A New Payload Partition Strategy in Color Image Steganography

Xin Liao, *Member, IEEE*, Yingbo Yu, Bin Li, *Senior Member, IEEE*, Zhongpeng Li, and Zheng Qin, *Member, IEEE*

***Abstract*— In traditional steganographic schemes, RGB three channels payloads are assigned equally in a true color image. In fact, the security of color image steganography relates not only to data-embedding algorithms but also to different payload partition. How to exploit inter-channel correlations to allocate payload for performance enhancement is still an open issue in color image steganography. In this paper, a novel channel-dependent payload partition strategy based on amplifying channel modification probabilities is proposed, so as to adaptively assign the embedding capacity among RGB channels. The modification probabilities of three corresponding pixels in RGB channels are simultaneously increased, and thus the embedding impacts could be clustered, in order to improve the empirical steganographic security against the channel co-occurrences detection. The experimental results show that the new color image steganographic schemes, incorporated with the proposed strategy, can effectively make the embedding changes concentrated mainly in textured regions, and achieve better performance on resisting the modern color image steganalysis.**

***Index Terms*— Image steganography, RGB channels, payload partition, modification probabilities.**

I. Introduction

STEGANOGRAPHY attempts to hide secret messages into innocuous digital media without arousing suspicion [1]. Recently, the most effective image steganographic schemes are based on designing distortion function to minimize statistical detectability [2], [3]. The impact of modifying cover image can be measured by the distortion function which is a summation of the embedding costs in the cover image pixels [4]. Since the advanced syndrome-trellis codes (STC) [5] performs well in minimizing the additive distortion costs, researchers have been paying close attention to designing distortion functions in recent years.

The distortion function of HUGO (highly undetectable stego) [6] computes the weighted sum of differences between pixel adjacency matrix features extracted from the cover and stego images. In contrast to HUGO, WOW (wavelet obtained weights) [7] uses three directional wavelet filters for obtaining the embedding cost, which assigns high costs to more predictable pixels and low costs to less predictable pixels. The idea of S-UNIWARD (spatial universal wavelet relative distortion) [8] is extended from WOW, which has a slightly modified distortion function. HILL (high pass, low-pass and low-pass) [9] utilizes one high-pass filter and two low pass filters to avoid the problem that the small embedding suitability of one direction causes strong effects on distortion values. The embedding costs in [10] are the sum of all detectability costs obtained from Fisher linear discriminant classifiers. Inspired by the model-based steganography [11], MG (multivariate Gaussian) [12] is a model-driven framework to obtain the costs. The cover is modeled as a sequence of independent quantized Gaussian, and the modification probabilities and cost values are derived to minimize the steganographic Fisher information [13] for a given embedding operation and payload. This approach is subsequently extended by utilizing a better variance estimator and the multivariate generalized Gaussian model (MVGG) [14]. Later Sedighi *et al.* [15] derived a closed form expression for the detector of content-adaptive LSB matching within the selected model, and then designed steganography based on minimizing the power of the optimal detector (MiPOD). Since the neighboring embedding changes will interact, Denemark *et al.* [16] and Li *et al.* [17] independently investigated the non-additive distortion function. Synch (synchronize) strategy [16] starts with the additive cost assignment and then constructs a non-additive distortion function in which non-synchronized embedding changes made to adjacent pixels are penalized. CMD (clustering modification directions) strategy [17] tries to preserve the correlation between neighboring pixels and synchronize the modification directions. In 2017, Zhang et al. designed joint distortion functions on pixel blocks, which exploits the interactive impact of changes between adjacent pixels [18]. They have

Manuscript received May 2, 2018; revised October 20, 2018; accepted January 23, 2019. Date of publication January 31, 2019; date of current version March 5, 2020. This work was supported in part by the National Natural Science Foundation of China under Grant 61402162, Grant 61572329, Grant 61872244, and Grant 61772191, in part by the Hunan Provincial Natural Science Foundation under Grant 2017JJ3040, in part by the Science and Technology Key Projects of Hunan Province under Grant 2015TP1004 and Grant 2016JC2012, in part by the Open Project Program of National Laboratory of Pattern Recognition under Grant 201900017, and in part by CERNET Innovation Project under Grant NGII20180412. This paper was recommended by Associate Editor P. Comesana-Alfaro. *(Corresponding author: Xin Liao.)*

X. Liao is with the College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China, and also with the Shenzhen Key Laboratory of Media Security, Shenzhen University, Shenzhen 518060, China (e-mail: xinliao@hnu.edu.cn).

Y. Yu and Z. Qin are with the College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China (e-mail: yuyb@hnu.edu.cn; zqin@hnu.edu.cn).

B. Li is with the Guangdong Key Laboratory of Intelligent Information Processing and Shenzhen Key Laboratory of Media Security, Shenzhen University, Shenzhen 518060, China, and also with the Peng Cheng Laboratory, Shenzhen 518052, China (e-mail: libin@szu.edu.cn).

Z. Li is with the Guangdong Key Laboratory of Intelligent Information Processing and Shenzhen Key Laboratory of Media Security, Shenzhen University, Shenzhen 518060, China (e-mail: lizhongpeng@email.szu.edu.cn).

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

Digital Object Identifier 10.1109/TCSVT.2019.2896270

shown significant improvements evaluated by the powerful steganalysis [19]–[21].

Note that the above steganographic methods are only designed for gray-scale images. In fact, true color images are prevalent in practical applications. The fundamental difference between true color image and gray-scale image is that a pixel of the true color image can be considered as a vector consisting of three components (Red, Green, Blue), while a pixel of the gray-scale image is only regarded as a scalar gray-level. In most conventional steganography, it is implicitly assumed that gray-scale image steganographic schemes can be directly applied to true color images by independently embedding messages into color channels. There are high inter-channel dependencies among RGB channels in a true color image, and thus researchers have made some helpful progress on color image steganography by means of sparse decomposition on RGB color bands and hiding messages in the matching pursuit domain [22]–[24]. Two steganographic frameworks for color images were presented by utilizing the adaptive least significant bit replacement approach with multi-level cryptography mechanism and secret key-directed block-by-block mechanism, respectively [25], [26]. However, compared with the distortion-minimization framework, these works would lead to higher embedding distortions. In 2016, Tang et al. proposed a color image steganography strategy called CMDC [27], which first clusters modification directions for color components and preserves the color channel correlations. Since the authors utilized optimal simulator with the same seed to embed messages in the sub-images of RGB channels, it might result in higher level of clustering modification directions for color components. The effect of modification clustering among the color components is not effective if different seeds are used. Furthermore, CMDC still assumes that the covert payload is assigned equally for each color channel.

It is worth noting that for some special color images (e.g. abundant brightness only in one or two color components), color image steganography with average payload partition would lead to some embedding changes concentrated in smooth regions. Thus, the uniform distribution would not be an appropriate choice of RGB channel payload assignment. It is reasonable to distribute the payload unevenly to be hidden in each color channel, in order to improve the performance of statistical undetectability.

By extending gray-scale image content-adaptive steganography to color images, the probability of pixel modification varies depending on the cover color image content. The steganography embedding can be optimized in terms of minimizing total distortion using steganographic codes. This is also true for color images, achieved by simple color concatenation (SCC), i.e., an intuitive embedding method through the cost values directly computed from the concatenation of RGB three channels. Three RGB components are concatenated into a new digital image, and then a modern distortion function is utilized to calculate the cost values. Due to the nonlinear property of modern distortion functions, a steganographer can obtain the new costs profile, and thus acquire the stego color image. SCC could automatically distribute the payload across color channels and potentially embed more bits into the noisier channel.

