A Strategy of Clustering Modification Directions in Spatial Image Steganography

Bin Li, *Member, IEEE*, Ming Wang, Xiaolong Li, Shunquan Tan, *Member, IEEE*, and Jiwu Huang, *Senior Member, IEEE*

***Abstract*— Most of the recently proposed steganographic schemes are based on minimizing an additive distortion function defined as the sum of embedding costs for individual pixels. In such an approach, mutual embedding impacts are often ignored. In this paper, we present an approach that can exploit the interactions among embedding changes in order to reduce the risk of detection by steganalysis. It employs a novel strategy, called clustering modification directions (CMDs), based on the assumption that when embedding modifications in heavily textured regions are locally heading toward the same direction, the steganographic security might be improved. To implement the strategy, a cover image is decomposed into several subimages, in which message segments are embedded with well-known schemes using additive distortion functions. The costs of pixels are updated dynamically to take mutual embedding impacts into account. Specifically, when neighboring pixels are changed toward a positive/negative direction, the cost of the considered pixel is biased toward the same direction. Experimental results show that our proposed CMD strategy, incorporated into existing steganographic schemes, can effectively overcome the challenges posed by the modern steganalyzers with high-dimensional features.**

***Index Terms*— Cost adjustment, distortion function, modification direction, steganalysis, steganography.**

I. Introduction

STEGANOGRAPHY [1]–[3] aims to hide secret messages into innocuous digital media without drawing suspicion. It faces challenges posed by modern steganalysis [4]–[11] which intends to detect the traces of data hiding. Currently, the most effective steganographic schemes [12]–[22] are based on minimizing a *distortion function* [23], [24] correlated with statistical detectability.

Manuscript received January 22, 2015; revised April 21, 2015; accepted May 4, 2015. Date of publication May 18, 2015; date of current version July 22, 2015. This work was supported in part by the 973 Program under Grant 2011CB302204, in part by the National Natural Science Foundation (NSF) of China under Grant U1135001, Grant 61332012, and Grant 61402295, in part by the Guangdong NSF under Grant 2014A030313557, and in part by the Shenzhen Research and Development Program under Grant JCYJ20140418182819173. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Patrick Bas.

B. Li, M. Wang, and J. Huang are with the College of Information Engineering, Shenzhen University, Shenzhen 518060, China, and also with the Shenzhen Key Laboratory of Media Security, Shenzhen 518060, China (e-mail: libin@szu.edu.cn; 2120130422@szu.edu.cn; jwhuang@szu.edu.cn).

X. Li is with the Institute of Computer Science and Technology, Peking University, Beijing 100871, China (e-mail: lixiaolong@pku.edu.cn).

S. Tan is with the College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, China, and also with the Shenzhen Key Laboratory of Media Security, Shenzhen 518060, China (e-mail: tansq@szu.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2015.2434600

The distortion function quantifies the effect of modifying an input cover object to the corresponding output stego object. A distortion function is considered *additive* when it is expressed as a sum of *costs*, which element-wisely evaluate the effect of respective embedding modification. Since near-optimal codes [25]–[27] perform well in minimizing the additive distortion, the research on additive distortion functions for spatial image steganography thrived over the recent years [12], [14]–[22]. The cost of a pixel in HUGO (highly undetectable stego) [12] is computed as a weighted sum of differences between feature vectors extracted from a cover image and their counterparts from a prospective stego image obtained by changing only the considered pixel. WOW (wavelet obtained weights) [15] assigns high costs to pixels which are more predictable by directional filters and low costs to less predictable pixels. S-UNIWARD (spatial universal wavelet relative distortion) [18]–[20] has a slightly modified cost function from WOW. S-UNIWARD and WOW have similar performance and they outperform HUGO. HILL (high-pass, low-pass, and low-pass) [21] further improves the cost function of WOW by using one high-pass filter and two low-pass filters. It follows the *spreading rule* [22] to make the embedding changes concentrated in textured areas, and performs better than WOW and S-UNIWARD.

The distortion introduced by data embedding is *non-additive* in essence, since there are inter-pixel correlations and interactions among embedding changes. Due to the fact that modern steganalysis has already exploited these facts by extracting features from high-order co-occurrence matrices, it is beneficial for steganography to follow. However, applying a non-additive function in steganography is more challenging as there are no practical codes capable of minimizing an arbitrary distortion function. Approximating the non-additive distortion function in an additive form is a good solution to balance the simplicity and effectiveness. Filler and Fridrich have made the first attempt by using the Gibbs construction [13], where three key techniques have been applied. Firstly, the distortion function is expressed as a sum of the local potentials (which can be regarded as a kind of costs) defined on cliques (a small group of pixels). In this way, practical codes for minimizing additive distortion can be applied. Secondly, an image is decomposed into several sub-lattices, where pixels within the same sub-lattice are separated by a distance larger than the support width of the potential function. Cost assignment and data embedding are performed in each sub-lattice sequentially. After embedding for a sub-lattice, the costs of pixels in the remaining sub-lattices are updated. In this way, the interactions among embedding changes have been taken

into consideration. A sweep denotes a single pass over all of the sub-lattices. Hence, thirdly, by repeating the embedding sweeps several times with a Gibbs sampler, it is hoped that the introduced embedding pattern will converge to a sample from optimal embedding. A practical implementation following this construction, is known as HUGO-BD (HUGO-bounding distortion) [28], and was originally proposed in [13]. It uses a distortion function expressed as an upper bound of the norm of the difference between feature vectors resulting from the HUGO-like procedure. HUGO-BD is better than its additive counterpart, HUGO, but it cannot outperform the recently proposed schemes with additive distortion functions [15], [18], [21]. It is also unclear how to adjust the existing additive schemes so that Gibbs construction could be applicable on them.

In this paper, we exploit embedding impacts to improve the performance of statistical undetectability for steganography. The major contribution is that we develop a new strategy, called *clustering modification directions* (CMD), which follows the clustering rule in our previous work [22] and can enhance the empirical steganographic security. We present a practical steganographic algorithm that assigns costs according to such a strategy and is easily applicable to the recently proposed additive schemes [15], [18], [21]. Specifically, we decompose a cover image into several sub-images. Distortion within a sub-image is defined in an additive form so that the existing practical steganographic codes [25]–[27] can be directly employed. The costs of pixels are firstly initialized by additive steganographic schemes such as [15], [18], and [21], and then are adjusted according to the modification directions of their neighboring pixels in the sub-images in which the data have been embedded. We intentionally differentiate the cost of increasing a pixel value and that of decreasing a pixel value so that the modifications would be locally oriented towards the same direction. Non-additivity is implicitly introduced into the overall distortion because the costs are dynamically updated. Experimental results show that although the proposed CMD strategy slightly increases the change rate (defined as the ratio of the modified pixels over the total number of pixels), it achieves better statistical undetectability against the state-of-the-art steganalyzers [7], [10], [11].

The rest of this paper is organized as follows. In Section II, we present the CMD strategy and show its effectiveness in improving steganographic security by a simulation. We give the algorithm that can implement the CMD strategy in Section III. To demonstrate the effectiveness of the proposed algorithm, we report extensive experimental results in Section IV, where the impacts of different parameters are shown, and the schemes incorporated with the proposed CMD strategy are compared to the state-of-the-art schemes, including HILL, S-UNIWARD, HUGO, and HUGO-BD. Finally, we conclude the paper in Section V.

II. Clustering Modification Directions and Steganographic Security

In this section, three effective rules for assigning costs in additive distortion functions are revisited. The proposed strategy, called clustering modification directions, is derived from one of the rules. The effectiveness of the strategy is tested in a simulation.

A. Revisiting the Rules in Cost Assignment

In our previous work [22], we have conceptually separated the cost assignment process into two phases. The first phase is to sort image elements according to their priorities. For effective priority ranking, three rules have been summarized: the complexity-first rule, the spreading rule, and the clustering rule. Following these rules, high priorities should be assigned to unpredictable pixels and their neighbourhoods, and embedding modifications should be clustered. The second phase is to assign costs according to a given distribution.

Since the two-phase cost assignment process is designed for additive distortion functions, it may not be immediately applicable in a non-additive case. Nevertheless, we note that the three rules may still be useful in the non-additive scenario. For instance, clustering embedding modifications in the neighborhood of unpredictable pixels should be beneficial to enhance the security of non-additive steganography as well. In fact, guiding the embedding modifications towards being clustered implicitly exploits the embedding impacts, and thus it will also be helpful in the non-additive case. We further investigate a special case of the clustering rule in the following.

B. The Strategy of Clustering Modification Directions

We have previously reported that under the same change rate, statistical undetectability can be improved by clustering the locations of embedding in local textured regions [22]. In this work, we further conjecture that not only the *locations* of embedding modifications, but also the *directions* of embedding modifications should be clustered to improve the undetectability performance. It can be regarded as a derivative strategy from the clustering rule, and we abbreviate it as CMD (clustering modification directions). Here the direction means the choice of positively or negatively changing the intensity of a pixel. For embedding schemes other than LSB (least significant bit) replacement, such as LSB matching (binary embedding), ternary embedding (± 1), and pentary embedding (both ± 2 and ± 1), we may have freedom to guide the directions by properly assigning costs. We discuss the ternary embedding case in this paper, where the magnitude of the change is limited to 1. For embedding schemes with larger magnitudes (e.g., pentary embedding), the allocation of different modification magnitudes is another issue that we intend to investigate in the future.

