG) [14] models the pixels as a sequence of independent but not identically distributed generalized Gaussian random variables and utilizes a better variance estimator. Sedighi *et al.* derived a closed form expression for the detector of content-adaptive least significant bit matching within the selected model, and embedded the payload based on minimizing the power of the optimal detector (MiPOD) [15]. Ref. [16] proposed a novel quantized Gaussian embedding method to model the hidden messages as a continuous random variable with Gaussian distribution, and maximizing the detection error of an optimal hypothesis testing detector. It is worth mentioning that this method could be extended to distortion minimization framework, so as to work with pixel embedding costs as well as residual variances.

2.2 Multiple Images Steganography

In an actual application scenario, a resourceful steganographer could utilize multiple images adaptively and embed secret data dispersedly.

Ker first postulated multiple images steganography, in which the embedding payload is split based on the opponent's pooling evidence [17]. Then he measured the security of multiple images steganography by using game theory [18] and KL divergence [19]. With respect to a natural definition of secure capacity, it was the first to show explicitly how the security steganographic capacity is influenced by the number of the cover images [20]. For independent identically distributed cover images, it was proved that the better strategy is to distribute the secret information evenly among all covers [21]. Later, max-greedy strategy was designed for payload distribution in multiple images steganography [22]. However, it is not accurate generally, and it iteratively estimates the image capacity, which is particularly time-consuming. Zhao *et al*. [23] fitted the relation curve of a well-defined secure factor and embedding payload, and utilized the images with large size and more upward convex relation curve to carry the total data.

Recently, Cogranne *et al.* [24] derived three payload distribution strategies detectability limited sender (DeLS), distortion limited sender (DiLS), image merging sender (IMS). DeLS and DiLS spread payload over cover images so that each image contributes with the same KL divergence and the same distortion value, respectively. Similar to the parallel message-distribution technique [25], IMS strategy concatenates all cover images into a new big image and the embedding payload is distributed through the cost values directly computed from the concatenation of all cover images. Sharifzadeh *et al*. [26] proposed a novel batch strategy named AdaBIM (adaptive batch size image merging steganographer), provided the closed-form detection error for image merging batch steganography with batch size, and also mathematically proved that smaller batch size is more secure for large enough payloads.

3 The Framework and Security Analysis for Multiple Images Steganography

In this section, a systematic framework of adaptive payload distribution in multiple images steganography is proposed based on image texture features, which could be considered as the general and flexible methodology to acquire new multiple images steganographic schemes. Furthermore, from the perspective of steganalyst's power, we provide the theoretical analysis about the security of multiple images steganography.

3.1 Adaptive Payload Distribution Based on Image Texture Features

Multiple images steganography embeds secret information into several cover images simultaneously, so as to achieve further secure covert communication, which is motivated in the following scenario illustrated in Fig. 1. A steganographer (Alice) aims to communicate with a passive conspirator (Bob) via an open and insecure channel, while an eavesdropper (Eve) monitors and detects the channel. Since Alice assigns and embeds the payload to a group of images, it is difficult for Eve to identify stegos from multiple images. The major issue in multiple images steganography is how to split the payload strategically among multiple images.

In multiple image steganography, only stego images are transmitted, and the cover images serve as an innocuous disguise chosen fairly arbitrarily by the sender [33]. With a steganographic tool at hand, the choice of cover images to be embedded with messages is at the sender's discretion. Kharrazi *et al.* [34] proposed a scheme for selecting the better cover images according to the availability of the knowledge of a potential steganalyzer. A steganographer (Alice) could possess a source of innocent covers, and choose cover images by herself. Specifically, Alice could use her own device to capture various images (such as landscapes, plants, animals and buildings), and select cover images randomly. Alice should delete cover images, and covers must not be reused. It is worth pointing out that the corresponding cover images would not be sent on the communication channel, and also be not available to the steganalyst (stego-only-detection) [35]. In practice, it is unlikely that Eve has arrested Alice and seized her camera, and thus has access to Alice's cover source [27]. It is unlikely for an adversary to have a copy of the corresponding image with no steganographically hidden content. The adversary could not compare and analyze the cover and stego versions bit-for-bit. In our paper, we assume that the adversary does not have access to cover images.

Given a cover image set $X = \{x_1, x_2, \ldots, x_n\}$ with capacities $(c_1, c_2, \ldots, c_n)$, where n is the number of cover images and the capacity c_i is the maximum length of payload which can be embedded into the cover image x_i. The total capacity of all cover images can be expressed as $\sum_{i=1}^{n} c_i$. M is a given secret information set, and $|M|$ denotes the length of the secret information. Generally, we suppose $\sum_{i=1}^{n} c_i \gg |M|$, i.e., the total capacity of cover images is far more than the length of embedding payload.

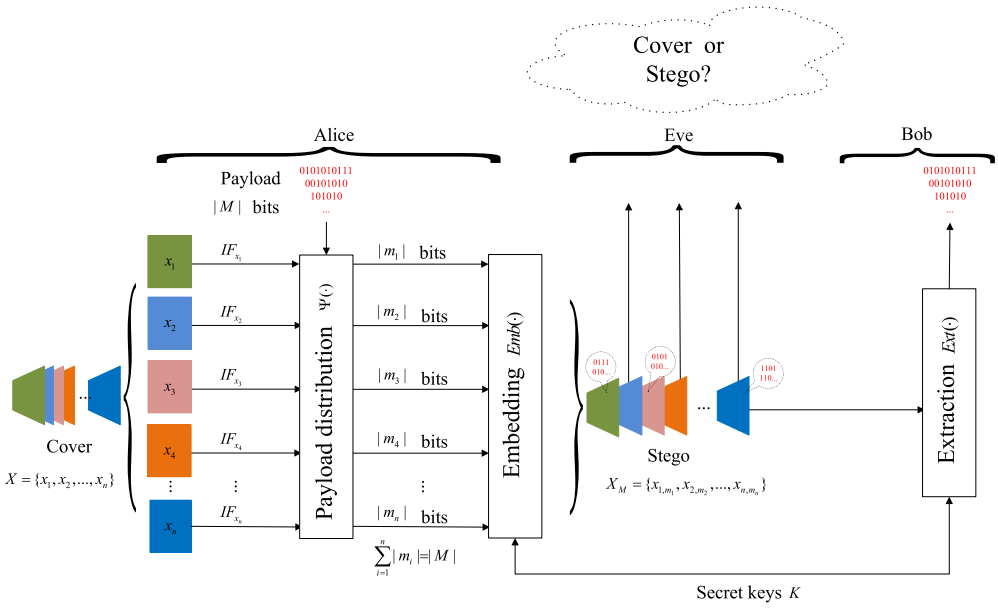


Fig. 1. The proposed framework of adaptive payload distribution in multiple images steganography based on image texture features.

Let $\Psi(\bullet)$ represent a strategy for distributing payload. The payload distribution M^* is shown in Eq. (1), associating with the images features IF_X of the cover set X

$$M^* = \Psi(M, IF_X) = [m_1, m_2, \ldots, m_n], \tag{1}$$

where m_i represents the corresponding sub-payload of the cover image x_i. IF_{x_i} represents the image texture features for a given cover image x_i in the cover set X, and IF_X is a stacked vector of IF_{x_i}, i.e., $IF_X = [IF_{x_1}, IF_{x_2}, \ldots, IF_{x_n}]$. $|m_i|$ denotes the length of m_i, and $\sum_{i=1}^{n} |m_i| = |M|$. The cover image x_i is allocated more sub-payload than x_j if it holds that

$$|m_i| > |m_j|. \tag{2}$$

Note that the steganographer's embedding keys should be shared with the intended recipient. The keys have been communicated over a secure channel prior to the use of the system. Given a embedding key set $K = \{k_1, k_2, \ldots, k_n\}$, the steganographer could embed the sub-payload m_i into the corresponding cover image x_i by single image steganographic algorithms using the key k_i. Thus, the embedding algorithm $Emb(\bullet)$ is

$$Emb(\bullet) : X \times M \times K \longmapsto X_M. \tag{3}$$

The stego image set X_M can be obtained by

$$\begin{cases} X_M = \{x_{1,m_1}, x_{2,m_2}, \ldots, x_{n,m_n}\} \\ x_{i,m_i} = Emb(x_i, m_i, k_i) \end{cases}, \tag{4}$$

where x_{i,m_i} represents the stego image by embedding the sub-payload m_i into the cover image x_i. If $|m_i| = 0$, it denotes the cover image x_i is not embedded, i.e., $x_i = x_{i,m_i}$. The stego image set X_M would be transmitted via the public communication channel.