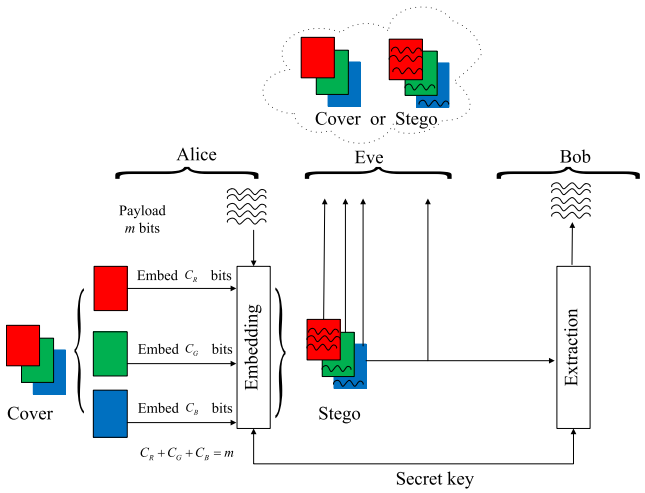


Fig. 1. Payload partition in color image steganography.

However, how to exploit inter-channel correlations to partition payload for different channels is still an open issue in color image steganography. We try our best to make one step forward in this paper. This work is motivated by the following scenario. Three entities are involved in adaptive color image steganography, as illustrated in Fig. 1. They are a steganographer (Alice) aiming to communicate with a passive conspirator (Bob) over an insecure channel, and an eavesdropper (Eve) monitoring and detecting the communication channel. Suppose Alice already has an innocent true color image. To conceal the covert payload well, she might split the payload into three parts and embed the parts into the individual channel of the color image. The major issue is how the payload should be spread among RGB channels, in order to evade Eve's detection.

From the perspective of steganalysis, the advanced color image steganalyzers always focus on the channel co-occurrences [28]–[31]. In order to improve the empirical steganographic security, we could exploit the embedding impacts of RGB channels. By intentionally adjusting the distortion costs of three corresponding pixels in each color channel, we amplify the channel modification probabilities. Specifically, for some pixels of RGB channels in heavily textured regions, the modification probabilities are simultaneously increased, and thus the embedding impacts would be clustered. Therefore, the anti-steganalysis performance might be enhanced.

In this paper, a new channel-dependent payload partition strategy based on amplifying channel modification probabilities (ACMP) is proposed. The proposed ACMP strategy could be incorporated into these state-of-the-art image steganographic methods. It is flexible and provides steganographers a general-purpose methodology to obtain new true color image steganographic schemes. Experimental results show that the new color image steganography schemes could not only efficiently make the embedding changes concentrated in textured regions, but also achieve better anti-steganalysis performance than average payload partition and simple color concatenation, against the state-of-the-art color image steganalysis.

The rest of this paper is organized as follows. After introducing some basic concepts, Section II formulates the target problem. The detailed descriptions of the proposed payload partition strategy and the corresponding discussions are presented in section III. The next section shows experimental comparisons and analysis, demonstrating the effectiveness of our proposed strategy. Finally, the conclusions are made in section V.

II. Problem Formulation

For a true color image $\mathbf{I}$, it can be represented as three n vectors $[\mathbf{R},\ \mathbf{G},\ \mathbf{B}]$, and by the scanning order of zigzag, $\mathbf{R} = (R_1, R_2, \cdots, R_n), \mathbf{G} = (G_1, G_2, \cdots, G_n), \mathbf{B} = (B_1, B_2 \cdots, B_n)$. $R_i,\ G_i,\ B_i \in \mathcal{I} \triangleq \{0, 1, \cdots, 255\}$ is the i-th element of each channel with the pixel dynamic range $\mathcal{I}$. The steganographer communicates messages to the receiver by modifying the cover color image $\mathbf{I}$ to the stego color image $\mathbf{I}' = [\mathbf{R}',\ \mathbf{G}',\ \mathbf{B}']$, where $\mathbf{R}' = (R'_1, R'_2, \cdots, R'_n) \in \mathcal{I}_1^R \times \mathcal{I}_2^R \cdots \times \mathcal{I}_n^R, \mathbf{G}' = (G'_1, G'_2, \cdots, G'_n) \in \mathcal{I}_1^G \times \mathcal{I}_2^G \cdots \times \mathcal{I}_n^G, \mathbf{B}' = (B'_1, B'_2 \cdots, B'_n) \in \mathcal{I}_1^B \times \mathcal{I}_2^B \cdots \times \mathcal{I}_n^B$.

As shown in Fig. 1, Alice would like to hide a fixed total amount of secret data m bits. She intends to determine, how much the payload C_R, C_G, C_B would be embedded into RGB channels respectively, subject to the payload constraint $C_R + C_G + C_B = m$ and some assumptions about maximum acceptable risks of detection.

However, the probability distribution of digital images is unknown, and the security would be compromised if overtraining and mismatching steganography to incomplete cover model [32]. In practice, the problem of designing secure steganographic schemes can be formulated as the minimal distortion embedding [2]. 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 RGB channel pixels $[\mathbf{R},\ \mathbf{G},\ \mathbf{B}]$, we can obtain the cost values $\boldsymbol{\rho}_R = (\rho_{R_1}, \rho_{R_2}, \cdots, \rho_{R_n}), \boldsymbol{\rho}_G = (\rho_{G_1}, \rho_{G_2}, \cdots, \rho_{G_n})$ and $\boldsymbol{\rho}_B = (\rho_{B_1}, \rho_{B_2}, \cdots, \rho_{B_n})$, respectively.

Color image steganography with different RGB channel payload partitions might result in distinct embedding distortions. The existences of color image steganalyzers [28]–[31] that can exploit inter-channel dependencies prove the detectability of a modification in just one colored pixel is not a sole function of the sum of distortions calculated in RGB channels. Therefore, incorporating inter-channel correlations into color image steganography would improve the empirical anti-steganalysis performance. We ought to explore the inter-channel dependencies to find adaptive payload partition in color image steganography.

III. The New Payload Partition Strategy

In this section, a new strategy for channel-dependent payload partition, named amplifying channel modification probabilities (ACMP), is investigated. The advantage of the novel strategy is to exploit three channel correlations to assign covert payload, and to be implemented together with these state-of-art image steganographic methods. The effectiveness of the proposed strategy is analyzed and discussed.

A. The Proposed ACMP Strategy

Assume the embedding operations will modify the i-th pixel R_i, G_i, B_i in RGB channels with the embedding probabilities $p_{R_i},\ p_{G_i},\ p_{B_i}$. In the advanced syndrome-trellis codes (STC), the steganographer communicates messages to the receiver by modifying the cover image to the stego image by using LSB matching or ± 1 embedding. That is to say, ternary embedding operations are applied to each pixel, which are represented by $\mathcal{I}_i^R = \{R_i,\ \max(R_i - 1, 0),\ \min(R_i + 1, 255)\}$, $\mathcal{I}_i^G = \{G_i,\ \max(G_i - 1, 0),\ \min(G_i + 1, 255)\}$, and $\mathcal{I}_i^B = \{B_i,\ \max(B_i - 1, 0),\ \min(B_i + 1, 255)\}$. Note that the maximal expected payload that can be communicated between the sender and receiver is the entropy of the manner of embedding probabilities [33]. Thus, we have the following equations.

$$\sum_{i=1}^{n} H(p_{R_i}) = C_R,\ \sum_{i=1}^{n} H(p_{G_i}) = C_G,\ \sum_{i=1}^{n} H(p_{B_i}) = C_B \tag{1}$$

where $H(x) = -2x\log(x) - (1 - 2x)\log(1 - 2x)$ is the ternary entropy function, and $\log(x)$ is at the base of 2. Note that not all the probabilities in each channel would be zero, so the single payload partition in RGB channels would be non-zero.