From the perspective of steganalysis, effective steganalytic schemes often detect the traces of data embedding by capturing the fluctuations, which act as high-frequency noise in an image. When embedding modifications are clustered and locally heading towards the same directions, the changes may act as low-frequency noise, which is blended into the image signal and may not deviate steganalytic statistics. Therefore, the CMD strategy may be effective in resisting steganalysis.

To verify whether the conjecture is reasonable, we perform a simulation as follows. Firstly, a number of 10,000 gray-scale

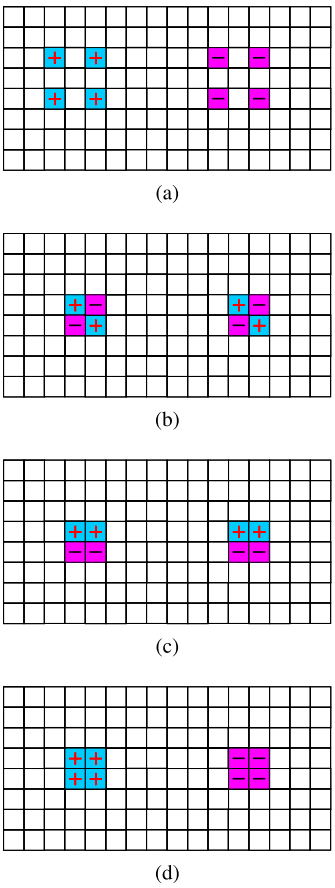


Fig. 1. Illustration of different noise patterns. The mark "+" stands for increasing the pixel value by one, and the mark "−" for decreasing by one. (a) Noise pattern A. (b) Noise pattern B. (c) Noise pattern C. (d) Noise pattern D.

images of size 512 × 512 pixels from BOSSBase ver 1.01 image database [29] are used as cover images. The images are divided into non-overlapping blocks of size 8 × 16. Then, a noise pattern is added to each image block to simulate the effect of data embedding. Four kinds of noise patterns are used, as illustrated in Fig. 1. Next, we compute the 686-dimensional SPAM (subtractive pixel adjacency matrix) steganalytic feature vector [5] for each image. The MMD (maximum mean discrepancy) [30], which quantifies the distance between the feature set of cover images and that of stego images, is computed for each noise pattern. Finally, we use the steganalyzer equipped with the 34,671-dimensional SRM (spatial rich model) features [7] and the ensemble classifiers [31] to evaluate the performance of each noise pattern on resisting steganalysis. A number of 5,000 randomly selected cover images and their corresponding stego counterparts are used for training. The remaining images are used for testing. The average value of the false positive rate and the false negative rate is computed as the classification error. The presence of a lower MMD or a higher classification error indicates a higher level of security.

It can be observed from Fig. 1 that the modification locations of Pattern A are more scattered than those of other three patterns, and the clustering effects of modification directions are increased from Pattern B to Pattern D. The obtained MMD values and the SRM evaluated classification errors are shown in Table I. The results show that Pattern A has the highest MMD value and the lowest classification error, while Pattern D has the lowest MMD value and the highest classification error. The evaluation results indicate that both the *locations* and the *directions* of the modifications have impacts on steganographic security. Therefore, it is reasonable to expect that the CMD strategy could be helpful to enhance steganographic security.

TABLE I
THE MMD AND THE STEGANALYTIC PERFORMANCE FOR FOUR NOISE PATTERNS

Noise Pattern	MMD	Steganalytic Classification Error
A	6.56×10^{-3}	1.05%
B	5.66×10^{-3}	1.35%
C	3.56×10^{-3}	5.19%
D	1.36×10^{-3}	12.55%

III. EMPLOYMENT OF THE CMD STRATEGY

In this section, we first clarify our methodology for designing steganography to implement the CMD strategy. Then we present a novel steganographic algorithm that adopts the CMD strategy by updating the costs. Next, we give an example to visualize its effect on embedding changes. Finally, we discuss the implementation details of the proposed algorithm and relevant parameters.

A. Methodology

It has been shown in Section II that when modification directions are more clustered, it is more difficult for steganalysis to reveal the traces of data embedding. In order to cluster modification directions, mutual embedding impacts should be considered. The following principles may be helpful in cost assignment to consider mutual embedding impacts:

1) It is not necessary to assign costs simultaneously.
2) Increasing a pixel value and decreasing a pixel value do not necessarily have the same cost.

These two principles were previously used to design HUGO [12] with additive distortion. In order to implement a steganographic scheme that not only follows the above principles, but also applies the CMD strategy, together with the fact that only steganographic codes for additive distortion are available, we propose the following solution. We first decompose the cover image into several portions, and accordingly divide the message data into several segments. The first segment of the message data is embedded into the first portion of the image. Next, the costs of the pixels in other portions of the image are updated according to the pixels that have already been modified. We can break the balance of the probability of increasing a pixel value and that of decreasing a pixel value via setting different costs for positive and negative changes. The remaining message data segments are sequentially embedded into the remaining portions of the image with the successively updated costs in sequence. In this way, any existing additive steganographic scheme [15], [17], [18], [20], [21] can be applied in data embedding for each

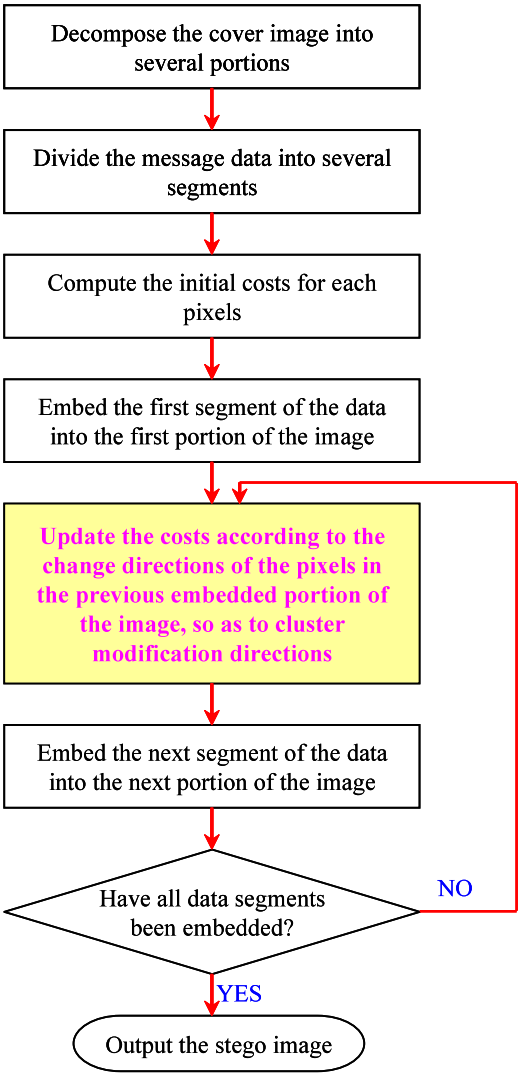


Fig. 2. Flowchart of the proposed solution to incorporate the CMD strategy.

image portion. We show the processing flow of the proposed solution in Fig. 2. Note that the most important stage is to update the costs in order to implement the CMD strategy. A practical steganographic algorithm that can follow such design methodology is described in the next subsection.

B. The Proposed CMD Algorithm

We use the upper case bold face typeset for a matrix, and the lower case for its element, *i.e.*, $\mathbf{C} = (c_{i,j})^{n_1 \times n_2}$, where n_1 and n_2 are the dimensions. We use $\mathbf{X}$ and $\mathbf{Y} \in \{0, \cdots, 255\}^{n_1 \times n_2}$ respectively to denote an 8-bit gray-scale cover image and its stego version. We consider the ternary embedding case, where $y_{i,j} \in \mathcal{I}_{i,j} = \{\min(x_{i,j}+1, 255), x_{i,j}, \max(x_{i,j}-1, 0)\}$. The cost of a pixel at location (i, j) is a triplet, *i.e.*, $\rho_{i,j} = (\rho^+_{i,j}, \rho^0_{i,j}, \rho^-_{i,j})$, where $\rho^+_{i,j}$ is the cost of increasing the pixel by one, $\rho^-_{i,j}$ is the cost of decreasing the pixel by one, and $\rho^0_{i,j}$ is the cost of not changing. We assume that $\forall i, j$, $\rho^0_{i,j} = 0$, hence if there is no modification, there is no distortion. For convenience, we use the symbols $\boldsymbol{\rho}^+ = (\rho^+_{i,j})^{n_1 \times n_2}$ and $\boldsymbol{\rho}^- = (\rho^-_{i,j})^{n_1 \times n_2}$ respectively to denote a matrix

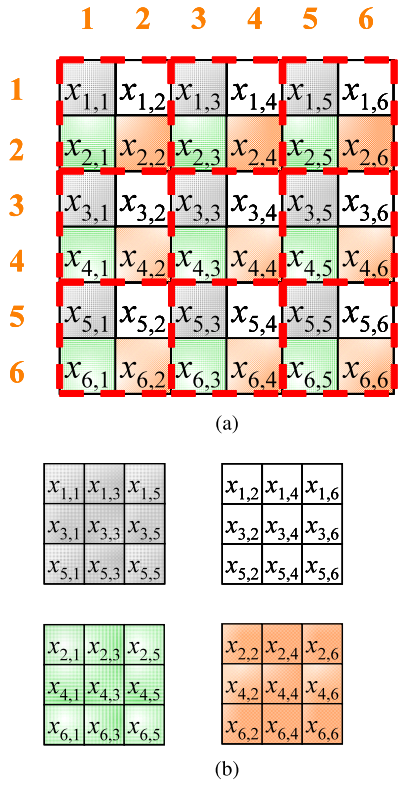


Fig. 3. An example of the division of an image into four disjoint sub-images. In a 2×2 sub-block of the sample image, the four elements are assigned to different sub-images. (a) A sample image of size 6×6 pixels. (b) Four sub-images.

representation of the corresponding costs. The detailed steps of the proposed algorithm are as follows.