In our work, we assume that knowledge of the size and order of the payload segments is determined by a secret key already shared between the communicating parties. Thus, the intended recipient could recombine the parts extracted from all the covers. Specifically, after acquiring the stego image set, the receiver could use the sharing information to obtain the payload distribution, and extract each sub-payload by using the extracting algorithm $Ext(\bullet)$ as below:

$$Ext(\bullet) : X_M \times K \longmapsto M. \tag{5}$$

The embedding payload M could be obtained by combining all the sub-payloads

$$\begin{cases} m_i = Ext(x_{i,m_i}, k_i) \\ M = \{m_1, m_2, \ldots, m_n\} \end{cases}. \tag{6}$$

It is worth noting that the payload allocation is shared between the steganographer and receiver. As pointed out in ref. [36], the allocation of embedding payload could be considered as a part of a shared secret key, and stored in the first few bits of embedding payload in a fixed position.

In the proposed framework of adaptive payload distribution in multiple images steganography, the following constraint is satisfied

$$Ext(Emb(x_i, m_i, k_i), k_i) = m_i, \ \forall x_i \in X, m_i \in M, k_i \in K. \tag{7}$$

Thus, multiple images steganography can be formulated by cover image set X, payload M, payload distribution strategy $\Psi(\bullet)$, embedding algorithm $Emb(\bullet)$, extracting algorithm $Ext(\bullet)$ and embedding keys K. Therefore, multiple images steganography Γ can be formulated as

$$\Gamma = (X, M, \Psi(\bullet), Emb(\bullet), Ext(\bullet), K). \tag{8}$$

And it is required to meet the following requirements.

Concealment. The steganographer could adaptively assign the embedding payload by using the payload distribution strategy $\Psi(\bullet)$, and then multiple images steganography is accomplished. The transmitted stego image set X_M would contain innocent and stego objects. For an outside observer, he could not differentiate stego images from innocent

images easily, and thus he would not determine the existence of covert communication.

Diversity. The embedding algorithm $Emb(\bullet)$ and extracting algorithm $Ext(\bullet)$ could be different and independent for each image x_i. The pair of embedding and extracting algorithms employed in multiple images steganography could be the existing single image steganographic algorithms such as WOW [7], S-UNIWARD [8], HILL [9], MiPOD [15] and so on. The steganographer would share the information about embedding-extracting matching operations with the receiver. For the sake of simplicity, for each image x_i, we only utilize the same single image steganographic algorithm in our experiments, and plan to adopt different ones in the future work.

Multi-Source. The steganographer will surely have access to more than one cover image. The cover images can be obtained in different ways. For instance, they might be downloaded via the Internet or acquired by the snapshot.

3.2 Theoretical Security Analysis

According to the security definition of steganography system, we investigate the steganalyst's knowledge, the recoverability of payload distribution, and information-theoretic security of multiple images steganography.

In our proposed framework, we assume that

1) A steganalyst could know the sizes of the individual payload chunks, but not know which cover image each chunk is allocated to. The payload distribution Ψ should be considered as a part of the steganographer's secret key shared with the intended recipient.
2) A steganalyst has the knowledge of the steganographic algorithm $Emb(\bullet)$ for embedding sub-payload in individual objects.
3) Extending the analysis of single image steganography and steganalysis [37], we assume that a steganalyst would gain knowledge about the adaptivity criterion, i.e., a steganalyst might try to recalculate its values from the stego images.

The image texture features is perfectly invariant if it holds that

$$IF_{x_i} = IF_{x_{i,m_i}}, \tag{9}$$

where IF_{x_i} denotes the image texture features of the cover image x_i, and $IF_{x_{i,m_i}}$ denotes the image texture features of the corresponding stego image x_{i,m_i} after embedding the sub-payload m_i.

Thus, in order to prevent the steganalyst from obtaining the image texture features IF_{x_i} of the cover image x_i from the corresponding stego image x_{i,m_i}, we state that the image texture features should be not perfectly invariant. Otherwise, it might be sufficient for a steganalyst to substantially gain detection performance. Thus, perfectly invariability of image texture features should be taken into account when designing secure multiple images steganographic schemes.

A given payload distribution Ψ has a recoverable order, if $\forall i, j\ (i \neq j)$ such that

$$\Psi_i(M, IF_X) > \Psi_j(M, IF_X) \Longrightarrow \Psi_i(M, IF_{X_M}) > \Psi_j(M, IF_{X_M}), \tag{10}$$

where $\Psi_i(M, IF_X)$ represents the ith element of $\Psi(M, IF_X)$, i.e., the payload allocation of the ith image in the image set X.

The recoverability of the order is a necessary and critical condition for the steganalyst's power. Even the weaker recoverability may be sufficient for a steganalyst to substantially gain detection performance. It should be pointed out that perfectly invariability of image texture features implies the recoverability of the order.

In steganographer side, a proper payload distribution Ψ is supposed to allocate the sub-payloads which are hard to recover from the stego images. Even if the steganalyst could obtain the chunk size of the split embedding payload, the steganalyst cannot deduce the exact payload distribution for each cover image. Thus, it emphasizes the importance of unrecoverability as a design goal for the payload distribution Ψ to create secure multiple images steganographic schemes.

Furthermore, we will concentrate on the stego-only-detection where the steganalyst is allowed to know only output of multiple images steganographic systems. The steganography system is information theoretically secure if the attacker cannot gain any information about secret data M or embedding key K by examining stego image X_M and distributing payload strategy Ψ. Thus, the mutual information $I((M, K); (X_M, \Psi))$ is zero. This can be expressed by expanding $I((M, K); (X_M, \Psi))$ as follows:

$$\begin{aligned} &I((M, K); (X_M, \Psi)) \\ &= H(M, K) - H((M, K)|(X_M, \Psi)) \\ &= H(M, K) - H(K|(X_M, \Psi)) - H(M|(X_M, K, \Psi)) \\ &= H(M) + H(K|M) - H(K|(X_M, \Psi)) - H(M|(X_M, K, \Psi)). \end{aligned} \tag{11}$$

Note that the attacker can determine secret data M completely from stego image X_M, embedding key K and distributing payload strategy Ψ, thus we have the conditional entropy

$$H(M|(X_M, K, \Psi)) = 0. \tag{12}$$

Considering that secret key K has to be independent of secret data M, the entropy $H(K|M) > 0$. Then, it follows that

$$H(K|(X_M, \Psi)) = H(M) + H(K|M) > H(M). \tag{13}$$

We can conclude that the conditional entropy of the embedding key must be greater than $H(M)$ to prevent an attack via K. The necessary uncertainty about secret data M must be at most the same size to make an attack on secret key K by the knowledge of stego image X_M and payload distribution strategy Ψ.

4 Two Proposed Payload Distribution Strategies

In this section, we first introduce an intuitive embedding strategy based on uniform payload distribution (ES-UPD). ES-UPD seldom pays attention to different properties among multiple images, and thus the embedding payload is equally partitioned and indiscriminately embedded into each cover image. It is reasonable to exploit the image texture features to partition payload for different images. Therefore, we propose

two embedding strategies based on image texture complexity (ES-ITC) and distortion distribution (ES-DD), in order to realize embedding payload distribution. ES-ITC assigns the amount of the sub-payload in each image, according to the image capacity derived from image texture complexity. The payload is embedded into as few images as possible, and the sub-payload of each image is equal to its estimated capacity. ES-DD strategy allocates the sub-payload depending on the statistical distribution of embedding distortion values, which are related to statistical detectability of embedding changes. ES-DD could cluster the embedding impacts of multiple images, and effectively make the embedding changes concentrated in textured image regions.

These embedding strategies can be combined with the state-of-the-art single image steganographic algorithms, so as to achieve multiple images steganography. It should be pointed out that the payload allocation should be considered as a part of a shared secret key or a small header, i.e., some auxiliary information about the detailed payload distribution should be shared between the steganographer and receiver. In a practical application, the auxiliary information can be transmitted by embedding it into the image header with LSB matching algorithm, which is a simple algorithm to embed information into the least significant bits of the image pixels. Therefore, the receiver could extract the secret message segments from all stego images, and then concatenate these segments to obtain the whole embedding payload.

4.1 Embedding Strategy Based on Uniform Payload Distribution (ES-UPD)

The intuitive embedding strategy is based on uniform payload distribution (ES-UPD), i.e., the embedding payload is distributed uniformly into all cover images. Thus, the length of sub-payload m_i for each image x_i can be computed by

$$|m_i| = \frac{|M|}{n}. \tag{14}$$

In ES-UPD strategy, the only requirement is that the length of the sub-payload m_i could not exceed the capacity c_i of its corresponding image, i.e., $|m_i| \leq c_i$. The image capacity c_i could be calculated by Eq. (20). If the length of sub-payload m_i exceeds the image capacity c_i, we could set $|m_i| = c_i$ and recalculate the average amount of sub-payload for the remaining cover images.