In order to minimize detectability, the embedding probabilities $p_{R_i}, p_{G_i}, p_{B_i}$ vary depending on the cover image content. Since detectability is not analytically tractable, many existing approaches worked with the notion of "distortion" that is believed to be in close relation to detectability [2], [5]. When the distortion is represented by an additive function, the total embedding distortion is a sum of distortion evaluated in each pixel. The steganographer would like to find the optimal choice of $p_{R_i},\ p_{G_i}, p_{B_i}$ that minimizes the total embedding distortion. Therefore, an optimization model with the constraint is formulated as below.

$$\begin{aligned} &\min \sum_{i=1}^{n} (p_{R_i}\rho_{R_i} + p_{G_i}\rho_{G_i} + p_{B_i}\rho_{B_i}) \\ &s.t.\ \sum_{k_1=1}^{n} H(p_{R_{k_1}}) + \sum_{k_2=1}^{n} H(p_{G_{k_2}}) + \sum_{k_3=1}^{n} H(p_{B_{k_3}}) = m \end{aligned} \tag{2}$$

Due to the additive property of the entropy function $H(x)$, the above payload constraint can be rewritten as below.

$$\sum_{k=1}^{n} [H(p_{R_k}) + H(p_{G_k}) + H(p_{B_k})] = m \tag{3}$$

For the given costs values $\boldsymbol{\rho}_R = (\rho_{R_1}, \rho_{R_2}, \cdots, \rho_{R_n})$, $\boldsymbol{\rho}_G = (\rho_{G_1}, \rho_{G_2}, \cdots, \rho_{G_n})$ and $\boldsymbol{\rho}_B = (\rho_{B_1}, \rho_{B_2}, \cdots, \rho_{B_n})$, according to the construction of simulate optimal embedding, the embedding probabilities would have a form of Gibbs distribution [34]. It means that once the cost values are determined, the steganographer can simulate optimal

embedding by designating the stego elements with the following probabilities.

$$p_{R_i} = \frac{e^{-\lambda \cdot \rho_{R_i}}}{1 + 2e^{-\lambda \cdot \rho_{R_i}}}, \quad p_{G_i} = \frac{e^{-\lambda \cdot \rho_{G_i}}}{1 + 2e^{-\lambda \cdot \rho_{G_i}}}, \quad p_{B_i} = \frac{e^{-\lambda \cdot \rho_{B_i}}}{1 + 2e^{-\lambda \cdot \rho_{B_i}}} \tag{4}$$

Here the parameter λ could be calculated numerically such that the payload constraint (3) holds. Therefore, for the minimization problem in (2), the above embedding probabilities $p_{R_i}, p_{G_i}, p_{B_i}$ are the optimal choice.

Then we substitute (4) into (3), and acquire the value of the parameter λ. Hence, the initial embedding probabilities $p_{R_i}, p_{G_i}, p_{B_i}$ are obtained.

We define p^t as a threshold probability for determining the modifications as below.

$$p^t = (p^{max} - \overline{p})(1 - 2m/n) + \overline{p} \tag{5}$$

where p^{max} and $\overline{p}$ are the max and average probability in three channels, respectively. The threshold probability p^t should be bigger than the average probability $\overline{p}$, and the increment is defined as the difference between the max probability p^{max} and the average probability $\overline{p}$. When the amount of secret data m becomes larger, more pixels could be selected for embedding, so the threshold probability p^t would decrease. In order to maintain the imperceptible image distortion, the max embedding payload rate is limited to 0.5 bpc (bits per channel), and thus the coefficient is set as $1 - 2m/n$.

Note that we only use one threshold probability p^t for all three color channels, instead of three separate parameters. The threshold probability p^t is determined by three color channels, and calculated by using all the embedding probabilities in RGB channels. Thus, all the pixels in three channels are correlated and taken into account together.

For the i-th pixel pixels R_i, G_i, B_i in RGB channels, determine if the initial embedding probabilities $p_{R_i}, p_{G_i}, p_{B_i}$ are greater than the threshold probability p^t, and then p_{R_i}, p_{G_i}, p_{B_i} would be modified. Now we calculate T_i as the modification identification.

$$T_i = f(p_{R_i}) + f(p_{G_i}) + f(p_{B_i}) \tag{6}$$

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

$$f(z) = \begin{cases} 1, & \text{if } z > p^t \\ 0, & \text{others} \end{cases} \tag{7}$$

According to the value of T_i, the distortion costs $\rho_{R_i}, \rho_{G_i}, \rho_{B_i}$ in RGB channels are updated as follows.

$$\rho'_{X_i} = \begin{cases} \rho_{X_i}/3\alpha, & \text{if } T_i = 3 \\ \rho_{X_i}/\alpha, & \text{if } T_i = 2 \ \& \ f(p_{X_i}) = 1 \\ \rho_{X_i}, & \text{others} \end{cases} \tag{8}$$

where $\alpha \geq 1$ is a scaling factor, and $X = \{R, G, B\}$ represents the red, green and blue channels.

For the case $T_i = 3$, all of three embedding probabilities p_{R_i}, p_{G_i}, p_{B_i} are greater than the threshold probability p^t. To ensure that three corresponding pixels p_{R_i}, p_{G_i}, p_{B_i} are embedded simultaneously, three distortion costs $\rho_{R_i}, \rho_{G_i}, \rho_{B_i}$ would be decreased homogeneously. For the case $T_i = 2$, two of the embedding probabilities p_{R_i}, p_{G_i}, p_{B_i} are greater than p^t and one is smaller. We only adjust two distortion costs with higher embedding probabilities. For the case $T_i = 1$, only one embedding probability is greater than p^t, we do not decrease three distortion costs, in order that all of three corresponding pixels p_{R_i}, p_{G_i}, p_{B_i} are not embedded. Therefore, the proposed ACMP strategy looks for high embedding probabilities in at least two channels, and then reduces the costs of the pixel values in all three channels. Specifically, if more than one embedding probabilities p_{R_i}, p_{G_i}, p_{B_i} of the corresponding pixels R_i, G_i, B_i are higher, the distortion costs ρ_{R_i}, ρ_{G_i}, ρ_{B_i} would be decreased, so as to amplify the channel modification probabilities and embed bits into R_i, G_i, B_i simultaneously. It might be effective in resisting modern steganalyzers equipped with channel co-occurrences features, and improving the empirical steganographic security.