1) Decompose the cover image into $L_1 \times L_2$ disjoint sub-images, where $L_1, L_2 \geq 1$. The index set of the pixels of a sub-image can be represented by

$$\begin{aligned} \mathcal{S}_{a,b} = \{(i,j) | i = a + k_a L_1,\ j = b + k_b L_2,\\ a \in \{1, \cdots, L_1\}, \quad k_a \in \{0, 1, \cdots, \lfloor \frac{n_1}{L_1} \rfloor - 1\},\\ b \in \{1, \cdots, L_2\}, \quad k_b \in \{0, 1, \cdots, \lfloor \frac{n_2}{L_2} \rfloor - 1\}\}, \end{aligned} \tag{1}$$

where $\lfloor \cdot \rfloor$ denotes the floor operator. Note that the decomposition corresponds to dividing the image into non-overlapping sub-blocks of size $L_1 \times L_2$, and the elements within each sub-block are from different sub-images. An example division of an image of size 6×6 pixels with $L_1 = L_2 = 2$ is shown in Fig. 3 (a). The image pixels $x_{1,1}$, $x_{1,3}$, $x_{1,5}$, $x_{3,1}$, $x_{3,5}$, $x_{3,5}$, $x_{5,1}$, $x_{5,3}$, and $x_{5,5}$ form the sub-image $\mathcal{S}_{1,1}$, and the image pixels $x_{1,2}$, $x_{1,4}$, $x_{1,6}$, $x_{3,2}$, $x_{3,4}$, $x_{3,6}$, $x_{5,2}$, $x_{5,4}$, and $x_{5,6}$ form the sub-image $\mathcal{S}_{1,2}$, and so on, as shown in Fig. 3 (b).
2) Given a piece of data payload of m bits, equally divide it into $L_1 \cdot L_2$ segments of length $m/(L_1 \cdot L_2)$ bits. Alternatively, we can choose to use segments with variable length.
3) Choose an embedding order for the sub-images. For convenience, we denote the sub-images by $\mathcal{S}_t$,

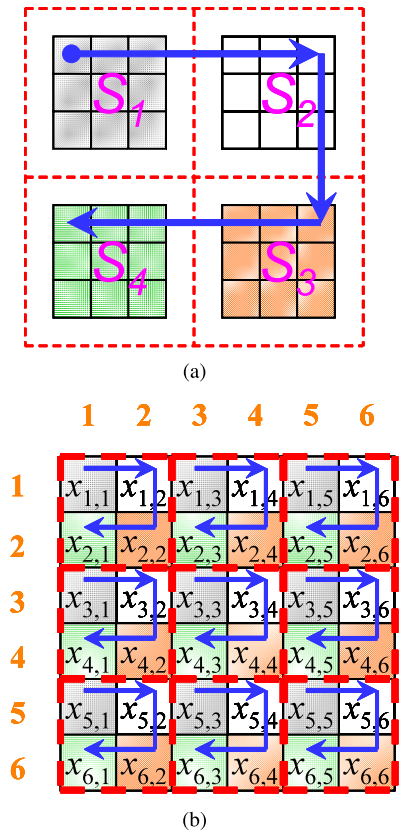


Fig. 4. Illustration of the embedding order. (a) An example embedding order for the four sub-images with horizontal zig-zag scan. (b) The embedding order in each sub-block of the sample image.

$t \in \{1, 2, \cdots, L_1 \cdot L_2\}$, where the index t specifies the order. As illustrated in Fig. 4 (a), assume we use a horizontal zig-zag order as the embedding order for the example image in Fig. 3 (a). Note that the elements in each sub-block are embedded in the same embedding order, as shown in Fig. 4 (b).

4) Start with $t = 1$. Initialize the stego image $\mathbf{Y} = \mathbf{X}$.
5) Compute the difference image between $\mathbf{Y}$ and $\mathbf{X}$, *i.e.*, $\mathbf{D} = \mathbf{Y} - \mathbf{X} = (d_{i,j})^{n_1 \times n_2}$.
6) Compute the *initial costs* of the image $\mathbf{Y}$ by adopting the cost assignment process from one of the existing additive steganographic schemes, such as WOW [15], S-UNIWARD [18], and HILL [21]. For example, by applying the cost assignment process in HILL, the initial costs are computed by

$$(c_{i,j})^{n_1 \times n_2} = \mathbf{C} = \frac{1}{|\mathbf{Y} \otimes \mathbf{H}| \otimes \mathbf{P_1}} \otimes \mathbf{P_2}. \tag{2}$$

In the above equation, $\mathbf{H}$ is a 3×3 KB (Ker–Böhme) high-pass filter [32], [33], $\mathbf{P_1}$ and $\mathbf{P_2}$ are respectively 3×3 and 15×15 average low-pass filters, and $\otimes$ stands for the operation of mirror-padded convolution. The operation $|\mathbf{A}|$ stands for taking the absolute value for each element in a matrix $\mathbf{A}$, and $\frac{1}{\mathbf{A}}$ for taking the reciprocal for each element. The initial costs will roughly determine where the embedding changes will be made in the image. We call this step *cost initialization*.

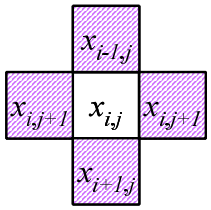


Fig. 5. The four-neighborhood $\mathcal{N}_{i,j}$ of the pixel at location (i, j).

7) If $t = 1$, set $\boldsymbol{\rho}^+ = \boldsymbol{\rho}^- = \mathbf{C}$. Otherwise, update the costs according to $\mathbf{D}$. Specifically, we use

$$\rho^+_{i,j} = \begin{cases} c_{i,j}/\alpha, & \text{if } \sum_{(i',j') \in \mathcal{N}_{i,j}} \delta(d_{i',j'} - 1) \\ & \quad > \sum_{(i',j') \in \mathcal{N}_{i,j}} \delta(d_{i',j'} + 1), \\ c_{i,j}, & \text{otherwise,} \end{cases} \tag{3}$$

and

$$\rho^-_{i,j} = \begin{cases} c_{i,j}/\alpha, & \text{if } \sum_{(i',j') \in \mathcal{N}_{i,j}} \delta(d_{i',j'} - 1) \\ & \quad < \sum_{(i',j') \in \mathcal{N}_{i,j}} \delta(d_{i',j'} + 1), \\ c_{i,j}, & \text{otherwise,} \end{cases} \tag{4}$$

where α is a *scaling factor*, $\mathcal{N}_{i,j}$ is the four-neighborhood of the pixel (i, j), as illustrated in Fig. 5, and $\delta(z)$ is an indicator function defined as

$$\delta(z) = \begin{cases} 1, & z = 0, \\ 0, & z \neq 0. \end{cases} \tag{5}$$

In this way, when more neighborhood pixels are changed in the positive/negative direction, the current pixel will have a lower cost in the same direction. When the pixel is on the image boundary, we use the available pixels in the four-neighborhood. To deal with the saturated pixels, we set $\rho^+_{i,j} = w$ if $x_{i,j} = 255$, and $\rho^-_{i,j} = w$ if $x_{i,j} = 0$, where w is an extremely large number (e.g., 10^{10}) named wet cost [24]. We call this step *cost updating*. Take the image from Fig. 3 and the embedding order from Fig. 4 (a) as an example. Suppose the pixels in $\mathcal{S}_1$, $\mathcal{S}_2$, and $\mathcal{S}_3$ have already been embedded data, and it is $\mathcal{S}_4$'s turn. The difference image $\mathbf{D}$ and the initial cost $\mathbf{C}$ are obtained as illustrated in Fig. 6, and suppose we use $\alpha = 9$. It can be observed that there are more positive than negative changes in the four-neighborhood of $x_{2,1}$ and $x_{2,5}$, therefore, the corresponding costs $\rho^+_{2,1}$ and $\rho^+_{2,5}$ are set as $c_{2,1}/9$ and $c_{2,5}/9$, respectively. Similarly, since there are more negative than positive changes in the four-neighborhood of $x_{4,3}$ and $x_{6,5}$, the corresponding costs $\rho^-_{4,3}$ and $\rho^-_{6,5}$ are set as $c_{4,3}/9$ and $c_{6,5}/9$, respectively. In this way, the cost matrices $\boldsymbol{\rho}^+$ and $\boldsymbol{\rho}^-$ are updated towards clustering the same modification directions.
8) Embed a segment of data to obtain $y_{i,j}$ with $\rho_{i,j} = (\rho^+_{i,j}, \rho^0_{i,j}, \rho^-_{i,j})$, where $(i, j) \in \mathcal{S}_t$. The optimal embedding simulator [24], or practical steganographic codes for minimizing the additive distortion, such as the STC (syndrome-trellis code) [27], can be applied for data embedding.