4.2 Embedding Strategy Based on Image Texture Complexity (ES-ITC)

In ES-ITC strategy, the new estimation method of image capacity is thoroughly investigated by using image entropy. As a standard statistical measure, image entropy can be used to characterize the texture of the input image. The image capacity of each image is first estimated, and the images with high capacity will be embedded in priority. The amount of sub-payload allocated to the selected cover images is equal to their image capacity.

As refs. [29], [30] pointed out, for a fixed statistical detectability, images with more complex textures can carry a larger secure payload than smoother or simpler images. The progress on the benchmarking of steganalysis [27] has also shown that image texture complexity as one of the important image properties would significantly affect the detectability of embedding payload. Images with complex texture are less vulnerable to steganalysis than that with simple texture, and thus more payload should be allocated to images with complex texture. Since image entropy measures could substantially reflect information about image texture characteristics [38], we could use image entropy to represent image texture complexity, and images with different levels of entropy can carry different amounts of hidden payload. On the other hand, the size of a cover image is a major factor in its capacity for hidden information. If the images have the same content, the larger image usually has a higher capacity. Thus, we estimate the capacity c_i of cover image x_i by image size and image entropy in this paper.

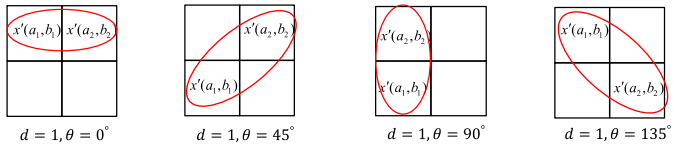


Fig. 2. Parameter setting of the gray-level co-occurrence matrix.

To capture the image texture precisely, we employ a high-pass filter $\mathbf{F}$ as a pre-processing. The filtered image set X' is represented by

$$X' = X \otimes \mathbf{F} = \{x'_1, x'_2, \ldots, x'_n\}, \tag{15}$$

where $\otimes$ denotes mirror-padded convolution. The filtered images have the same sizes as the original ones. In this paper, we choose 3×3 KerBöhme filter [39] due to its superior performance in steganalysis. The 3×3 KerBöhme filter is

$$\mathbf{F} = \begin{bmatrix} -1 & 2 & -1 \\ 2 & -4 & 2 \\ -1 & 2 & -1 \end{bmatrix}. \tag{16}$$

Assuming that the size of cover image x_i is $r_i \times s_i$, the gray-level co-occurrence matrix [40] of the filtered image x'_i is

$$\begin{aligned} P(u, v, d, \theta) = \\ \xi\{(a_1, b_1), (a_2, b_2) \mid x'_i(a_1, b_1) = u, x'_i(a_2, b_2) = v, \\ |(a_1, b_1) - (a_2, b_2)| = d, < (a_1, b_1), (a_2, b_2) > = \theta \}, \end{aligned} \tag{17}$$

where $1 \leq a_1, a_2 \leq r_i,\ 1 \leq b_1, b_2 \leq s_i$, $x'_i(a_1, b_1)$, $x'_i(a_2, b_2)$ are two pixels in the positions (a_1, b_1), (a_2, b_2) of image x'_i, and u, v are the corresponding pixel values. d is the distance between (a_1, b_1) and (a_2, b_2), and θ is the angle between the two points and abscissa axis. ξ is used to calculate the number of elements in the set.

The gray-level co-occurrence matrix $P(u, v, d, \theta)$ is used to count the number of times that the pixel values u and v appear simultaneously. We set $d = 1, \theta = 0^\circ, 45^\circ, 90^\circ, 135^\circ$ as shown in Fig. 2. Thus, we can obtain four different gray-level co-occurrence matrices for image x'_i.

The entropy h_i of image x'_i is computed on the basis of the above gray-level co-occurrence matrix $P(u, v, d, \theta)$

$$h_i = -\sum_u \sum_v P(u, v, d, \theta) \log_2 P(u, v, d, \theta), \tag{18}$$

where $\theta \in \{0°, 45°, 90°, 135°\}$. We can acquire four image entropies h_i and compute the average $\bar{h}_i$ for image x_i'

$$\bar{h}_i = \frac{\sum_\theta h_i(\theta)}{4}. \tag{19}$$

Therefore, the image entropy set of the cover image set X is $H = \{\bar{h}_1, \bar{h}_2, \ldots, \bar{h}_n\}$. Finally we calculate the capacity c_i of cover image x_i with the size of $r_i \times s_i$ by using the below equation:

$$c_i = \frac{r_i s_i (\bar{h}_i - \bar{h}_{min})}{\bar{h}_{max} - \bar{h}_{min}}, \tag{20}$$

where $\bar{h}_{min}$ and $\bar{h}_{max}$ denote the minimum and maximum value in H, respectively.

To verify whether Eq. (20) is a proper way to denote the embedding capacity of a cover image, we randomly collect 100 images with the size of 512×512 from BOSSBase set [41] and calculate the capacity according to Eq. (20). We calculate the image entropy of covers and then obtain the estimated embedding capacity of cover images. Generally, secret information bits are supposed to embedded into the images with complex textures. Fig. 3 illustrates four typical cover images and their estimated embedding capacities. From left to right, the more complex the image content is, the higher embedding capacity the image has. We can observe that a highly textured image has higher embedding capacity.

For the cover image set $X = \{x_1, \ldots, x_n\}$, we obtain the image capacities $C = \{c_1, \ldots, c_n\}$, and then sort them in a descending order $C_s = \{c_{s_1}, \ldots, c_{s_n}\}$. We embed the payload into the cover images according to the descending order of their image capacities, and the sub-payload m_{s_i} of each image is equal to its estimated capacity c_{s_i}. The total capacity of these images should not be less than the length of embedding payload $|M|$. Specifically, the payload distribution can be formulated as below:

$$|m_{s_i}| = \begin{cases} c_{s_i} & i = 1, 2, \ldots, p^* - 1 \\ |M| - \sum_{i=1}^{p^*-1} |m_{s_i}| & i = p^* \\ 0 & i = p^* + 1, p^* + 2, \ldots, n \end{cases}, \tag{21}$$

where p^* represents the fewest number of cover images satisfying the payload requirement, i.e.,

$$p^* = \arg \min_{1 \le p \le n} \sum_{i=1}^{p} c_{s_i} \ge |M|. \tag{22}$$

4.3 Embedding Strategy Based on Distortion Distribution (ES-DD)

ES-DD mainly distributes the embedding payload depending on the distribution of distortion values. Note that the impact of embedding modifications can be measured using a distortion function between the cover image and stego image, which is assumed to be related to statistical detectability of embedding changes. By applying the modern distortion function to cover image, we can obtain the distortion values. For example, for a given cover image, the pixel matrix is $\mathbf{I}$, and the distortion values matrix $\boldsymbol{\varrho}$ can be computed by adopting the distortion function in HILL [9] as follows:

(a) (b) (c) (d)

Fig. 3. The estimated embedding capacities of four typical images from BOSSbase set by using the proposed ES-ITC strategy. (a) "92.pgm", $c = 80,591$ (b) "1.pgm", $c = 94,005$ (c) "59.pgm", $c = 215,389$ (d) "10.pgm", $c = 230,669$.

$$\boldsymbol{\varrho} = \frac{1}{|\mathbf{I} \otimes \mathbf{H}^{(1)}| \otimes \mathbf{L}_1} \otimes \mathbf{L}_2, \tag{23}$$

where $\mathbf{H}^{(1)}$ is the 3×3 KerBöhme high-pass filter, and $\mathbf{L}_1$ and $\mathbf{L}_2$ are 3×3 and 15×15 average low-pass filters, respectively. $\otimes$ stands for the operation of mirror-padded convolution.

The above filter-based cost function utilizes a high-pass filter and two low-pass filters to locate the less predictable parts in an image. It is worth mentioning that the cost value for one pixel is calculated by the local region pixels, i.e., the distortion cost is determined by the local texture and complexity. Thus, we think that the distortion function is a universal and general measurement for all the pixels in different images, not just for one cover image.

All the pixels of the cover images in the cover image set X are sorted in an ascending order based on their distortion values and only the first $|M|$ pixels will be the pixels for data embedding, where $|M|$ is the length of embedding payload.