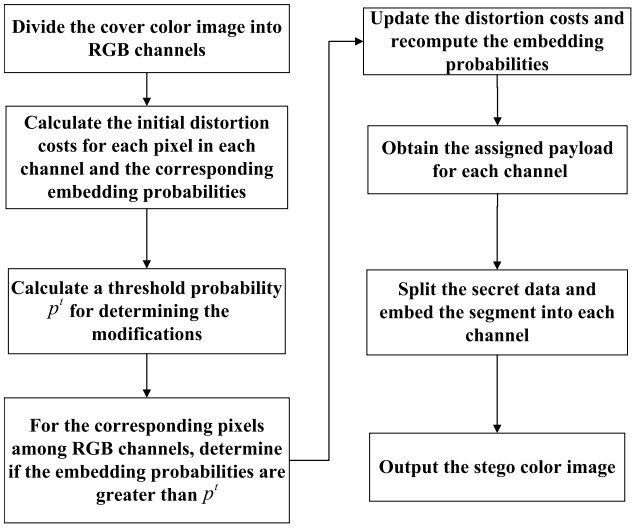


Fig. 2. Flowchart of the proposed ACMP strategy.

Furthermore, we use the updated distortion costs ρ'_{R_i}, ρ'_{G_i}, ρ'_{B_i} to replace the initial distortion costs $\rho_{R_i}, \rho_{G_i}, \rho_{B_i}$ in (4), and then substitute it into (3). The updated parameter λ' is recalculated and thus the new embedding probabilities $p'_{R_i}, p'_{G_i}, p'_{B_i}$ are obtained. According to (1), we can acquire the embedding payload C_R, C_G, C_B in each color channel. For a given payload partition, we split the secret data and embed the segment into each color channel. The optimal embedding simulator, or practical steganographic code STC, can be applied for data embedding in each color channel. Finally, the stego color image is obtained.

The proposed ACMP strategy is only required to execute two iterations. The flowchart of the ACMP strategy is illustrated in Fig. 2. In the first round, we calculate the initial distortion costs and the corresponding embedding probabilities, and then modify the distortion costs in order to amplify the channel modification probabilities. In the second round, we recompute the new embedding probabilities by using

the modified distortion costs. The assigned payload in RGB channels is directly obtained by (1).

It can be observed that, for high embedding payload rate, the proposed ACMP strategy could obtain large enhancement of anti-steganalysis performance. The reason is that the modifications in the ACMP strategy are related to the payload rate. According to (5-7), when the payload rate is high, the threshold probability p^t is smaller and thus more distortion costs would be modified. The anti-steganalysis performance could be increased notably. In contrast, when the payload rate is low, the effect of distortion costs modification is not obvious, and thus the advantage of the proposed strategy is not prominent. The above conclusion is also validated by the numerical results in section IV.

The modifications of the distortion costs are determined by the scaling factor α. As shown in section IV-B, the scaling factor α has a slight impact on the anti-steganalysis performance. It might be difficult for an adversary to recover the payload assignment without the cover image and scaling factor α [37]. In order to ensure the accurate data extraction, some auxiliary information about the detailed payload partition C_R, C_G, C_B and the scaling factor α should be shared between the sender and receiver. In a practical application, these values could be encoded as four 18-bit segments. Totally 72 bits of the auxiliary information are embedded into some LSBs of RGB pixels by using LSB matching algorithm with a shared stego key. Finally, the recipient reads the secret messages by using the same STC applied to each channel and concatenating three parts.

B. Discussions

In the proposed ACMP strategy, RGB three channels are considered discriminately. The default strategy of color image steganography is to divide the messages into three equal parts and indiscriminately embed each part into one of RGB channels. Although the simple color concatenation (SCC) strategy could automatically distribute the payload unevenly, it still considers three channels equally. Moreover, the correlations among the i-th pixel R_i, G_i, B_i in RGB channels is explored. The ACMP strategy looks for high embedding probabilities in at least two channels, and then reduces the costs of the pixel values in all three channels. For the pixels in textured regions, three embedding probabilities $p_{R_i}, p_{G_i}, p_{B_i}$ are simultaneously amplified, and thus the embedding impacts would be clustered. The ACMP strategy could pay attention to having a more homogeneous (between channels) embedding. In addition, the detailed payload allocation is completely depending on different properties among RGB channels. The threshold probability p^t is determined by three color channels, and calculated by using all the embedding probabilities in RGB channels. For three color components, the number of distortion costs to be modified is distinct, and thus the number of secret bits to be embedded is different.

The proposed ACMP strategy could efficiently make the embedding changes concentrated in textured regions. For a given tolerable distortion ρ_0, the steganographer communicates messages to the receiver by modifying the image pixels, and the distortion ρ would increase with the increase of the embedding capacity. When the distortion ρ approaches to ρ_0, the present embedding capacity is called as "maximum secure capacity". For some special true color images (e.g. green grass, blue sky), there is a great difference of brightness among RGB components. It implies that texture regions of three color channels are significantly distinct. If the embedding payload is still distributed equally, some pixels in the smooth regions would be modified. That is to say, for some color channel without abundant brightness, the number of secret bits to be embedded might exceed the "maximum secure capacity". On the contrary, the proposed ACMP strategy assigns the embedding payload adaptively by accumulating three channel distortion costs, which are the approximate evaluation of image smoothness. Therefore, the ACMP strategy is able to make the embedding changes concentrated in heavily textured regions, and thus obtain anti-steganalysis performance enhancement. The related experiments are shown in section IV-C.

Compared with tradition image steganographic methods, the procedure of the proposed ACMP strategy is an additional module, which could be divided into three parts. The first part is to calculate the max probability p^{max}, average probability $\overline{p}$, and threshold probability p^t. For a color image with size of $n_1 \times n_2$, the computation complexity of these operations is no more than $O(3 \times n_1 \times n_2)$. The second part is to calculate the modification identification T_i. The steganographer are required to do some basic arithmetic operations for each pixel, so the computation cost is $O(3 \times n_1 \times n_2)$. The last part is to modify the distortion costs in RGB channels, and the computation complexity is $O(3 \times n_1 \times n_2)$. Thus, the overall increased computation complexity is $O(3 \times n_1 \times n_2)$. In simple color concatenation (SCC), three color components are concatenated into a new image, and thus the computation complexity is also $O(3 \times n_1 \times n_2)$. The new color image steganographic schemes incorporated with the proposed ACMP strategy can be solved in polynomial time.

It can be observed in section IV, the proposed ACMP strategy could acquire better anti-steganalysis performance than SCC. Further, in the proposed ACMP strategy, all the pixels in three channels are correlated and considered together. When embedding the secret data into one channel, other two channels are simultaneously taken into account. Therefore, the ACMP strategy could not only fully exploit the difference of image texture in three channels, but also efficiently cluster the embedding impacts among RGB channels. For some special color images with relatively different brightness among RGB components, it is wiser for a steganographer to use ACMP instead of SCC.