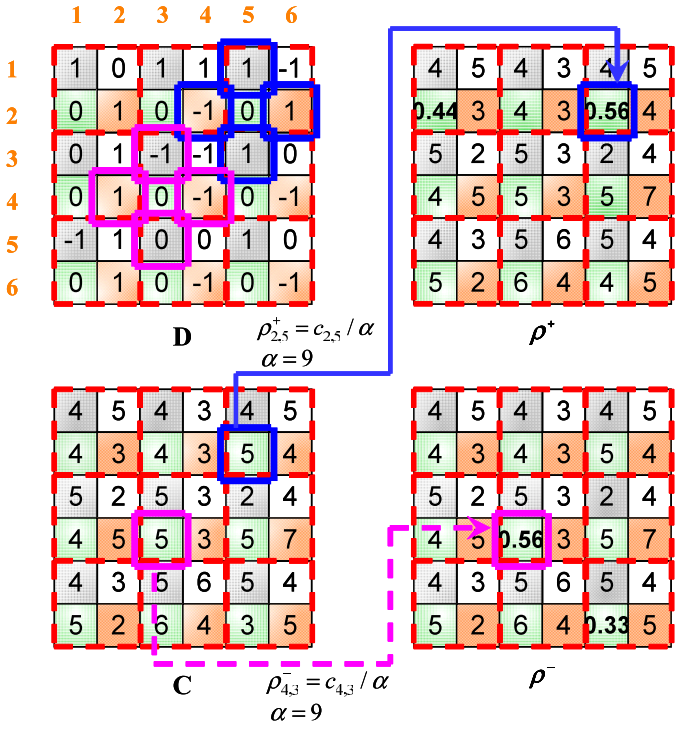


Fig. 6. An example of the process of updating costs in ρ^+ and ρ^- according to the difference image **D** and the initial cost matrix **C**.

9) Increase t by one. If $t < L_1 \cdot L_2$, go back to Step 5. Otherwise, terminate the process and output **Y** as the stego image.

Since the core idea of the proposed algorithm is to implement the CMD strategy, we call our algorithm the CMD algorithm. When applying the existing additive scheme, *i.e.*, WOW, S-UNIWARD, and HILL, for initial costs, we abbreviate the entire steganographic scheme as WOW-CMD, S-UNIWARD-CMD, and HILL-CMD, respectively.

C. Visualizing Embedding Changes

To verify whether the proposed algorithm can effectively cluster modification directions, we give an example to visualize the embedding changes. A sample cover image of size 128 × 128 pixels, containing smooth regions, edges, and textured regions, as shown in Fig. 7(a), is cropped from the full-size image "1013.pgm", which is from the BOSSBase ver 1.01 image database [29], as shown in Fig. 7(b). We embed data with an embedding rate of 0.4 bits per pixel by using HILL, S-UNIWARD, and their corresponding CMD-based counterparts. The parameter α for the CMD algorithm is set to 9, and the horizontal zig-zag embedding order is used. We show the difference images between the cover and the stego in Fig. 7(c) to 7(f), and highlight some selected parts with rectangles.

All embedding schemes make more changes in the textured regions than in the smooth regions. The number of changes is higher in Fig. 7(d) and 7(e) than in 7(c). Similarly, the number of changes is higher in Fig. 7(g) and 7(h) than in 7(f). It indicates that the CMD algorithm maintains the content-adaptivity, but leads to an increasing change rate. In the highlighted parts of Fig. 7(c) and 7(f), there are some scattered embedding changes, which means the neighbors of the changed pixels are not modified, or their modifications are heading towards different directions. The number of scattered embedding changes are fundamentally reduced in the corresponding highlighted parts in Fig. 7(d), 7(e), 7(g), and 7(h). The modifications are usually consecutive and locally heading towards the same direction in the CMD-based schemes, indicating the proposed algorithm is effective.

D. Discussions

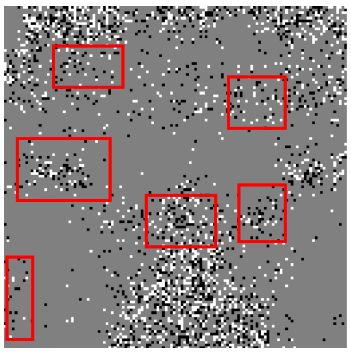
The costs of the elements in sub-images $\mathcal{S}_t$ ($t \in \{2, 3, \cdots, L_1 \cdot L_2\}$) have been dynamically adjusted due to two factors. The first factor is that as shown in (2), the initial costs are computed by using the stego image in which the sub-images $\mathcal{S}_k$ ($k \in \{1, \cdots, t-1\}$) have been modified. The second factor is that the costs of sub-images $\mathcal{S}_t$ ($t \in \{2, 3, \cdots, L_1 \cdot L_2\}$) are updated according to (3) and (4), which are affected by the modification directions of the elements in the previously embedded sub-images $\mathcal{S}_k$ ($k \in \{1, \cdots, t-1\}$). As a consequence, the embedding impacts have been considered in the algorithm and both the locations and the directions of the embedding modifications will be clustered.

With the dynamic cost updating process, it may not be easy for an adversary to estimate the accurate costs from the stego image, which may be exploited by adaptive steganalysis [10], [11]. It may also be difficult for an adversary to recover the embedding changes without a cover image, since no reversible clue can be found in the stego image.

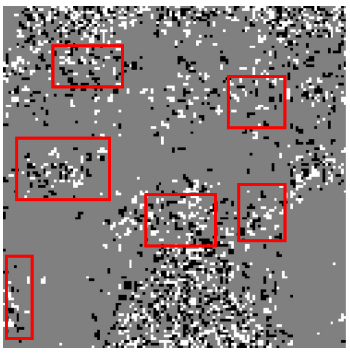
In our proposed algorithm, there are some parameters that can be adjusted. Firstly, the number of sub-images is determined by the parameters L_1 and L_2. In practice, we often use $L_1 = L_2 = L$, where L is called the *dimension parameter*. When $L = 1$, the CMD strategy is disabled. The complexity of the proposed algorithm will exponentially grow with L, since the cost updating process will run for $L^2 - 1$ times. As shown in Section IV-C, the dimension parameters ($L > 1$) have a slight impact on the strength of clustering modification directions and the change rate. Secondly, the embedding order of the sub-images may have an impact on the modification clustering, and thus on the steganographic security. A rule of thumb is that the embedding order should be horizontally or vertically connected. In this way, we can better exploit the embedding impacts in the four-neighborhood during the cost updating process. We may have the scanning order of row-by-row, zig-zag, Hilbert scan [34], etc. To resist possible targeted attacks on the embedding order, we can randomize the order for different images. For example, when $L = 2$, we can randomly select one of the eight zig-zag orders in Fig. 8 for each image. Thirdly, the scaling factor α will control the tradeoff between the change rate and the strength of clustering modification direction. For $\alpha > 1$, $\rho^+_{i,j}$ and $\rho^-_{i,j}$ differ by a factor of α. The probabilities of positively and negatively changing pixel values are different. Compared to the case when $\rho^+_{i,j} = \rho^-_{i,j}$, where the probabilities are the same, the entropy for the uncertainty in the first case is lower than that in the second case. Consequently the change rate of the first case

(a) Cover image

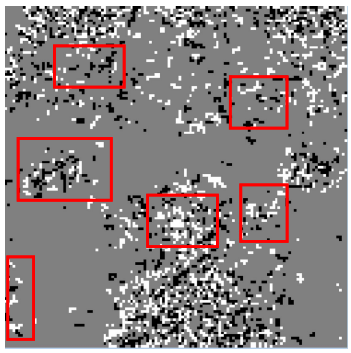
(b) Full-size image "1013.pgm" from BOSSBase ver 1.01 image database



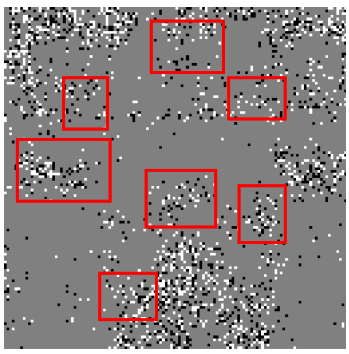
(c) HILL



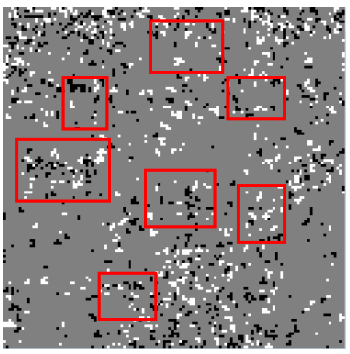
(d) HILL-CMD ($L_1 = L_2 = 2$)



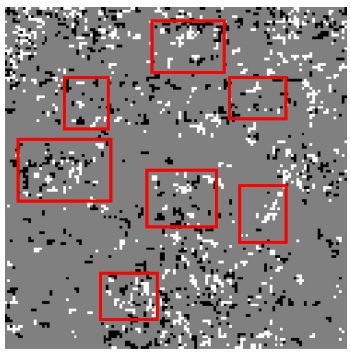
(e) HILL-CMD ($L_1 = L_2 = 4$)



(f) S-UNIWARD



(g) S-UNIWARD-CMD ($L_1 = L_2 = 2$)



(h) S-UNIWARD-CMD ($L_1 = L_2 = 4$)

Fig. 7. Embedding changes for a sample cover image (a), cropped from a full-size image (b). (c) to (h) are the difference images between the cover and the stego; white pixels represent positive changes; dark pixels represent negative changes. Note that in the highlighted regions of figures, HILL-CMD and S-UNIWARD-CMD result in more clustered changes as well as concentrated modification directions. Due to possibly low printing resolution, readers are encouraged to zoom in the figures on a computer screen for better clarity.