In this paper, we denote a pixel set S consisting of these chosen pixels. ES-DD strategy distributes the payload into multiple images as follows. For a given cover image x_i with the size of $r_i \times s_i$, if there exist some pixels belonging to S, the cover image x_i would be selected for embedding. The length of the sub-payload is the number of selected pixels in x_i for data embedding. Specifically, assuming $x_i(a, b)$ represents the pixel in the position (a, b) of cover image x_i, the length of the corresponding sub-payload m_i can be computed by using the below equations:

$$|m_i| = \sum_{1 \le a \le r_i} \sum_{1 \le b \le s_i} f(x_i(a, b)), \tag{24}$$

where $f(z)$ is an indicator function defined as

$$f(z) = \begin{cases} 1, & z \in S \\ 0, & z \notin S \end{cases}. \tag{25}$$

4.4 Computational Complexity Analysis

In this subsection, we investigate the computational complexity of two proposed embedding strategies. For simplicity, suppose we have n cover images, and all images have the same size of $r \times s$. The proposed embedding strategy ES-ITC first traverses n cover images and computes each image capacity based on image entropy. The computation complexity of these operations is $O(nrs)$. Then all the images are sorted by their capacities. We, in priority, allocate the sub-payload to the cover images with the highest capacities until the total payload is completely distributed. The average

computation cost of the sorting and allocation is $O(n\log n)$. Therefore, if $r \times s > \log n$, the computation complexity of ES-ITC is $O(nrs)$. Otherwise, the computation complexity is $O(n\log n)$. In the proposed embedding strategy ES-DD, the distortion values of all pixels in n cover images are computed, and its computation complexity is $O(nrs)$. Then all pixels are sorted in an ascending order based on their distortion values, and the embedding payload M is allocated according to the distribution of the first $|M|$ pixels in the ascending order, which costs $O(nrs\log(nrs))$. In total, the computation complexity of ES-DD is $O(nrs\log(nrs))$. Therefore, the new multiple images steganographic schemes incorporated with the proposed strategies ES-ITC and ES-DD could be solved in polynomial time.

5 Experimental Results

In this section, several comparative experiments are presented to demonstrate the effectiveness of two proposed payload distribution strategies ES-ITC and ES-DD. Section 5.1 introduces detailed experimental procedures. Sections 5.2 and 5.3 respectively show the experimental results of comparing the proposed strategies ES-ITC, ES-DD with the intuitive strategy ES-UPD and the state-of-the-art strategy IMS. In Section 5.4, we compare the numerical results of embedding payload distribution for different payload distribution strategies. Section 5.5 provides experimental results in terms of per image detection performance and compares the results. We also incorporate the idea of adaptive batch size [26] into our proposed strategies in Section 5.6.

5.1 Experimental Procedures

In the steganography and steganalysis framework, we suppose that some actors transmit multiple images respectively, and the steganalyzer detects all the images and knows their senders. The blind universal pooled steganalysis can detect the guilty actors relative accurately. The guilty actors represent outliers in the feature space, and they could be identified by an outlier detection algorithm. In this paper, we evaluate the security and undetectability of multiple images steganographic schemes using the state-of-the-art blind universal pooled steganalysis [36]. The pooled steganalysis aims to identify a guilty actor or actors, who have executed steganographic operations on the corresponding images. The local outlier factor (LOF) method [42] is used to measure the possibility that an actor is guilty. We use the LOF values to rank the actors according to their guiltiness. The larger LOF value is, the higher ranking the actor is, and the actor will be identified as guilty with higher probability.

In the following experiments, WOW [7], S-UNIWARD [8], HILL [9] and MiPOD [15] are combined with the payload distribution strategies to evaluate the performance. In WOW, the Hölder-norm parameter in the aggregation rule $p = -1$. In S-UNIWARD, we use the 8-tap Daubechies directional filter bank and the stabilizing constant $\alpha = 1$. In HILL, the high-pass filter is the 3×3 Ker-Böhme filter, and two low-pass filters are 3×3 and 15×15 average filters, respectively. In MiPOD, we use a two dimensional Wiener filter with the width of $w = 2$, and medium blocks with the means of $p = 9$ and $l = 9$.

Following the experiment setting in ref. [24], we set the average payload rate $\overline{R}$ bpp (bits per pixel) in our paper. Suppose we have n cover images and all images have the same size $r \times s$, the total length of the messages embedded into batch images will be equal to $\overline{R}nrs$ bits. In content-adaptive steganographic algorithms, the maximum embedding rate is usually set as 0.5. Thus, in our experiments we investigate the cases that the average embedding rate $\overline{R}$ ranges from 0.1 to 0.5.

In the experiments, we assume only one guilty actor out of total n_a actors, because the performance of the blind universal pooled steganalyzer is best in this case [36]. We carry out the experiments by adopting all pairs of the payload distribution strategies and the embedding algorithms for different numbers of actors. In the following experiments, the testing images are all from the BOSSBase set [41] which contains 10,000 gray-scale images with a size of 512×512. The detailed procedures are as below.

1) Randomly divide n cover images into n_a groups, and each group of images has one actor. The number of cover images per actor is $n_i = n/n_a$. Randomly select one guilty actor out of n_a actors. The guilty actor embeds the payload into cover images.
2) Extract features from all images of n_a actors. Since SRM steganalytic method [43] could detect the tested embedding algorithms accurately, we utilize it to extract 34,671-dimensional features for all the images.
3) Group the extracted features by the actor, and calculate the distances between all pairs of two actors based on their features using the maximum mean discrepancy [44].
4) Finally, we compute the guiltiness of each actor by using LOF method and acquire the LOF values of all actors.

We obtain the average LOF values of all actors over an ensemble of 10 independent trials of the experiments, and evaluate the performance by the guilty actor's ranking. Compare the guilty actor's rankings in different multiple images steganographic schemes, and then acquire the comparison results of security performance.

5.2 Comparison With ES-UPD Against the Blind Universal Pooled Steganalysis

In this subsection, we mainly show the experimental results to compare the performance of the proposed payload distribution strategies ES-ITC, ES-DD and the intuitive strategy ES-UPD resisting the blind universal pooled steganalysis.

In this experiment, WOW [7], S-UNIWARD [8] and HILL [9] are incorporated with the payload distribution strategies ES-ITC, ES-DD and ES-UPD. The number of actors $n_a \in \{10, 20, 40\}$. For each n_a, divide the 10,000 images from BOSSBase set into n_a groups, each of which is assigned to one actor randomly. The number of cover images per actor n_i is equal to $10000/n_a$.

Tables 1, 2, and 3 respectively show the average LOF values of all actors under five payload rates by combining the payload distribution strategies ES-UPD, ES-ITC, ES-DD, when the number of actors is 10 and the embedding algorithm is WOW. The average LOF values of all actors with the

TABLE 1
Experimental Results by Combining ES-UPD With WOW Against the Blind Universal Pooled Steganalysis

Ranking	0.1 bpp	0.2 bpp	0.3 bpp	0.4 bpp	0.5 bpp
1	1.2372	1.2352	1.2241	1.1518	1.3151
2	1.2369	1.1219	1.1415	1.1367	1.1058
3	1.1159	1.1142	1.1118	1.1367	1.1033
4	1.1147	1.1128	1.1048	1.1278	1.0803
5	1.0759	1.0742	1.0947	1.0911	1.0452
6	1.0505	1.0489	1.0793	1.0517	1.0074
7	1.0314	1.0381	1.0394	0.9807	0.9394
8	0.9759	0.9745	0.9657	0.9194	0.9112
9	0.9481	0.9466	0.9381	0.9117	0.8807
10	0.8591	0.8578	0.8500	0.8897	0.8522

The underline results are the average LOF values of the guilty actor.

TABLE 2
Experimental Results by Combining ES-ITC With WOW Against the Blind Universal Pooled Steganalysis

Ranking	0.1 bpp	0.2 bpp	0.3 bpp	0.4 bpp	0.5 bpp
1	1.2399	1.2398	1.2380	1.2586	1.2340
2	1.1261	1.1339	1.2128	1.2324	1.2312
3	1.1183	1.1183	1.1904	1.2299	1.2056
4	1.1183	1.1183	1.1166	1.1116	1.0874
5	1.0783	1.1170	1.1166	1.1116	1.0874
6	1.0526	1.0527	1.0512	1.0464	1.0563
7	1.0222	1.0161	0.9939	1.0080	1.0484
8	0.9781	0.9780	0.9623	0.9444	0.9307
9	0.9501	0.9501	0.9487	0.9340	0.9137
10	0.8610	0.8609	0.8597	0.8558	0.8372

The underline results are the average LOF values of the guilty actor.

same payload rate are sorted in descending order. The underline results are the average LOF values of the guilty actor. The higher the guilty actor ranking, the higher probability that the guilty actor is identified, i.e., the lower security performance of multiple images steganography. It is shown that the guilty actor's rankings are 7, 7, 7, 7, 3 by ES-ITC, 7, 7, 7, 7, 7 by ES-DD and 7, 7, 6, 2, 1 by ES-UPD, respectively. ES-UPD has comparable performance against the blind universal pooled steganalysis algorithm in small payload case, compared with the proposed ES-ITC and ES-DD. However, when the payload quantity becomes large, the guilty actor is much easier to be identified than our proposed strategies. We can see that adaptive payload allocation is effective and considerable in multiple images steganography.