We have to point out that the new color image steganographic schemes incorporated with the proposed ACMP strategy would be considered as "overly adaptive" steganography, which might be less secure. This is a result that was inspired by game-theoretical analyses of steganography [35], [36] and can also be seen in WOW being insecure against the new steganalytic feature sets (e.g., maxSRMd2 [20]). Thus, this might lead to an adapted version of SCRM [28] and SGRM [31] to easily detect the new color image steganographic schemes equipped with the ACMP strategy, even without knowing the scaling

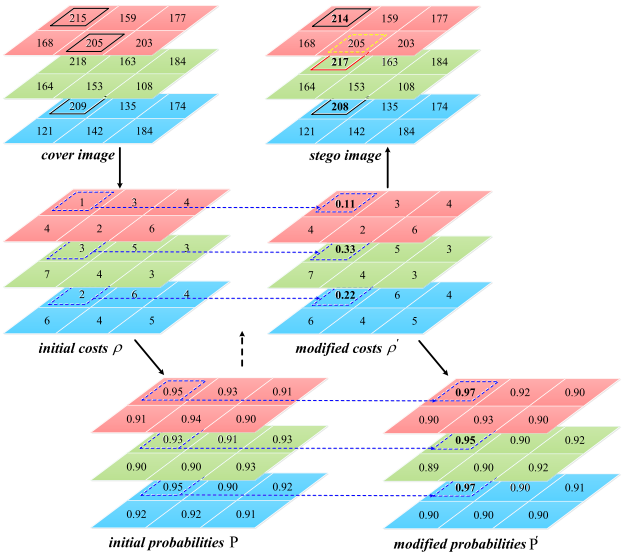


Fig. 3. An example of the proposed ACMP strategy.

factor α. It is worth incorporating the knowledge of embedding probabilities with game-theoretic analyses, and investigating how to resist new adaptive steganalysis approaches. That is an important part of our future work.

C. An Illustration Example

In this subsection, we use a simple example to illustrate the proposed strategy. Suppose we have a color cover image as shown in Fig. 3, it can be represented as three vectors $[\mathbf{R}, \mathbf{G}, \mathbf{B}]$, and by the scanning order of zig-zag, $\mathbf{R} = (R_1, R_2, R_3, R_4, R_5, R_6) = (215, 159, 177, 168, 205, 203)$, $\mathbf{G} = (G_1, G_2, G_3, G_4, G_5, G_6) = (218, 163, 184, 164, 153, 108)$, $\mathbf{B} = (B_1, B_2, B_3, B_4, B_5, B_6) = (209, 135, 174, 121, 142, 184)$. Suppose 7 bits messages will be embedded into cover image, and thus the positions marked by the black solid box in cover image will be modified. The corresponding distortion costs $\boldsymbol{\rho}$ are obtained by using the existing distortion function. Assume the initial costs $\boldsymbol{\rho}_R = (1, 3, 4, 4, 2, 6)$, $\boldsymbol{\rho}_G = (3, 5, 3, 7, 4, 3)$, $\boldsymbol{\rho}_B = (2, 6, 4, 6, 4, 5)$, and the scaling factor $\alpha = 3$.

According to the initial costs $\boldsymbol{\rho}$, we can compute the initial embedding probabilities $\mathbf{P}$, so the average probability $\overline{p}$ and the maximum probability p^{max} are 0.92 and 0.95, respectively. According to (5), $p^t = 0.92 + (0.95 - 0.92) \times (1 - 2 \times 7/18) = 0.926$. It is shown that the embedding probabilities of R_1, G_1, B_1 are bigger than p^t, so the modification identification $T_1 = 3$. All the costs in three channels would be modified, $\rho'_{R_1} = 1/9 = 0.11$, $\rho'_{G_1} = 3/9 = 0.33$ and $\rho'_{B_1} = 2/9 = 0.22$. Although the embedding probability of G_6 is bigger than p^t, those of R_6, B_6 are smaller than p^t. Thus, the cost values of $\rho_{R_6}, \rho_{G_6}, \rho_{B_6}$ do not need to be changed. (R_2, G_2, B_2), (R_3, G_3, B_3) and (R_5, G_5, B_5) are experiencing similar cases. For R_4, G_4, B_4, all the embedding probabilities of three channels are smaller than p^t, so their cost values are not required to be modified.

According to the updated distortion costs $\boldsymbol{\rho}'$, the corresponding embedding probabilities are modified. Note that the new embedding probabilities of the pixels R_1, G_1, B_1 are simultaneously amplified. We embed the messages into the cover image and then obtain the stego image. It is shown that the positions marked by the solid box in the final stego image are changed. The position marked by the red solid box G_1 would be modified, while the position marked by the yellow dotted box R_5 would not be modified. R_1, G_1, B_1 are simultaneously embedded, which might be effective in resisting modern steganalyzers equipped with channel co-occurrences features. Therefore, the proposed ACMP strategy could amplify the modification probabilities of these corresponding pixels in RGB channels, and then improve the anti-steganalysis performance.

IV. Experimental Results

In this section, several experimental results and analysis are presented to demonstrate the feasibility and effectiveness of the proposed ACMP strategy.

A. General Setup

In a real application, to verify the steganographic security with respect to a blind steganalyzer is generally accepted. Image steganalysis is always based on extracting steganalytic features, which are regularly considered as the probability of pixel residuals in co-occurrences. For the covers and their corresponding stego images with different steganographic schemes and embedding payload rates, the features for the steganalysis tools are extracted. Half of the cover and stego features are taken into ensemble classifier to learn and train features, and the remaining half are used to test in ensemble classifier for calculating detection errors. The ensemble classifier [38] with Fisher linear discriminant as the base learner is incorporated in our experiments, because it enables fast training in high-dimensional feature spaces and has a comparable performance to that of SVM [39] working on low-dimensional feature sets. The detection performance is quantified using the ensemble's "out-of-bag" error rate E_{oob}. E_{oob} is an unbiased estimate of the testing error, which is the average decision error rate of the probability of false positive rate (detecting cover as stego) and the probability of false negative rate (missed detection). We experiment 10 times by randomly splitting the training and testing images in the following subsections, and calculate the average E_{oob}. The higher E_{oob} is, the better steganographic security is. In this paper, the E_{oob} value is expressed in percentage.

Two mainstream universal feature sets for color image steganalysis SCRM (spatio-color rich model) with 18,157 features [28] and SGRM (steerable Gaussian rich model) with 22,563 features [31] are employed to evaluate the security performance of the involved color image steganographic schemes. SCRM consists of two different components. The first one is computed for each color channel, and the other component is a collection of three channel co-occurrences. SGRM estimates the image edge direction by applying steerable Gaussian filters, and computes the co-occurrence matrices of pixel pairs. Both of them are the state-of-art steganalyzers, and the experiments included in [28] and [31] have demonstrated that

TABLE I
STEGANALYTIC PERFORMANCE FOR HILL-ACMP SCHEME WITH DIFFERENT VALUES OF THE SCALING FACTOR α

α	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
E_{oob}	21.82	21.88	22.00	21.55	21.39	21.57	21.24	21.02	21.01

these steganalysis features work especially well against the steganographic schemes designed to hide messages in color images represented in the spatial domain.

In the following experiments, WOW [7], S-UNIWARD [8] and HILL [9] are combined with the proposed ACMP strategy 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-B*ö*hme filter, and two low-pass filters are 3×3 and 15×15 average filters, respectively. All the parameter settings ensure that the corresponding methods can provide enough capacity while maintaining the highest statistical undetectability. When applying the proposed ACMP strategy to these state-of-the-art image steganographic methods, we abbreviate the entire color image steganographic scheme as WOW-ACMP, S-UNIWARD-ACMP and HILL-ACMP, respectively.

B. Impact of the Scaling Factor

In the proposed method, the scaling factor α is used to adjust the distortion costs. It is important to evaluate the effect of the scaling factor α on the anti-steganalysis performance in the proposed strategy. If α is too large, the costs would become much smaller, resulting in many pixels with extremely high modification probability. It will bring excessive influence on the realization of STC. Thus, we limit the value range of α. We take HILL-ACMP scheme as an example when the embedding payload rate is 0.4 bpc (bits per channel), and vary the value of the scaling factor α. The resulting steganalytic performance of SCRM is given in Table I.