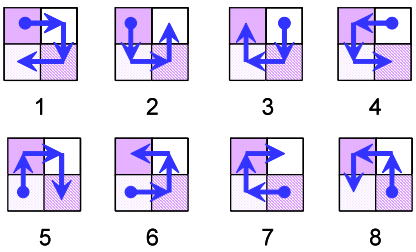
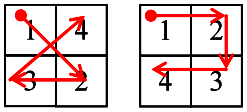


Fig. 8. Different zig-zag embedding orders for sub-images with $L = 2$.

will be higher. When we set $\alpha = 1$, the costs are directly assigned according to the initial costs, and the CMD strategy is disabled. It is similar to the Gibbs construction [13] with only one sweep. As a result, both the change rate and the effect of clustering modification directions are controlled by the scaling factor α. The best α to resist steganalysis can be determined experimentally as shown in Section IV-C.

Both the proposed CMD algorithm and the Gibbs construction [13] share some common procedures. For example, they both require to divide the image into sub-images (or sub-lattices), and update the costs (or local potentials) according to previous sub-images. However, there are also several important differences. Firstly, the embedding sweeps are repeated several times in the Gibbs construction to make the embedding pattern converge. In the proposed algorithm, each sub-image only needs to be processed once. This difference makes the proposed algorithm run faster. Secondly, the division into sub-lattices in the Gibbs construction aims to guarantee the independence of embedding changes between sub-lattices. It might be better to use a large



(a) (b)

Fig. 9. Two example of embedding orders for sub-images with $L = 2$. (a) Crossing. (b) Horizontal zig-zag.

number of sub-lattices. The division into sub-images in the proposed algorithm aims to cluster modification directions. The number of sub-images may be as small as four when we use $L = 2$. Thirdly, the proposed algorithm does not start with a non-additive distortion function so that the optimality of the proposed approach cannot be proved as in the Gibbs construction. Instead, non-additive distortion is implicitly introduced by the adjustment of costs during the cost updating process, where clustered modification directions are considered as having lower distortion.

IV. Experimental Evaluation

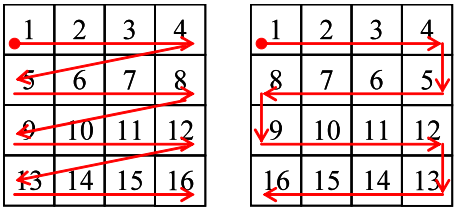
We evaluate the performance of the proposed algorithm with various configurations, including using different embedding orders, dimension parameters, scaling factors, and image data sets. We also assess the impact of using various initial cost assignment schemes and using non-uniform payload allocation rates in sub-images.

A. General Setup

All experiments except the one described in Section IV-I are conducted on BOSSBase ver 1.01 image database [29]. This set contains 10,000 gray-scale images of size 512×512 pixels, and is widely used as the standard evaluation set by the research community of steganography and steganalysis. We use the optimal embedding simulator [24] by default, and the STC (syndrome-trellis code) [27] in Section IV-F. Unless stated otherwise, the performance is evaluated by the steganalyzer using the 34,671-dimensional SRM feature set [7] with the ensemble classifiers [31], where Fisher linear discriminants are used as base learners. In Section IV-C and IV-G, we also use two kinds of adaptive steganalyzers, the tSRM [10] and the maxSRMd2 [11], for evaluation. A number of 5,000 randomly selected cover images and their stego counterparts are used for training, and the remaining 5,000 image pairs are used for testing. The testing classification error is computed as the mean value of the false positive rate and the false negative rate, averaged over 10 random splits of the data set. Except for Section IV-E, the embedding payload rate is 0.4 bpp (bit per pixel).

B. Impact of the Embedding Order

With the HILL-CMD scheme, we try three kinds of embedding orders, *i.e.,* crossing, horizontal zig-zag, and randomized zig-zag, for $L = 2$, as illustrated in Fig. 8 and 9, and two kinds of embedding orders, *i.e.,* row-by-row and horizontal zig-zag, for $L = 4$, as illustrated in Fig. 10. For the randomized zig-zag



(a) (b)

Fig. 10. Two example of embedding orders for sub-images with $L = 4$. (a) Row-by-row. (b) Horizontal zig-zag.

embedding order, we randomly select one of the eight embedding orders in Fig. 8 for each image. The original scheme HILL is included for comparison. The classification errors and the change rates are reported in Table II. It can be observed that a low change rate cannot ensure a high classification error. The zig-zag order is more effective than its counterparts (crossing or row-by-row). In order to explain why, we define an evaluation metric, called FCC (frequency of consecutive changes), to compute the average frequency of occurrences in the row/column direction for consecutive positive/negative changes. The n-th order FCC, denoted by $F(n)$, is obtained by

$$F(n) = \frac{1}{4}\big(H(n,1) + H(n,-1) + V(n,1) + V(n,-1)\big), \quad (6)$$

where

$$H(n,k) = \frac{\sum_{i=1}^{n_1}\sum_{j=1}^{n_2-n+1}\big(\delta(d_{i,j}-k)\cdots\delta(d_{i,j+n}-k)\big)}{n_1(n_2-n+1)}, \quad (7)$$

$$V(n,k) = \frac{\sum_{i=1}^{n_1-n+1}\sum_{j=1}^{n_2}\big(\delta(d_{i,j}-k)\cdots\delta(d_{i+n,j}-k)\big)}{(n_1-n+1)n_2}, \quad (8)$$

and $\delta(z)$ is defined in (5). The higher the strength of clustering modification directions, the higher the FCC. We measure the second to the fourth order FCC for each image. In Table II, we report the average FCC over the whole stego image set. It can be observed that the horizontal zig-zag order has a higher value of average FCC than its counterparts. In the following experiments we use the horizontal zig-zag order by default. It should be noted that a high FCC does not necessarily lead to high steganographic security. Other factors, including the change rate and the dimension parameter, may also affect the performance, as shown in the following subsections.

C. Impact of the Dimension Parameter and the Scaling Factor

The number of the sub-images is determined by the dimension parameter L. We considered $L = 2$, 4, and 8. For each L, we also vary the scaling factor α, and the resulting steganalytic performance is shown in Fig. 11 for HILL-CMD. It can be observed that the best scaling factor does not change significantly for different L. The best performance is achieved when $L = 2$ with $\alpha = 9$.

In Fig. 12 we show the relation between the change rate and the scaling factor. It is clear that no matter what L is, the change rate increases along with α. For the same α,

TABLE II
THE PERFORMANCE WITH DIFFERENT EMBEDDING ORDERS FOR SUB-IMAGES

Scheme	Embedding Order	Dimension	Classification Error	Change Rate	FCC (2nd Order)	FCC (3rd Order)	FCC(4-th Order)
HILL	N/A	N/A	0.2498	0.0853	0.00522	0.00102	0.00024
HILL-CMD	crossing	$L = 2$	0.2768	0.1044	0.01445	0.00397	0.00095
HILL-CMD	randomized zig-zag	$L = 2$	0.2949	0.1087	0.01713	0.00499	0.00127
HILL-CMD	horizontal zig-zag	$L = 2$	0.3002	0.1095	0.01758	0.00517	0.00135
HILL-CMD	row-by-row	$L = 4$	0.2958	0.1124	0.01923	0.00721	0.00249
HILL-CMD	horizontal zig-zag	$L = 4$	0.2985	0.1130	0.01955	0.00736	0.00254

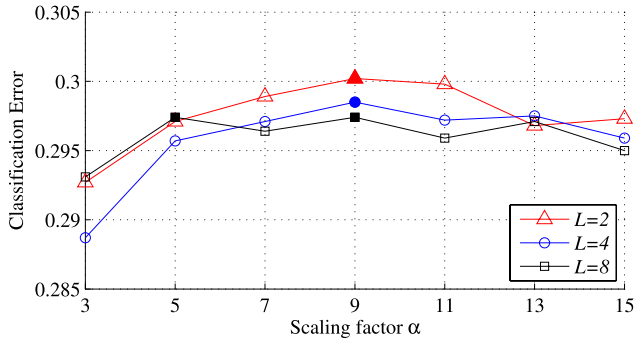


Fig. 11. Steganalytic performance (SRM) for HILL-CMD with different dimension parameters and scaling factors.

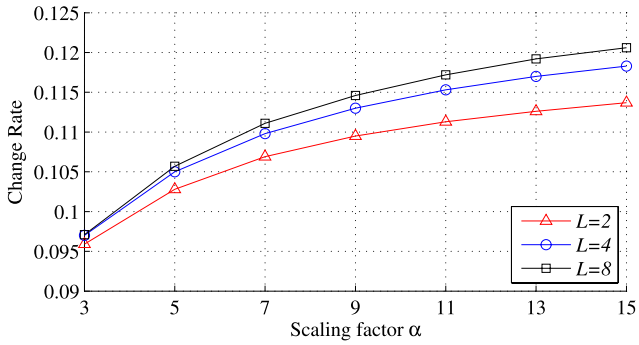


Fig. 12. Change rate for HILL-CMD with different dimension parameters and scaling factors.