TABLE 3
Experimental Results by Combining ES-DD With WOW Against the Blind Universal Pooled Steganalysis

Ranking	0.1 bpp	0.2 bpp	0.3 bpp	0.4 bpp	0.5 bpp
1	1.2390	1.2411	1.2438	1.2459	1.2284
2	1.1255	1.1273	1.1297	1.1367	1.1988
3	1.1178	1.1195	1.1219	1.1239	1.1924
4	1.1176	1.1195	1.1219	1.1238	1.1080
5	1.0775	1.0794	1.0817	1.1238	1.1080
6	1.0521	1.0539	1.0561	1.0579	1.0430
7	1.0251	1.0179	1.0090	0.9983	0.9972
8	0.9774	0.9791	0.9812	0.9829	0.9691
9	0.9495	0.9511	0.9532	0.9547	0.9413
10	0.8604	0.8619	0.8637	0.8652	0.8530

The underline results are the average LOF values of the guilty actor.

In order to illustrate the performance of the proposed embedding strategies clearly, more scenarios with different numbers of actors are considered. Fig. 4 shows the comparison results of the guilty actor's ranking by combining ES-ITC, ES-DD, ES-UPD with WOW, S-UNIWARD, HILL, when the number of actors is 10, 20, 40, respectively.

It can be observed that with the increase of embedding payload rates, all the guilty actor's rankings obtained by ES-ITC, ES-DD and ES-UPD become higher, and thus the security performance of multiple images steganography become worse. Furthermore, when the embedding payload rate is low, the security performance of ES-UPD is similar to that of ES-ITC and ES-DD. When the embedding payload rate is large, such as 0.3 bpp, the guilty actor's rankings are much higher obtained by ES-UPD than the proposed ES-ITC and ES-DD, indicating that the proposed ES-ITC and ES-DD are more resistant to the steganalysis in large payload scenario.

5.3 Comparison With IMS Against the Blind Universal Pooled Steganalysis

In this subsection, we compare ES-ITC, ES-DD with the state-of-the-art strategy IMS [24]. The number of actors n_a is fixed to 20, and the numbers of cover images per actor n_i are set to 100 and 200, respectively. The comparison results are presented in Fig. 5. It can be observed that the guilty actor's rankings obtained by ES-DD and IMS are comparative, and thus the security performance of ES-DD is similar to that of IMS. The performance of ES-ITC is somewhat worse than that of ES-DD and IMS, and the performance

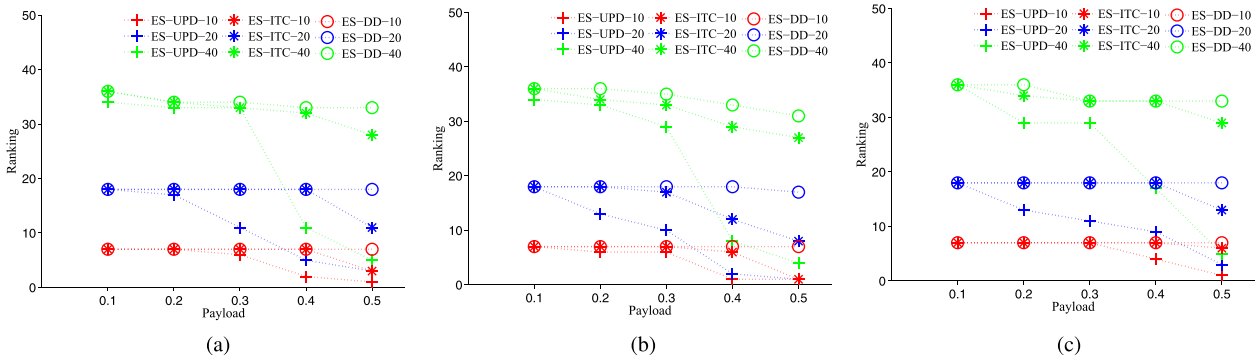


Fig. 4. Comparisons of ES-ITC, ES-DD, ES-UPD with WOW (a), S-UNIWARD (b), HILL (c) when the numbers of actors are 10 (red color), 20 (blue color) and 40 (green color).

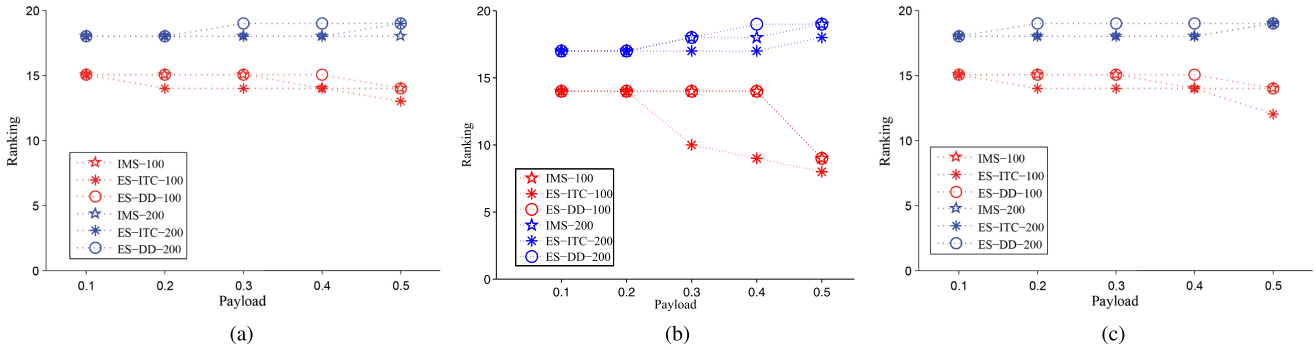


Fig. 5. Comparisons of ES-ITC, ES-DD, IMS with WOW (a), S-UNIWARD (b), HILL (c) when the number of actors is 20, and the number of cover images per actor are 100 (red color), 200 (blue color).

gap would widen with the increase of the number of cover images per actor and the embedding payload.

Furthermore, we combine the payload distribution strategies ES-ITC, ES-DD, IMS, ES-UPD with the state-of-the-art embedding algorithm MiPOD [15], and compare the security performance. It is worth noting that, we individually include the embedding algorithm MiPOD in the experiment due to the specific way this algorithm works. It does not try to minimize the probability of embedding distortion (such as WOW, S-UNIWARD, HILL), and its distortion function is based on the detectability. In this experiment, the number of actors n_a is set to 20, and the numbers of cover images per actor n_i are 100 and 200. Fig. 6 shows the comparison results of the guilty actor's rankings. By incorporating with the embedding algorithm MiPOD, compared with ES-UPD, the guilty actor's rankings obtained by ES-ITC, ES-DD, IMS are lower and thus they could acquire large enhancement of anti-steganalysis performance. The security performance of ES-DD, IMS are substantially similar, and they are slightly better than that of ES-ITC, especially for higher payload rates.

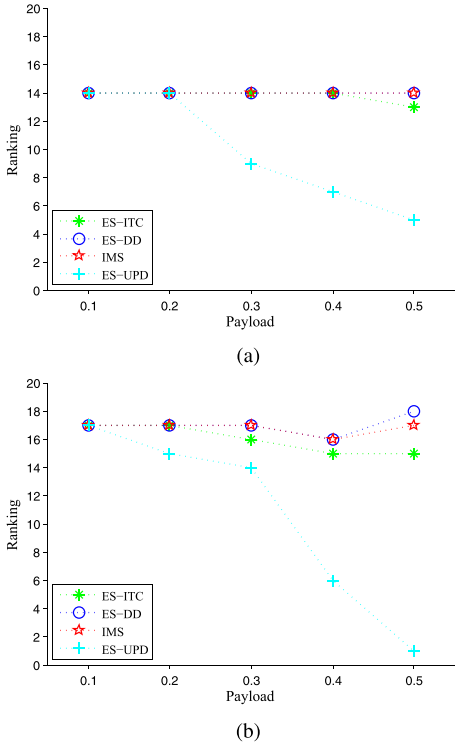


Fig. 6. Comparisons of ES-ITC, ES-DD, IMS, ES-UPD with MiPOD when the number of actors is 20, and the numbers of cover images per actor are 100 (a) and 200 (b).

Note that IMS deals with all cover images as a big image concatenation, and computes the cost values directly from the image concatenation, which is difficult for multiple cover images with different image sizes. The operations of ES-ITC and ES-DD are easy to implement, thus it is wiser for a steganographer to use ES-ITC and ES-DD instead of IMS in practical applications.