It can be observed the scaling factor α has a slight impact on the anti-steganalysis performance of new color image steganographic schemes with ACMP strategy. The security performance is the best when $\alpha = 3$, and the performance would be worse if $\alpha > 3$. Therefore, we will set $\alpha = 3$ in the following experiments.

C. Embedding Changes Analysis

To verify whether the proposed ACMP strategy could effectively concentrate the embedding modifications into the textured areas, Fig. 4 illustrates the cover color image and the corresponding embedding changes using two image steganographic schemes WOW and WOW-ACMP, with the same embedding payload rate 0.4 bpc. A color image "539.ppm", as shown in Fig. 4(a), is chosen from BOSSBase image set [40], and Fig. 4(b) shows the blue channel of the cover image. Fig. 4(c) and Fig. 4(d) are the difference of blue channel between the cover and stego images by using WOW and WOW-ACMP, respectively. Here dark pixels represent the actual embedding changes.

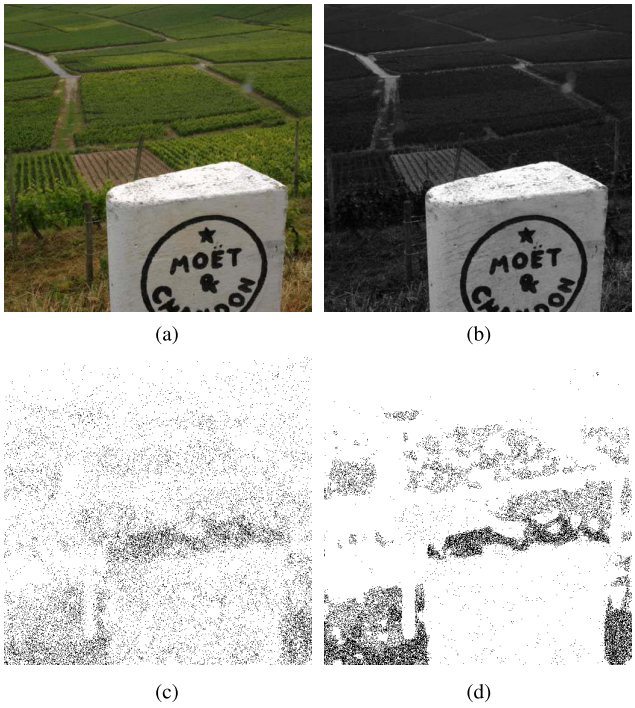


Fig. 4. Illustration of cover color image and actual embedding changes executed by WOW and WOW-ACMP. (a) Cover image. (b) Blue channel. (c) Embedding changes in blue channel (WOW). (d) Embedding changes in blue channel (WOW-ACMP).

It can be observed that the locations of embedding changes vary for different image steganographic schemes. In WOW scheme, some embedding changes in blue channel are located in smooth areas. When combining with the proposed ACMP strategy, WOW-ACMP could make the embedding changes concentrated in textured regions. The reason for the differences is that, for the given color image, the number of secret bits to be embedded into blue channel has exceeded the "maximum secure capacity". Fig. 4(b) indicates that there is not abundant brightness in blue component. More secret bits are supposed to embed in red and green channels, while less secret bits are assigned to blue channel. Therefore, the allocated payload in RGB color components should be distinct instead of uniform partition. The proposed ACMP strategy could efficiently make the embedding changes concentrated mainly in textured regions, and thus obtain anti-steganalysis performance enhancement.

D. Performance for Payload Partition

In this subsection, we will show the detailed payload partition for RGB channels using our proposed ACMP strategy. Some classic color images are applied, and the embedding payload rate is 0.2 bpc. The percentage values (%) of payload partition in RGB channels for classic color images using WOW-ACMP, S-UNIWARD-ACMP and HILL-ACMP are given in Table II.

It is shown that the payload partitions using the proposed ACMP strategy are quite different from average

TABLE II

THE PERCENTAGE VALUES (%) OF PAYLOAD PARTITIONS IN RGB CHANNELS FOR CLASSIC COLOR IMAGES USING WOW-ACMP, S-UNIWARD-ACMP AND HILL-ACMP

	WOW-ACMP			S-UNIWARD-ACMP			HILL-ACMP		
	Red	Green	Blue	Red	Green	Bluen	Red	Green	Blue
Airplane	26.53	37.28	36.19	29.50	35.34	35.16	24.86	32.01	43.13
Baboon	29.02	34.18	36.80	29.80	33.97	36.23	36.40	37.11	26.49
Barb	36.48	22.74	40.77	35.57	25.69	38.74	33.41	31.93	34.66
House	35.81	41.21	22.98	35.46	37.70	26.84	34.98	41.47	23.55
Lake	21.44	39.18	39.38	25.72	36.87	37.41	33.29	47.68	19.03
Lena	11.78	33.91	54.31	17.13	34.46	48.42	8.64	29.16	62.19
Peppers	36.63	31.23	32.13	36.11	30.52	33.37	66.75	21.85	11.40
Tiffany	16.97	49.81	33.21	16.91	46.11	36.97	8.84	47.38	43.77

TABLE III

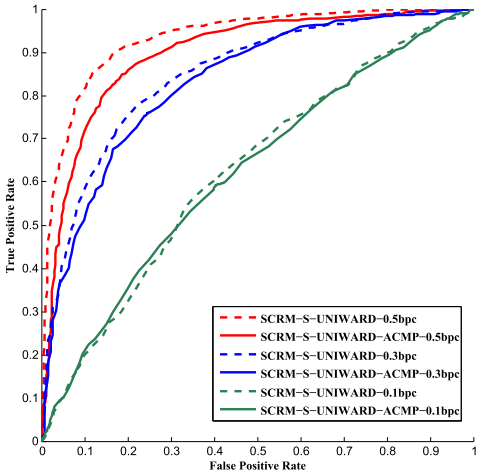
COMPARISONS OF ERRORS E_{oob} BASED ON THE TESTING IMAGE DATABASE AGAINST SCRM AND SGRM STEGANALYSIS

Payload	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**
WOW (SCRM)	40.19	31.06	24.39	18.49	14.73
WOW-ACMP (SCRM)	40.44	31.38	24.63	19.98	15.21
S-UNIWARD (SCRM)	40.16	29.87	22.27	17.44	13.67
S-UNIWARD-ACMP (SCRM)	40.46	31.15	23.68	20.00	16.78
HILL (SCRM)	40.25	31.63	24.56	19.54	15.83
HILL-ACMP (SCRM)	40.93	32.06	26.49	21.99	16.49
WOW (SGRM)	45.60	40.05	35.67	29.71	25.41
WOW-ACMP (SGRM)	45.69	41.50	36.53	32.62	26.27
S-UNIWARD (SGRM)	45.60	40.49	34.95	29.81	23.50
S-UNIWARD-ACMP (SGRM)	46.50	41.07	35.76	30.54	28.74
HILL (SGRM)	46.17	41.33	35.45	30.20	25.50
HILL-ACMP (SGRM)	46.24	41.36	37.40	32.79	28.89

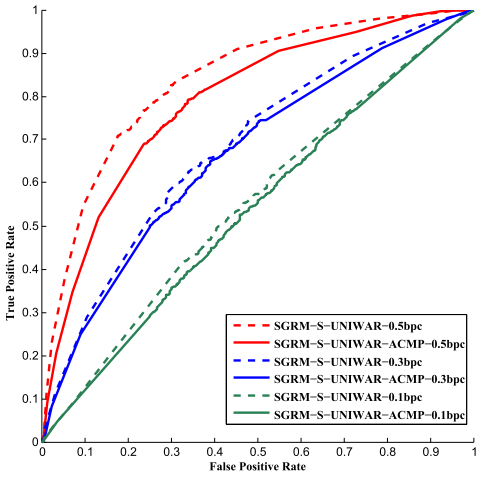
payload assignment. The proposed ACMP strategy could assign the embedding payload adaptively.