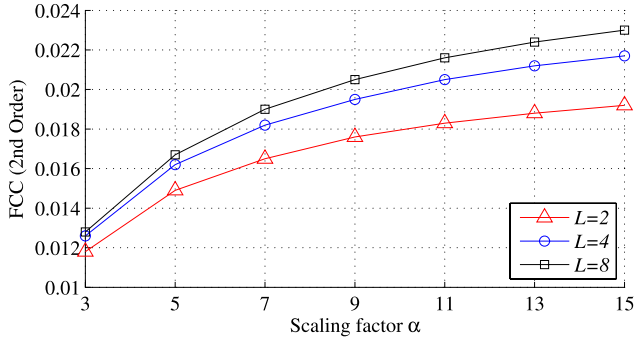


Fig. 13. FCC (2nd order) for HILL-CMD with different dimension parameters and scaling factors.

a smaller L leads to a lower change rate. In Fig. 13, we show the relation between the second order FCC and the scaling factor. It is easy to understand that the larger the scaling factor, the higher the FCC. For the same α, a larger L leads to a higher FCC.

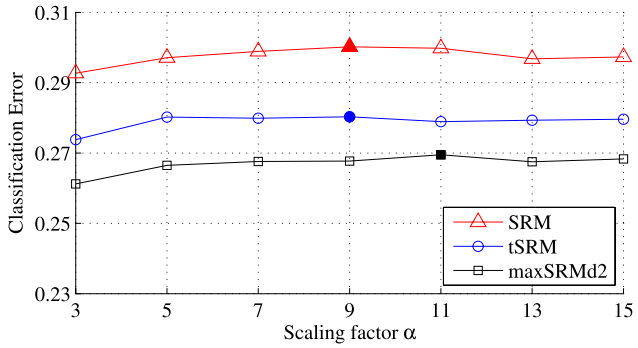


Fig. 14. Steganalytic performance (SRM, tSRM, and maxSRMd2) for HILL-CMD ($L = 2$) with different scaling factors.

Combining the results from Fig. 11 to Fig. 13, we may conclude that the steganographic security is not only related to the change rate, but also has a close relation to how the image is modified, e.g., whether the modification directions are clustered. The tradeoff between the change rate and the strength of clustering modification directions can be adjusted by tuning the scaling factor α in the proposed algorithm.

As discussed in Section III-D, the computational complexity of the proposed algorithm increases with L. We compare the execution time of the steganographic schemes with and without the CMD strategy in Table IV. The results are obtained by averaging the time needed to generate 100 stego images with a Matlab implementation on a computer with Intel i7-3770 CPU and 32GB RAM. It can be observed that the implementation by adopting the CMD strategy with a small dimension parameter does not take much time. We may use $L = 2$ for computational simplicity, and a larger L for ensuring enough randomization to resist possible variants of the selection-channel based attacks [10], [11].

When $L = 2$ is used, we vary α and test the performance with respect to three different steganalyzers including SRM, tSRM, and maxSRMd2. We use the initial cost of HILL to estimate the cost of HILL-CMD in the selection-channel-aware steganalytic schemes. The parameter p is set as 0.35 in tSRM and the embedding rate is assumed to be known in maxSRMd2. It can be observed from the results in Fig. 14 that the best α is distributed from 7 to 11. As a result, we use a combination of parameters with $L = 2$ and $\alpha = 9$ in the following experiments as default.

D. Impact of the Initial Cost Assignment Scheme

To verify whether the proposed algorithm can be generalizable to other additive schemes, we test

TABLE III
THE PERFORMANCE OF S-UNIWARD-CMD AND WOW-CMD WITH DIFFERENT PARAMETERS

Scheme	L	α	Classification Error	Change Rate
S-UNIWARD-CMD	2	1	0.2058	0.0743
S-UNIWARD-CMD	2	9	0.2538	0.1012
S-UNIWARD-CMD	8	1	0.2077	0.0734
S-UNIWARD-CMD	8	9	0.259	0.1067
WOW-CMD	2	1	0.2077	0.0897
WOW-CMD	2	9	0.2548	0.1124
WOW-CMD	8	1	0.2078	0.0891
WOW-CMD	8	9	0.2553	0.1173

TABLE IV
THE AVERAGE EXECUTION TIME FOR AN IMAGE WITH SIZE 512 × 512 PIXELS BY USING A COMPUTER WITH INTEL i7-3770 AND 32GB RAM

Scheme	L	Time (Second)
HILL	N/A	0.5591
HILL-CMD	2	0.6070
HILL-CMD	4	0.7793
HILL-CMD	8	1.4220
S-UNIWARD	N/A	0.6820
S-UNIWARD-CMD	2	0.8141
S-UNIWARD-CMD	4	1.4367
S-UNIWARD-CMD	8	4.0950

S-UNIWARD-CMD and WOW-CMD. We use four different parameter combinations for S-UNIWARD-CMD and WOW-CMD, respectively. When obtaining the initial cost of S-UNIWARD, the parameter is set to $\sigma = 1$ according to [20]. The results for the payload rate of 0.4 bpp are reported in Table III, which shows that under the same L, the scheme with a cost updating process ($\alpha = 9$) leads to a higher change rate but a lower classification error than its counterpart without the updating process ($\alpha = 1$). It confirms that applying the proposed algorithm is beneficial to steganographic security. We observe that although both S-UNIWARD-CMD and WOW-CMD work well, they are inferior to HILL-CMD with $L = 2$ and $\alpha = 9$, which achieves a high classification error of 0.3002 as shown in Table II. The results clearly show the choice of the initial cost assignment schemes has a major impact on the performance of the CMD-based schemes.

E. Comparison to State-of-the-Art Methods

We compare the schemes HILL-CMD and S-UNIWARD-CMD with some currently popular methods, including HILL, S-UNIWARD, HUGO, and HUGO-BD (Gibbs construction). In HUGO, we use the parameter $T = 255$ with the model correction strategy [12]. It is the only binary embedding scheme that we used for comparison. In HUGO-BD, we use two Gibbs sweeps as recommended by [13] and employ the ternary embedding. Six different payload rates, ranging from 0.05 to 0.5 bpp, are used. The results are demonstrated in Fig. 15. We can observe that

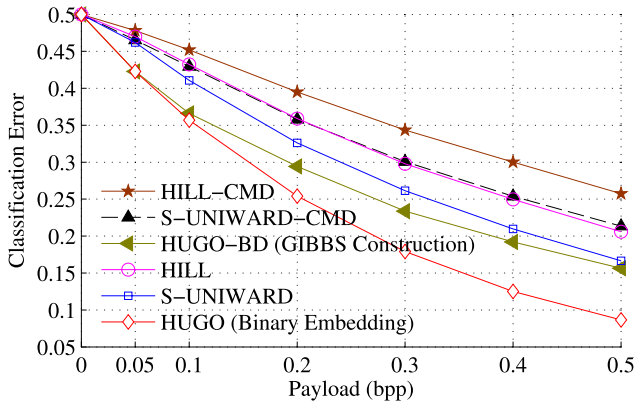


Fig. 15. Steganalytic performance (SRM) for different steganographic schemes with the optimal embedding simulator.

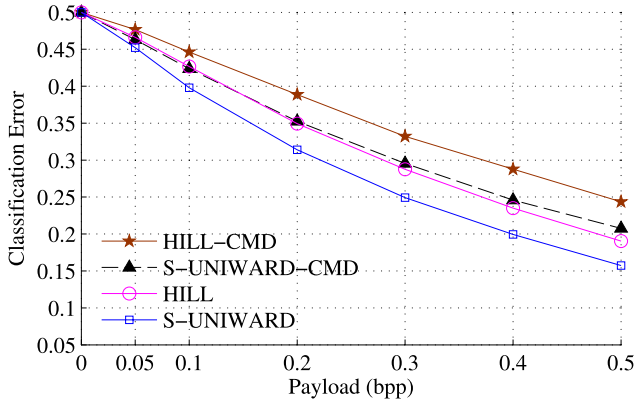


Fig. 16. Steganalytic performance (SRM) for different steganographic schemes with the STC.

the CMD-based schemes have a higher level of statistical undetectability.

F. Performance With the STC

We employ the STC [27] instead of the optimal embedding simulator for HILL, S-UNIWARD, HILL-CMD, and S-UNIWARD-CMD. The performance is reported in Fig. 16. Compared to the results in Fig. 15, the performance with a practical steganographic code is just slightly inferior to the optimal embedding simulator. The CMD-based schemes consistently perform better than their counterparts.