5.4 Numerical Results of Embedding Payload Distribution for Different Payload Distribution Strategies

This subsection provides the numerical distribution of embedding payload for multiple images, showing the difference of these payload distribution strategies ES-ITC, ES-DD, IMS. Note that in the intuitive strategy ES-UPD, the embedding payload for each image is invariant, thus we ignore them in the figures. Obviously, the payload distribution for ES-ITC, ES-DD, IMS are different from ES-UPD.

It can also be observed in Fig. 7, in the proposed ES-ITC strategy, the assigned sub-payload for some cover images are zero and these innocent images are used to confound the detector. ES-ITC attempts to embed the payload into as fewer images as possible. For ES-DD and IMS, although the assigned sub-payload for each image is similar, the numerical results of payload distribution by IMS are scattered, i.e., the variance of numerical sub-payloads is larger. In all, the numerical distributions of embedding payload for ES-ITC, ES-DD, IMS are completely diverse.

5.5 Anti-Detection Performance Against SRM Steganalysis

In this subsection, in order to comprehensively compare the security performance of the payload distribution strategies ES-ITC, ES-DD, IMS, ES-UPD, we provide the numerical results in terms of per image detection performance against the state-of-the-art image steganalyzer SRM [43].

Suppose the steganographer has been identified successfully by the blind universal pooled steganalysis, we further apply the 34,671-dimensional SRM feature set with the ensemble classifiers to the guilty actor's images. 5,000 and 5,000 images are chosen randomly as training/validation and testing set, respectively. The detection performance is quantified

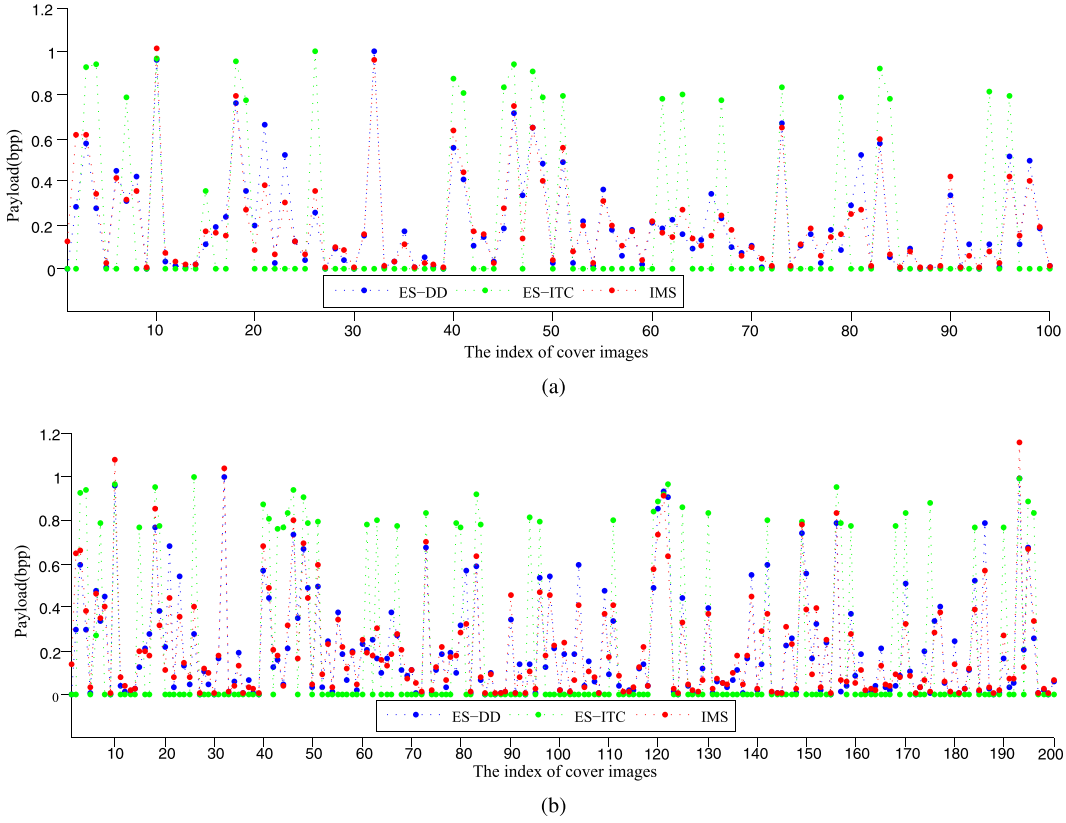


Fig. 7. The numerical results of payload distribution among 100 (a) and 200 (b) guilty actor's images for the payload distribution strategies ES-ITC, ES-DD and IMS when the payload rate is 0.2 bpp and the embedding algorithm is WOW. Note that in ES-UPD strategy, the embedding payload for each image is 0.002 and 0.001, respectively, hence we ignore them in the figures.

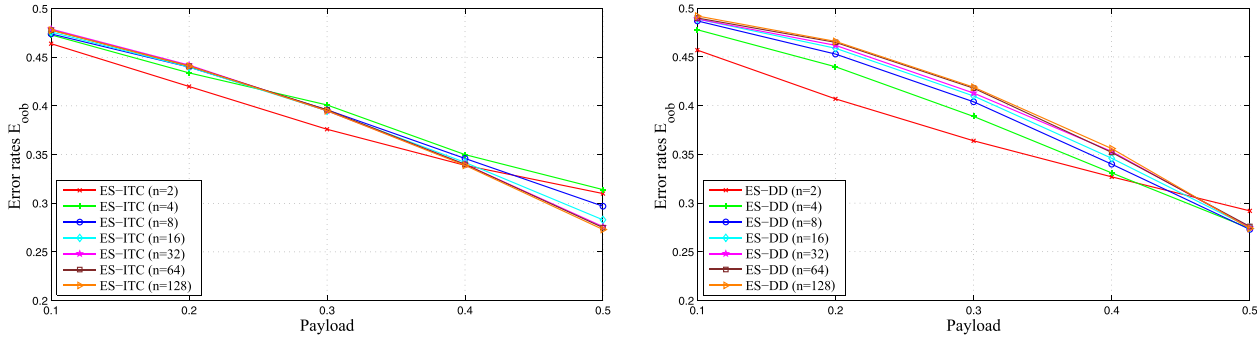
by the ensemble's "out-of-bag" error rate E_{oob}, which is the sum value of the false positive rate and the false negative rate. The greater E_{oob} is, the better steganographic security is. We carry out the experiment 10 times by randomly splitting the training and testing images and calculate the average E_{oob} value, which is expressed in percentage. The comparative performance of four payload distribution strategies ES-ITC, ES-DD, IMS, ES-UPD with four embedding algorithms WOW, S-UNIWARD, HILL, MiPOD are given in Table 4. It can be observed that with the increase of embedding payload rates, the detection error rates are decreased, i.e., the security performance of multiple image steganography is decreased. Compared with ES-UPD, the proposed payload distribution strategies ES-ITC, ES-DD could obtain more than 3 percent improvements in anti-steganalysis performance. Their steganographic security performance against SRM steganalysis is similar to that of IMS. Nevertheless, our proposed strategies do not require concatenation of all the cover images, which are much easier in practical implementation.

5.6 Adaptive Batch Size Image Steganography

As ref. [26] pointed out, better undetectability is achieved by using a larger batch size in low payloads, and it is secure to employ a smaller batch size for high payloads. Following this principle, we execute ES-ITC and ES-DD by batching images with size n, where n depends on the payload. In our experiments, assume the batch size n to be the power of 2, and the largest batch size is 128. 4,096 cover-stego pairs are randomly selected for training/validation, and another 4,096 cover-stego pairs are used for testing. Combining with HILL, we conduct the experiments of two proposed ES-ITC and ES-DD in different payloads with various batch sizes ($n = 2, 4, 8, 16, 32, 64, 128$). We further evaluate the security performance of ES-ITC and ES-DD by using 34,671-dimensional maxSRMd2 feature set [45] with the ensemble classifier.

TABLE 4
Comparisons of Error Rates E_{oob} for Per Image Detectability Against SRM Steganalysis

Embedding Algorithm	Payload Distribution Strategy	Payload				
		0.1	0.2	0.3	0.4	0.5
WOW	ES-ITC	0.484	0.454	0.410	0.389	0.333
	ES-DD	0.481	0.454	0.415	0.357	0.275
	IMS	0.481	0.453	0.423	0.356	0.286
	ES-UPD	0.443	0.403	0.341	0.296	0.242
S-UNIWARD	ES-ITC	0.488	0.435	0.400	0.361	0.321
	ES-DD	0.480	0.454	0.411	0.343	0.276
	IMS	0.479	0.451	0.401	0.348	0.279
	ES-UPD	0.450	0.393	0.326	0.281	0.233
HILL	ES-ITC	0.491	0.451	0.420	0.392	0.343
	ES-DD	0.483	0.462	0.439	0.397	0.363
	IMS	0.484	0.463	0.434	0.389	0.318
	ES-UPD	0.448	0.412	0.362	0.335	0.267
MiPOD	ES-ITC	0.488	0.451	0.421	0.397	0.354
	ES-DD	0.482	0.468	0.436	0.393	0.348
	IMS	0.482	0.462	0.448	0.411	0.359
	ES-UPD	0.441	0.409	0.356	0.320	0.281



(a) ES-ITC (b) ES-DD

Fig. 8. Detection error rates E_{oob} against maxSRMd2 steganalysis in different payloads for ES-ITC and ES-DD with different batch sizes ($n = 2, 4, 8, 16, 32, 64, 128$).