E. Comparisons to State-of-the-Art Schemes

In this subsection, we first use the testing image database consisted of 1034 color 768 × 576 TIF images from McGill [41], 1338 color 512 × 384 TIF images from UCID [42]. The embedding payload rates range from 0.1 bpc to 0.5 bpc. That is to say, for a color 512 × 384 TIF image from UCID database, the embedding payload ranges from 58,982 bits to 294,912 bits. We compare the performance of the state-of-the-art steganographic schemes WOW, S-UNIWARD, HILL, and the new ones equipped with the proposed ACMP strategy, against the SCRM and SGRM steganalysis. Table III shows all the detection errors E_{oob} obtained by the proposed schemes are higher. For example, the detection error of S-UNIWARD-ACMP against SCRM steganalysis is 20.00 when the embedding payload rate is 0.4 bpc. Compared with the error 17.44 when S-UNIWARD is utilized with average payload



(a)



(b)

Fig. 5. ROC curves illustrating the anti-steganalysis performance of S-UNIWARD and S-UNIWARD-ACMP, against the SCRM and SGRM steganalysis. (a) ROC curves of S-UNIWARD and S-UNIWARDACMP resisting SCRM. (b) ROC curves of S-UNIWARD and S-UNIWARDACMP resisting SGRM.

distribution, ours can improve the anti-steganalysis performance by 2.56. Furthermore, Fig. 5 reports the receiver-operating characteristic (ROC) curves, to illustrate the

TABLE IV

COMPARISONS OF ERRORS E_{oob} BETWEEN HILL AND HILL-ACMP BASED ON THE BOSSBASE IMAGE SET AGAINST SCRM AND SGRM STEGANALYSIS

Payload	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**
HILL (SCRM)	29.33	17.12	10.70	6.97	4.54
HILL-ACMP (SCRM)	30.81	18.40	11.63	7.05	4.60
HILL (SGRM)	44.83	39.50	35.98	28.79	25.32
HILL-ACMP (SGRM)	46.11	41.23	36.28	29.68	25.83

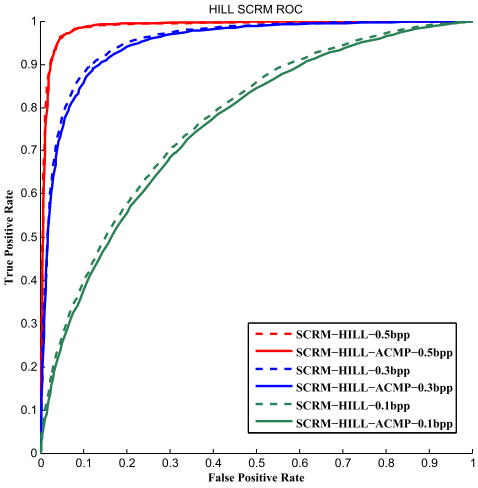


Fig. 6. ROC curves of HILL and HILL-ACMP resisting SCRM steganalysis.

anti-steganalysis performance of S-UNIWARD and the new color image steganographic scheme S-UNIWARD-ACMP with the embedding payload rates 0.1 bpc, 0.3 bpc and 0.5 bpc, against the SCRM and SGRM steganalysis. It is also shown that the proposed ACMP strategy could obtain improvements in the detection performance.

To further evaluate the performance, the following image set is used in the experiments. The image set is obtained from the standard color BOSSBase image set [40], containing 10,000 full-resolution raw color images. We first apply Photoshop CS6 for demosaicking these raw images, and then resample the obtained images to true color images with the size of 512 × 512 using a bilinear kernel. A number of 5000 randomly selected cover images and their stego counterparts are used for training, while the rest 5000 cover images and their stego counterparts are used for testing. Although both the training images and testing images are selected from the BoSSBase image set, an image is included in either the training phase or the testing phase. Table IV shows the comparisons of detection errors between HILL and HILL-ACMP in resisting the SCRM and SGRM steganalysis. The results indicate the new color image steganographic scheme with the ACMP strategy could achieve better performance on resisting the modern steganalysis. For example, with the embedding payload rate 0.2 bpc, the detection error of HILL against SGRM steganalysis is 39.50, the detection error rate of the proposed HILL-ACMP is 41.23, which is improved by 1.73. Moreover, Fig. 6 shows the ROC curves of HILL and HILL-ACMP resisting the SCRM steganalysis, when the embedding payload rates are 0.1 bpc, 0.3 bpc and 0.5 bpc. It can also be observed that HILL-ACMP performs better in resisting the advanced color image steganalyzers.

From the above, we can conclude that the proposed adaptive color image steganography with the ACMP strategy is more secure, which are evaluated by the modern powerful color image steganalysis. Furthermore, for high embedding payload rate, the probability threshold p^t is smaller and thus more distortion costs would be modified. The effect of distortion costs modification would be obvious, and the proposed ACMP strategy might acquire large enhancement of anti-steganalysis performance.

TABLE V

COMPARISONS OF STEGANALYTIC PERFORMANCE BETWEEN HILL-SCC AND HILL-ACMP

Payload	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**
HILL-SCC (SCRM)	40.50	31.85	26.09	20.63	17.43
HILL-ACMP (SCRM)	40.93	32.06	26.49	21.99	16.49
HILL-SCC (SGRM)	45.87	41.02	37.29	31.25	28.62
HILL-ACMP (SGRM)	46.24	41.36	37.39	32.79	28.89

TABLE VI

DETECTION ACCURACIES (%) FOR HILL, HILL-SCC AND HILL-ACMP AGAINST THE CNN-BASED STEGANALYSIS APPROACH

Payload	**0.1**	**0.3**
HILL	71.63	91.32
HILL-SCC	67.14	88.36
HILL-ACMP	66.89	89.94

F. Comparisons to Simple Color Concatenation

Simple color concatenation (SCC) would consider a color image as a three times larger gray-scale image, and then embed the payload into the new larger image. When the modern distortion function in HILL method is utilized, the corresponding color image steganographic scheme is denoted as HILL-SCC.

The comparison results of detection errors E_{oob} between HILL-SCC and HILL-ACMP are given in Table V. Compared with this simple color concatenation, the new color image steganographic scheme using the proposed ACMP strategy could achieve better statistical undetectability against the state-of-the-art steganalyzer. For example, with the embedding payload rate 0.4 bpc, the detection error of HILL-SCC against SCRM steganalysis is 20.63, and the detection error of the proposed HILL-ACMP is 21.99, which is improved by 1.36.