G. Performance for Adaptive Steganalysis

Two adaptive steganalytic schemes, tSRM [10] and maxSRMd2 [11], are effective in detecting the traces of spatial steganography. In these steganalyzers, the selection channel of the targeted steganography is estimated by estimating the costs from the stego image. We use the initial cost of HILL and that of S-UNIWARD to estimate the cost of HILL-CMD and that of S-UNIWARD-CMD, respectively. It might seem unfair to test the CMD-based schemes with inaccurate costs; but in fact it is a reasonable strategy given the uncertainty of the cost updating step which is unknown to an adversary. The parameter p is set as 0.35 in tSRM as recommended by its authors and the

TABLE V
THE PERFORMANCE FOR DIFFERENT PAYLOAD ALLOCATION RATES IN EACH SUB-IMAGE WHEN $L = 2$

Payload Allocated in $\mathcal{S}_1$-$\mathcal{S}_2$-$\mathcal{S}_3$-$\mathcal{S}_4$	Change Rate in $\mathcal{S}_1$	Change Rate in $\mathcal{S}_2$	Change Rate in $\mathcal{S}_3$	Change Rate in $\mathcal{S}_4$	Mean of the Change Rates	Variance of the Change Rates	Classification Error
25%-25%-25%-25%	0.0862	0.1097	0.1155	0.1266	0.1095	0.2904×10^{-3}	0.3002
28%-26%-24%-22%	0.0990	0.1169	0.1056	0.1232	0.1112	0.1189×10^{-3}	0.2989
28%-24%-26%-22%	0.0990	0.1091	0.1038	0.1308	0.1107	0.1970×10^{-3}	0.2968
29%-26%-24%-21%	0.1034	0.1180	0.1020	0.1234	0.1117	0.1132×10^{-3}	0.2974

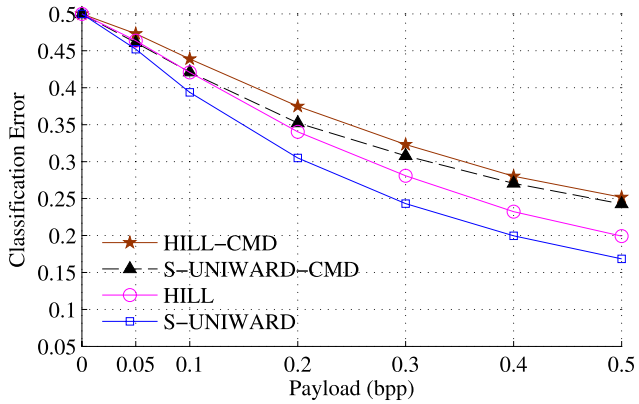


Fig. 17. Steganalytic performance (tSRM) for different steganographic schemes with the optimal embedding simulator.

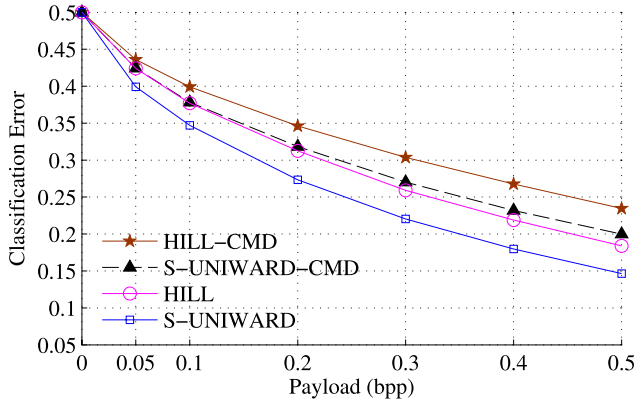


Fig. 18. Steganalytic performance (maxSRMd2) for different steganographic schemes with the optimal embedding simulator.

embedding rate is assumed to be known in maxSRMd2. The results are shown in Fig. 17 and Fig. 18. We can observe that for different payload rates, the non-additive schemes with the CMD strategy always have an advantage over their additive counterparts. We note that for high payload rates, tSRM performs worse than SRM for S-UNIWARD-CMD. We attribute this phenomenon to the mismatch of the selection-channel by using the constant parameter p in tSRM.

H. Performance With Non-Uniform Payload Allocation

In the default setting of the proposed algorithm, each sub-image carries equal amount of payload. Since the costs are updated sequentially for $\mathcal{S}_2, \cdots, \mathcal{S}_{L^2}$, the distribution of costs as well as the change rate is different for each sub-image. Take $L = 2$ for example. There are four sub-images, $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$, and $\mathcal{S}_4$, each carrying 25% of the total payload. The respective change rate in each sub-image (averaged from the 10,000 images in the BOSSBase set) is shown in Table V. It can be observed that the change rate monotonously increases for successive sub-images. It should be noted that although the last sub-image $\mathcal{S}_4$ may have the largest change rate, it is still difficult for an adversary to find the traces of embedding from the difference in the change rate. The reason is two-fold. Firstly, due to the CMD strategy, the embedding changes are locally heading towards the same direction. It may be difficult to identify whether the pixels have been modified. Secondly, it may be difficult for an adversary to obtain an accurate estimation of the cover and thus an accurate estimation of the change rate.

Just in case of an attack on the monotonously increasing change rates in sub-images, we can assign unequal amount of payload to sub-images. To this end, the first few sub-images may need to carry more payload than the last few sub-images in order to make the change rate more balanced. Note that for the purpose of achieving equal change rates in sub-images, the allocated payload should vary for each image and the receiver may need such side-information for message extraction. Instead, we can use constant non-uniform payload allocation. We have tried three kinds of constant non-uniform payload allocation schemes for $L = 2$ and the results are reported in Table V. It can be observed that compared to the case of uniform payload allocation, the variations in the change rate in the sub-images have been reduced; however, the overall change rate for the whole image has increased. A slight performance drop in steganalytic classification error can also be observed. As long as there is no successful attack for change rate estimation, we expect it is safe to allocate payload uniformly.

I. Performance on Another Image Set

In order to investigate whether the performance of the CMD-based scheme is over-optimized to the standard BOSSBase image database, we conduct additional experiments on another never-compressed image set. A total number of 8,000 images are in this set, originating from various sources, as described in Table VI. We believe the large variety of image sources will help to evaluate the performance more reasonably. The full-resolution color images in the set were firstly converted to gray-scale images, and then resized with bicubic interpolation so that the smaller side is 768 pixels, and finally cropped to 768×768 pixels. We call such a set as MRNC (Mixed Resized Never-Compressed) database.

We respectively use HILL-CMD and CMD with the optimal simulator for embedding, and use SRM and maxSRMd2

TABLE VI
THE COMPOSITION OF THE MRNC IMAGE SET

Image Source	Number of Images	Description
Dresden	1491	Described in [35] with Lightroom 2.5 for preprocessing the images in RAW format
McGill	1189	Described in [36]
NRCS	1543	Downloaded from [37]
SYSU	2232	Captured by a Panasonic DMC-FZ30 camera and a Nikon D300 camera
DLUT	522	Captured by a Kodak DC290 camera
CASIA	321	Captured by a Canon EOS 600D camera and a Nikon D7000 camera
SZU	702	Captured by a Canon EOS 60D camera

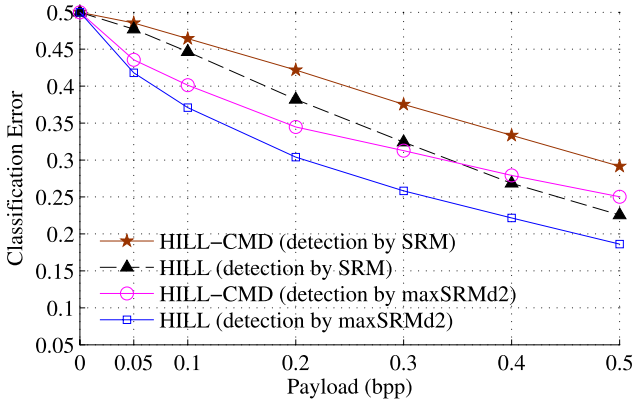


Fig. 19. Steganalytic performance (SRM and maxSRMd2) on the MRNC image set for different steganographic schemes with the optimal embedding simulator.

for detection. A number of 5,000 randomly selected cover images and their stego counterparts are used for training, while the remaining 3,000 image pairs are used for testing. The classification error is averaged 10 times by randomly splitting the training and the testing sets. The results are shown in Fig. 19. It can be observed that HILL-CMD performs better than HILL on the new image set, indicating the proposed algorithm is not over-optimized to the BOSSBase image set.

V. CONCLUSION

In this paper, we present a strategy called CMD (clustering modification directions), which shows that the steganographic security may be improved when the modification directions are more consecutive under the same change rate. The strategy is implemented in an algorithm where a cover image is decomposed into several sub-images, and additive distortion is minimized in each of the sub-images individually. Since the costs of pixels within each sub-image are dynamically adjusted, the overall distortion is non-additive. The costs are updated according to the modification directions of the sub-images that are already embedded data, and thus the probabilities of following the same modification directions are higher.

The proposed steganographic algorithm has three benefits. First, it exploits mutual embedding impacts to resist steganalysis. Second, it can utilize practical near-optimal steganographic codes, such as the STC. Third, it can be used together with the state-of-the-art schemes with additive distortion functions, such as HILL, S-UNIWARD, WOW. Moreover, since the costs are dynamically updated, it will be more challenging for an adversary to estimate the selection-channel accurately.

Extensive experiments show that the proposed steganographic algorithm with the CMD strategy works quite well. It can help improve the recently proposed additive schemes and it is very effective in resisting steganalyzers equipped with high-dimensional features and ensemble classifiers. The embedding changes introduced by the CMD algorithm is more like low-frequency noise, which makes it difficult for current steganalytic features to reveal embedding traces. Future steganalysis is expected to consider more reliable statistics for possible detection.

ACKNOWLEDGMENT

The authors appreciate the anonymous reviewers and Dr. Vojtech Holub for providing valuable comments, and thank the members of DDE Laboratory in SUNY Binghamton for sharing their implementation codes on the webpage (http://dde.binghamton.edu/download/). They also appreciate Dr. Weiqi Luo for providing SYSU image database, Dr. Bo Wang and Dr. Yanqing Guo for providing DLUT image database, Dr. Wei Wang for providing CASIA image database, and Dr. Xin Liao for providing the information of McGill image database. Special thanks go to Dr. Pawel Korus for his help in proofreading.