The experimental results in Fig. 8 show that using larger batch size in ES-ITC and ES-DD can improve the performance at lower payload, which is consistent with the theorem in ref. [26]. The security performance of ES-ITC is improved by increasing the batch size for low payloads, while small batch sizes would obtain improvements for larger payloads. ES-DD with larger batch sizes is less vulnerable to steganalysis for different payloads except for 0.5 bpp, i.e., using larger batch size results in high detection error in small payloads. It can be observed that the idea of adjusting batch size dynamically can also be applicable to our proposed strategies, and improve the undetectability significantly. We present the comparisons among ES-ITC, ES-DD with adaptive batch size, and AdBIM against maxSRMd2 steganalysis, as shown in Table 5. Compared with ES-DD and AdaBIM, ES-ITC has slightly lower security performance. The performance of ES-DD is slightly better than that of AdaBIM in low payloads (no more than 0.2 bpp), while AdaBIM is better with the increase of payload.

6 Discussions

In this paper, we propose two payload allocation strategies ES-ITC and ES-DD for multiple image steganography. Compared with the intuitive strategy ES-UPD, ES-ITC and ES-DD distribute the embedding payload in each cover image adaptively, according to image texture features. As Figs. 4, 5, and 6 are shown, ES-ITC and ES-DD have better resistance against universal pooled steganalysis, especially in large payload cases. As far as we are concerned, there are two reasons: 1) Two proposed strategies distribute the embedding payload according to the estimated secure capacity of the cover images, guaranteeing that the amount of the embedded secret data does not exceed the "maximum secure capacity" of the individual covers, which makes these images more resistance to steganalysis. 2) Two proposed strategies assign different payload quantities to different cover images, which makes the opponents much harder to guess the payload allocations than ES-UPD. Therefore, the allocated payload should be dependent on the given cover image instead of uniform payload distribution among the group of cover images, in order to obtain anti-steganalysis performance enhancement. It also shows that a suitable payload distribution strategy is essential in multiple images steganography.

TABLE 5
Comparisons of Error Rates E_{oob} Among ES-ITC, ES-DD With Adaptive Batch Size, and AdaBIM Against maxSRMd2 Steganalysis

Payload Distribution Strategy	Payload				
	0.1	0.2	0.3	0.4	0.5
ES-ITC with adaptive batch size	0.479	0.442	0.401	0.350	0.314
ES-DD with adaptive batch size	0.492	0.466	0.419	0.356	0.292
AdaBIM	0.491	0.463	0.422	0.373	0.317

In the proposed strategy ES-ITC, we assign the amount of the sub-payload in each image, according to the image capacity derived from image texture complexity. Image texture complexity would be changed after data embedding. The steganalyst has to estimate the image capacity from the stego images, rather than the cover images, leading to inaccurate approximations. Thus, the payload distribution estimated from stego images in ES-ITC does not guarantee to preserve the order recoverability. For the proposed strategies ES-DD, all the pixels of the cover images are sorted in an ascending order based on their distortion values, and only the first $|M|$ pixels will be embedded data, where $|M|$ is the length of embedding payload. Due to the modification by data embedding, it would lead to a rough approximation for the statistical distribution of distortion costs from the stego images. Thus, in the proposed strategy ES-DD, the payload distribution estimated from stego images also does not guarantee to preserve the order recoverability. In all, in the two proposed strategies, the image texture features are not perfectly invariant, and the payload distribution has good unrecoverability. Even if a steganalyst has the knowledge of the allocation quantity of the sub-payload chunks, it is still difficult to recover the correspondence of the sub-payload chunks to the cover images only from the stego images. The related experimental results (Table 4) in terms of per image detection performance have shown that the detection error rates of ES-ITC and ES-DD are greater than those of ES-UPD. It indicates that the uneven allocation of the sub-payload in the cover images enhances the steganalyst's difficulty to determine the quantity of the sub-payload in each image, increasing resistance to the modern single image steganalyzer.

Compared with ES-DD and IMS, the security performance of ES-ITC is slightly low, especially for higher

payload rates (Figs. 5 and 6). When the embedding payload rate is higher, the greedy algorithm in ES-ITC is prone to concentrate the embedding payload in cover images with high security capacity in priority, which might result in more embedding changes concentrated in textured images. Note that the modern steganalyzer is trained to learn the difference between cover images and stego images, and ES-ITC would increase the difference in the textured images. Thus, ES-ITC might be a litter easier for the modern steganalyzers to learn and obtain the steganalysis features.

Both ES-DD and IMS are based on the embedding distortion, and their security performance against the modern universal pooled steganalysis and single image steganalyzer are similar. However, Fig. 7 has shown the difference of the numerical results of payload distribution between ES-DD and IMS. We think that such a difference mainly comes from distinct approaches of distortion value computation. In IMS strategy, all cover images are concatenated into a new big image, and then the embedding payload is distributed through the cost values directly computed from the concatenation of all cover images, resulting in higher cost values in the joint. Further, when the cover image set is large, the concatenation implementation requires large memory. Moreover, the implementation becomes complex if the cover images are with different sizes. In contrast, ES-DD avoids the above issues by individually computing the distortion values of all pixels in the cover image set, and the payload is allocated to each image according to the distortion distribution. Note that the most effective image steganographic schemes are based on designing a distortion function to minimize statistical detectability. Since ES-DD mainly allocates more payloads to cover images with fewer distortions values, in this sense, ES-DD strategy is undetectability optimal.

As ref. [27] pointed out, a steganographer must act identically to any casual user of the communication channel, which implies hiding also the use of steganographic software, and destroying cover images. Generally, the sender/receiver could execute data embedding/extracting operations in steganographic schemes offline, and thus conceal the special steganographic software [46]. Furthermore, in order to avoid security pitfalls, a steganographer could select cover images by herself, and the input cover images of the special steganographic software should not be reused. Thus, the adversary (steganalyst) who focuses on monitoring the communication channel does not know whether the images are processed by the special steganographic software and embedded with messages or not.

Generally, one engaging in covert communication can always apply a cryptographic algorithm to the data before embedding it to achieve additional security [47]. Thus, in a practical application, the embedding payload could be considered as pseudorandom bitstream [48]. In our steganographic schemes, a steganographer first splits the bitstream into several segments according to the proposed embedding strategies, and then embed these segments into multiple images. It would be meaningless if an adversary has only one of the stego images and recover a small part of the covert content from it. However, the intended recipient could recover the embedding payload from multiple images. Specifically, the intended recipient first extracts the segment from each image, and then combines these segments into the whole bitstream. Finally, decrypt the bitstream and obtain the original covert messages.

7 Conclusion

In this paper, we mainly investigate payload distribution in multiple images steganography. To highlight the key problems and analyze the theoretical security, a systematic framework for adaptive payload distribution based on image texture features is presented, which could be regarded as the general-purpose methodology that creates the new multiple images steganographic schemes. We propose two payload allocation strategies based on image texture complexity (ES-ITC) and distortion distribution (ES-DD), which could be incorporated into these state-of-the-art single image steganographic algorithms. Extensive experimental results demonstrate that the proposed strategies could obtain better security performance in multiple images steganography.

We believe that multiple images steganography is of significance to both theoretical approaches and practical implementations. Since the JPEG format can achieve not only higher compression rate but also good visual quality, JPEG images are prevalent and widely used on the Internet. In the future, we plan to extend the proposed payload distribution strategies to multiple JPEG images steganography.

Acknowledgments

This work was supported by National Natural Science Foundation of China (Grant Nos. 61972142 and 61772191), Hunan Provincial Natural Science Foundation of China (Grant No. 2020JJ4212) and Open Project Program of National Laboratory of Pattern Recognition (Grant No. 201900017).

References

[1] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 474–481, May 1998.

[2] A. Elatawy, Q. Duan, and E. S. Alshaer, "A novel class of robust covert channels using out-of-order packets," *IEEE Trans. Dependable Secure Comput.*, vol. 14, no. 2, pp. 116–129, Mar./Apr. 2017.

[3] W. Lu, Y. Xue, Y. Yeung, H. Liu, J. Huang, and Y. Shi, "Secure halftone image steganography based on pixel density transition," *IEEE Trans. Dependable Secure Comput.*, to be published, doi: 10.1109/TDSC.2019.2933621.