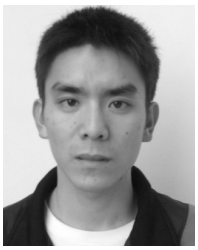
REFERENCES

[1] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2009.
[2] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis," *J. Inf. Hiding Multimedia Signal Process.*, vol. 2, no. 2, pp. 142–172, Apr. 2011.
[3] A. D. Ker *et al.*, "Moving steganography and steganalysis from the laboratory into the real world," in *Proc. 1st ACM Workshop Inf. Hiding Multimedia Secur.*, Montpellier, France, Jun. 2013, pp. 45–58.
[4] R. Böhme, *Advanced Statistical Steganalysis*. Berlin, Germany: Springer-Verlag, 2010.
[5] 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.
[6] G. Gul and F. Kurugollu, "A new methodology in steganalysis: Breaking highly undetectable steganograpy (HUGO)," in *Proc. 13th Int. Conf. Inf. Hiding*, vol. 6958. Prague, Czech Republic, May 2011, pp. 71–84.
[7] 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.
[8] Y. Shi, P. Sutthiwan, and L. Chen, "Textural features for steganalysis," in *Proc. 14th Int. Conf. Inf. Hiding*, vol. 7692. Berkeley, CA, USA, May 2012, pp. 63–77.
[9] L. Chen, Y. Q. Shi, P. Sutthiwan, and X. Niu, "Non-uniform quantization in breaking HUGO," in *Proc. 12th Int. Workshop Digit.-Forensics Watermarking*, Auckland, New Zealand, Jul. 2014, pp. 48–62.
[10] W. Tang, H. Li, W. Luo, and J. Huang, "Adaptive steganalysis against WOW embedding algorithm," in *Proc. 2nd ACM Workshop Inf. Hiding Multimedia Secur.*, Salzburg, Austria, Jun. 2014, pp. 91–96.
[11] 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 Secur.*, Atlanta, GA, USA, Dec. 2014, pp. 48–53.
[12] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Proc. 12th Int. Workshop Inf. Hiding*, vol. 6387. Calgary, AB, Canada, Jun. 2010, pp. 161–177.
[13] T. Filler and J. Fridrich, "Gibbs construction in steganography," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 705–720, Dec. 2010.

[14] F. Pan, J. Li, X. Li, and Y. Guo, "Steganography based on minimizing embedding impact function and HVS," in *Proc. IEEE Int. Conf. Electron., Commun., Control*, Zhejiang, China, Sep. 2011, pp. 490–493.
[15] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proc. IEEE Int. Workshop Inf. Forensic Secur.*, Tenerife, Spain, Dec. 2012, pp. 234–239.
[16] G. Liu, W. Liu, Y. Dai, and S. Lian, "Adaptive steganography based on syndrome-trellis codes and local complexity," in *Proc. 4th IEEE Int. Conf. Multimedia Inf. Netw. Secur.*, Nanjing, China, Nov. 2012, pp. 323–327.
[17] J. Fridrich and J. Kodovský, "Multivariate Gaussian model for designing additive distortion for steganography," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Vancouver, BC, Canada, May 2013, pp. 2949–2953.
[18] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," in *Proc. 1st ACM Workshop Inf. Hiding Multimedia Secur.*, Montpellier, France, Jun. 2013, pp. 59–68.
[19] T. Denemark, J. Fridrich, and V. Holub, "Further study on the security of S-UNIWARD," *Proc. SPIE, Electron. Imag., Media Watermarking, Secur., Forensics*, vol. 9028, pp. 902805-1–902805-13, Feb. 2014.
[20] V. Holub, J. Fridrich, and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP J. Inf. Secur.*, vol. 2014, pp. 1–13, Jan. 2014.
[21] B. Li, M. Wang, J. Huang, and X. Li, "A new cost function for spatial image steganography," in *Proc. IEEE Int. Conf. Image Process.*, Paris, France, Oct. 2014, pp. 4206–4210.
[22] 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.
[23] J. Fridrich, "Minimizing the embedding impact in steganography," in *Proc. 8th ACM Workshop Multimedia Secur.*, Geneva, Switzerland, Sep. 2006, pp. 2–10.
[24] J. Fridrich and T. Filler, "Practical methods for minimizing embedding impact in steganography," *Proc. SPIE, Electron. Imag., Secur., Steganogr., Watermarking Multimedia Contents IX*, vol. 6505, pp. 650502-1–650502-15, Jan. 2007.
[25] W. Zhang, S. Wang, and X. Zhang, "Improving embedding efficiency of covering codes for applications in steganography," *IEEE Commun. Lett.*, vol. 11, no. 8, pp. 680–682, Aug. 2007.
[26] W. Zhang, X. Zhang, and S. Wang, "Near-optimal codes for information embedding in gray-scale signals," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1262–1270, Mar. 2010.
[27] 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.
[28] V. Holub, "Content adaptive steganography—Design and detection," Ph.D. dissertation, Dept. Elect. Comput. Eng., Binghamton Univ., Binghamton, NY, USA, 2014.
[29] P. Bas, T. Filler, and T. Pevný, "'Break our steganographic system': The ins and outs of organizing BOSS," in *Proc. 13th Int. Workshop Inf. Hiding*, vol. 6958. Prague, Czech Republic, May 2011, pp. 59–70.
[30] T. Pevný and J. Fridrich, "Benchmarking for steganography," in *Proc. 10th Int. Workshop Inf. Hiding*, vol. 5284. Santa Barbara, CA, USA, May 2008, pp. 251–267.
[31] J. Kodovský, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 432–444, Apr. 2012.
[32] R. Böhme, "Improved statistical steganalysis using models of heterogeneous cover signals," Ph.D. dissertation, Faculty Comput. Sci., Technische Univ. Dresden, Germany, 2008.
[33] V. Holub and J. Fridrich, "Optimizing pixel predictors for steganalysis," *Proc. SPIE, Media Watermarking, Secur., Forensics*, vol. 8303, pp. 830309-1–830309-13, Jan. 2012.
[34] J. Zhang, S.-I. Kamata, and Y. Ueshige, "A pseudo-Hilbert scan algorithm for arbitrarily-sized rectangle region," in *Proc. Int. Workshop Intell. Comput. Pattern Anal./Synthesis*, vol. 4153. Xi'an, China, Aug. 2006, pp. 290–299.
[35] T. Gloe and R. Böhme, "The 'Dresden image database' for benchmarking digital image forensics," in *Proc. ACM 25th Symp. Appl. Comput.*, vol. 2. 2010, pp. 1584–1590.
[36] A. Olmos and F. A. A. Kingdom, "A biologically inspired algorithm for the recovery of shading and reflectance images," *Perception*, vol. 33, no. 12, pp. 1463–1473, 2004.
[37] *NRCS Photo Gallery*. [Online]. Available: http://photogallery.nrcs.usda.gov/res/sites/PhotoGallery/index.html, accessed Aug. 14, 2014

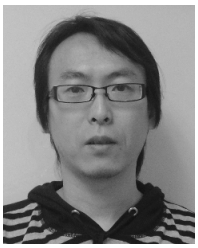
Bin Li (S'07–M'09) received the B.E. degree in communication engineering and the Ph.D. degree in communication and information system from Sun Yat-sen University, Guangzhou, China, in 2004 and 2009, respectively.

He was a Visiting Scholar with the New Jersey Institute of Technology, Newark, NJ, USA, from 2007 to 2008. He is currently an Associate Professor with Shenzhen University, Shenzhen, China, where he joined in 2009. He is also a member of the Shenzhen Key Laboratory of Media Security. His current research interests include image processing, multimedia forensics, and pattern recognition.



Ming Wang received the B.S. degree from the Hunan Institute of Science and Technology, Yueyang, China.

He is currently pursuing the M.S. degree with Shenzhen University, Shenzhen, China. His current research interest is information hiding.



Xiaolong Li received the B.S. degree from Peking University, Beijing, China, in 1999, the M.S. degree from Ecole Polytechnique, Palaiseau, France, in 2002, and the Ph.D. degree in mathematics from the École Normale Supérieure de Cachan, Cachan, France, in 2006.

He is currently a Researcher with the Institute of Computer Science and Technology, Peking University, where he was a Post-Doctoral Fellow from 2007 to 2009. His research interests are image processing and information hiding.

Shunquan Tan (M'10) received the B.S. degree in computational mathematics and applied software and the Ph.D. degree in computer software and theory from Sun Yat-sen University, Guangzhou, China, in 2002 and 2007, respectively.

He is currently a Lecturer with the College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, China. He is also a member of the Shenzhen Key Laboratory of Media Security. His current research interests include steganography, steganalysis, multimedia forensics, and deep machine learning.

Jiwu Huang (M'98–SM'00) received the B.S. degree from Xidian University, Xi'an, China, in 1982, the M.S. degree from Tsinghua University, Beijing, China, in 1987, and the Ph.D. degree from the Institute of Automation, Chinese Academy of Sciences, Beijing, in 1998.

He was with the School of Information Science and Technology, Sun Yat-sen University, Guangzhou, China. He is currently a Professor with the College of Information Engineering, Shenzhen University, Shenzhen, China. His current research interests include multimedia forensics and security. He is also a member of the IEEE Circuits and Systems Society Multimedia Systems and Applications Technical Committee and the IEEE Signal Processing Society Information Forensics and Security Technical Committee. He served as an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and a General Co-Chair of the IEEE Workshop on Information Forensics and Security in 2013.