[4] Z. Qian, H. Zhou, X. Zhang, and W. Zhang, "Separable reversible data hiding in encrypted JPEG bitstreams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 6, pp. 1055–1067, Nov./Dec. 2018.

[5] L. Y. Zhang, Y. Zheng, J. Weng, C. Wang, Z. Shan, and K. Ren, "You can access but you cannot leak: Defending against illegal content redistribution in encrypted cloud media center," *IEEE Trans. Dependable Secure Comput.*, to be published, doi: 10.1109/TDSC.2018.2864748.

[6] B. Li, S. Tan, M. Wang, and J. Huang, "Investigation on cost assignment in spatial image steganography," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 8, pp. 1264–1277, Aug. 2014.

[7] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proc. IEEE Int. Workshop Inf. Forensic Security*, 2012, pp. 234–239.

[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, 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.*, 2014, pp. 4026–4210.

[10] T. Denemark and J. Fridrich, "Improving steganographic security by synchronizing the selection channel," in *Proc. ACM Workshop Inf. Hiding Multimedia Secur.*, 2015, pp. 5–14.

[11] B. Li, M. Wang, X. Li, S. Tan, and J. Huang, "A strategy of clustering modification directions in spatial image steganography," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1905–1917, Sep. 2015.
[12] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Proc. Int. Workshop Inf. Hiding*, 2010, pp. 161–177.
[13] J. Fridrich and J. Kodovský, "Multivariate Gaussian model for designing additive distortion for steganography," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, 2013, pp. 2949–2953.
[14] V. Sedighi, J. Fridrich, and R. Cogranne, "Content-adaptive pentary steganography using the multivariate generalized Gaussian cover model," in *Proc. SPIE, Media Watermarking Secur. Forensics*, 2015, pp. 0H01–0H13.
[15] 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.
[16] M. Sharifzadeh, M. Aloraini, and D. Schonfeld, "Quantized Gaussian embedding steganography," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, 2019, pp. 2637–2641.
[17] A. D. Ker, "Batch steganography and pooled steganalysis," in *Proc. Int. Workshop Inf. Hiding*, 2006, pp. 265–281.
[18] A. D. Ker, "Batch steganography and the threshold game," in *Proc. Int. Conf. Secur. Steganography Watermarking Multimedia Contents*, 2007, pp. 401–413.
[19] A. D. Ker, "Steganographic strategies for a square distortion function," in *Proc. Int. Conf. Secur. Forensics Steganography Watermarking Multimedia Contents*, 2008, pp. 401–413.
[20] A. D. Ker, "A capacity result for batch steganography," *IEEE Signal Process. Lett.*, vol. 14, no. 8, pp. 525–528, Aug. 2007.
[21] A. D. Ker, "Perturbation hiding and the batch steganography problem," in *Proc. Int. Workshop Inf. Hiding*, 2008, pp. 45–49.
[22] A. D. Ker and T. Pevný, "Batch steganography in the real world," in *Proc. ACM Workshop Multimedia Secur.*, 2012, pp. 1–10.
[23] Z. Zhao *et al.*, "Embedding strategy for batch adaptive steganography," in *Proc. Int. Workshop Digit. Watermarking*, 2016, pp. 494–505.
[24] 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.*, 2017, pp. 2122–2126.
[25] M. Sharifzadeh *et al.*, "A new parallel message-distribution technique for cost-based steganography," 2017. [Online]. Available: https://arxiv.org/abs/1705.08616
[26] M. Sharifzadeh, M. Aloraini, and D. Schonfeld, "Adaptive batch size image merging steganography and quantized Gaussian image steganography," *IEEE Trans. Inf. Forensics Security*, vol. 15, no. 1, pp. 867–879, 2020, doi: 10.1109/TIFS.2019.2929441.
[27] A. D. Ker *et al.*, "Moving steganography and steganalysis from the laboratory into the real world," in *Proc. ACM Workshop Inf. Hiding Multimedia Secur.*, 2013, pp. 45–48.
[28] X. Liao and J. Yin, "Two embedding strategies for payload distribution in multiple images steganography," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, 2018, pp. 1982–1986.
[29] 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.
[30] T. Filler and J. Fridrich, "Gibbs construction in steganography," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 705–720, Dec. 2010.
[31] 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.
[32] J. Kodovsky, J. Fridrich, and V. Holub, "On dangers of overtraining steganography to incomplete cover model," in *Proc. ACM Workshop Multimedia Secur.*, 2011, pp. 69–76.
[33] T. Pevný and J. Fridrich, "Benchmarking for steganography," in *Proc. Int. Workshop Inf. Hiding*, 2008, pp. 251–267.
[34] M. Kharrazi, H. T. Sencar, and N. Memon, "Cover selection for steganographic embedding," in *Proc. IEEE Int. Conf. Image Process.*, 2006, pp. 117–120.
[35] N. J. Hopper, J. Langford, and L. von Ahn, "Provably secure steganography," *IEEE Trans. Comput.*, vol. 58, no. 5, pp. 662–676, May 2009.
[36] A. D. Ker and T. Pevný, "The steganographer is the outlier: Realistic large-scale steganalysis," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 9, pp. 1424–11435, Sep. 2014.
[37] P. Schöttle, S. Korff, and R. Böttlehme, "Weighted stego-image steganalysis for naive content-adaptive embedding," in *Proc. IEEE Int. Workshop Inf. Forensics Security*, 2012, pp. 193–198.
[38] M. E. Jernigan and F. D'Astous, "Entropy-based texture analysis in the spatial frequency domain," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. PAMI-6, no. 2, pp. 237–243, Mar. 1984.
[39] V. Holub and J. Fridrich, "Optimizing pixel predictors for steganalysis," in *Proc. SPIE Media Watermarking Secur. Forensics*, 2012, pp. 1–13.
[40] W. Wang, J. Dong, and T. Tan, "Effective image splicing detection based on image chroma," in *Proc. IEEE Int. Conf. Image Process.*, 2010, pp. 1257–1260.
[41] P. Bas, T. Filler, and T. Pevný, "Break our steganographic system - The ins and outs of organizing boss," in *Proc. Int. Conf. Inf. Hiding*, 2011, pp. 59–70.
[42] M. M. Breunig *et al.*, "LOF: Identifying density-based local outliers," in *Proc. ACM SIGMOD Int. Conf. Manage. Data*, 2000, pp. 93–104.
[43] J. Fridrich and J. Kodovský, "Rich models for steganalysis of digital images," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 868–882, Jun. 2012.
[44] A. Gretton *et al.*, "A kernel method for the two-sample problem," in *Proc. Int. Conf. Neural Inf. Process. Syst.*, 2007, pp. 513–520.
[45] 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. Forensic Security*, 2014, pp. 48–53.
[46] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2009.
[47] S. Craver, "On public-key steganography in the presence of an active warden," in *Proc. Int. Workshop Inf. Hiding*, 1998, pp. 355–368.
[48] R. Böhme, *Advanced Statistical Steganalysis*. Berlin, Germany: Springer-Verlag, 2010.

Xin Liao (Member, IEEE) received the BE and PhD degrees in information security from the Beijing University of Posts and Telecommunications, Beijing, China, in 2007 and 2012, respectively. He was a visiting scholar with the University of Maryland, College Park, Maryland, from 2016 to 2017. He is currently an associate professor with Hunan University, Changsha, China, where he joined in 2012. His current research interests include image steganography, watermarking, and multimedia forensics.

Jiaojiao Yin received the BE degree in computer science from Henan Normal University, Xinxiang, China, in 2015, and the MS degree in computer science from Hunan University, Changsha, China, in 2018. Her current research interests include image steganography and watermarking.

Mingliang Chen received the BE and MS degrees in electronic information engineering from Shanghai Jiao Tong University, Shanghai, China, in 2013 and 2016, respectively. He is working toward the PhD degree with the Department of Electrical and Computer Engineering, University of Maryland, College Park, Maryland, since 2016. He received Jimmy H.C. Lin Award for Innovation from the University of Maryland, in 2019. His current interests include image processing, multimedia, and machine learning.

Zheng Qin received the PhD degree in computer software and theory from Chongqing University, Chongqing, China, in 2001. From 2010 to 2011, he served as a visiting scholar with the Department of Computer Science, Michigan State University. He is currently a professor with the College of Computer Science and Electronic Engineering, Hunan University, where he also serves as the vice dean. He also serves as the director of the Hunan Key Laboratory of Big Data Research and Application and the vice director of the Hunan Engineering Laboratory of Authentication and Data Security. His main interests include network and data security, privacy, data analytics and applications, machine learning, and applied cryptography.