G. Anti-Steganalysis Performance of the CNN-Based Steganalysis Approach

Recently, convolutional neural network (CNN) has attracted increasing attention due to the excellent performance. Researchers have begun to investigate the potential of CNN in image steganalysis [43], [44]. In order to investigate whether the proposed method is effective in resisting steganalyzers

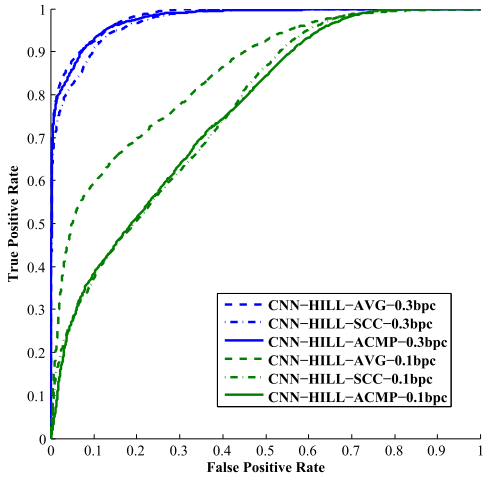


Fig. 7. ROC curves of HILL, HILL-SCC and HILL-ACMP resisting the CNN-based steganalysis approach.

equipped with CNN, we conduct additional experiments by using the modern CNN-based steganalysis approach [43].

The BOSSbase image set consisting of 10,000 color images of size 512×512 is randomly split into a training set with 4,000 cover and stego image pairs, a validation set with 1,000 image pairs, and a testing set containing 5,000 image pairs. All of the CNN experiments are conducted by using a modified version of the Caffe toolbox [45]. We run our experiments using NVIDIA TITAN XP GPU with 12GB RAM. Mini-batch stochastic gradient descent is utilized to solve all the CNN in the experiments. The cross-entropy loss function is adopted to minimize the distance between the true label and the predicted label. In the training and validation, the batch size is set to 16 images, the momentum value is fixed to 0.9, the weight decay is 0.0005, and the maximal iteration epoch is 200. The initial learning rate is set to 0.0001, and scheduled to decay with the learning rate policy "inv" where the power is 0.75 and the gamma is 0.0001.

We compare the detection performance of HILL, HILL-SCC and HILL-ACMP with the embedding payload rates 0.1 bpc and 0.3 bpc. Table VI shows the detection accuracies and Fig. 7 illustrates the corresponding ROC curves. It can be observed that the new color image steganographic scheme equipped with the proposed ACMP strategy could provide better performance than average payload partition, and have competitive performance compared with simple color concatenation. When the embedding payload rate is higher, such as 0.3 bpc, the proposed ACMP strategy considers the inter-channel correlations among RGB channels, which might result in more embedding changes concentrated in one or two textured channels. Note that CNN is trained to learn the difference between cover images and stego images, and HILL-ACMP would increase the difference in the textured channels. Thus, for higher payload rates, compared with HILL-SCC, it might be a litter easier for the modern CNN-based steganalyzers to learn and obtain the steganalysis features, which are extracted from stego images generated by HILL-ACMP. In addition, although the modern CNN-based steganalysis approach [43] could automatically combine feature extraction and classification steps in the unique framework, the detector is not specifically designed for color image features, and then the "fully automatic" tool could not be optimized. Thus, ACMP and SCC would have competitive performance against the advanced CNN-based steganalyzer.

V. Conclusions

Conventional true color image steganography seldom pays attention to different properties among RGB channels, and thus the embedding payload is equally partitioned and indiscriminately embedded into each channel. In this paper, we mainly focus on utilizing the correlations among three color components for performance enhancement. Our contributions can be summarized in the following aspects.

1) To the best of our knowledge, this is the first time to investigate payload partition in color image steganography. We exploit inter-channel correlations to allocate embedding payload for RGB channels.
2) We design a novel amplifying channel modification probabilities strategy, which could cluster the embedding impacts of RGB channels, and effectively make the embedding changes concentrated in textured regions.
3) The proposed ACMP strategy could be incorporated into these state-of-the-art steganographic methods. Compared with average payload partition and simple color concatenation, experimental results demonstrate that new color image steganographic schemes could acquire anti-steganalysis performance enhancement.

It should be pointed out that our work in this paper only focuses on the true color images in raster formats. In contrast to RGB model, YCbCr model is more practical in image processing, especially for JPEG color images. Since the human visual system is much more sensitive to variations in brightness than color, chroma subsampling always encodes chrominance components Cb and Cr with lower resolution, and thus there are different sample rates and fewer correlations in YCbCr color model. In the future, we plan to extend the proposed payload partition strategy to JPEG color image steganography.

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. D. Ker *et al.*, "Moving steganography and steganalysis from the laboratory into the real world," in *Proc. ACM Workshop Inf. Hiding Multimedia Secur.*, Montpellier, France, 2013, pp. 45–58.
[3] X. Liao, Z. Qin, and L. Ding, "Data embedding in digital images using critical functions," *Signal Process., Image Commun.*, vol. 58, pp. 146–156, Oct. 2017.
[4] 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.
[5] 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.
[6] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Proc. Int. Workshop Inf. Hiding*, Calgary, AB, Canada, 2010, pp. 161–177.
[7] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, Tenerife, Spain, Dec. 2012, pp. 234–239.
[8] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," in *Proc. ACM Workshop Inf. Hiding Multimedia Secur.*, Montpellier, France, 2013, pp. 59–68.

[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.*, Paris, France, Oct. 2014, pp. 4206–4210.

[10] S. Kouider, M. Chaumont, and W. Puech, "Adaptive steganography by oracle (ASO)," in *Proc. IEEE Int. Conf. Multimedia Expo*, San Jose, CA, USA, 2013, pp. 1–6.

[11] P. Sallee, "Model-based steganography," in *Proc. Int. Workshop Digit. Watermarking*, Seoul, South Korea, 2003, pp. 154–167.

[12] 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.

[13] A. D. Ker, "Estimating steganographic Fisher information in real images," in *Proc. Int. Workshops Inf. Hiding*, Darmstadt, Germany, 2009, pp. 73–88.

[14] V. Sedighi, J. Fridrich, and R. Cogranne, "Content-adaptive pentary steganography using the multivariate generalized Gaussian cover model," *Proc. SPIE*, vol. 9409, Mar. 2015, Art. no. 94090H.

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

[17] 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.

[18] W. Zhang, Z. Zhang, L. Zhang, H. Li, and N. Yu, "Decomposing joint distortion for adaptive steganography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 27, no. 10, pp. 2274–2280, Oct. 2017.

[19] 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.

[20] T. Denemark, V. Sedighi, and V. Holub, "Selection-channel-aware rich model for steganalysis of digital images," in *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, Atlanta, GA, USA, Dec. 2014, pp. 48–53.

[21] Y. Ma, X. Luo, X. Li, Z. Bao, and Y. Zhang, "Selection of rich model steganalysis features based on decision rough set α-positive region reduction," *IEEE Trans. Circuits Syst. Video Technol.*, to be published. doi: 10.1109/TCSVT.2018.2799243.

[22] G. Cancelli and M. Barni, "MPSteg-color: A new steganographic technique for color images," in *Proc. Int. Workshop Inf. Hiding*, Saint Malo, France, 2007, pp. 1–15.

[23] G. Cancelli and M. Barni, "MPSteg-color: Data hiding through redundant basis decomposition," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 346–358, Sep. 2009.

[24] S. Ahani and S. Ghaemmaghami, "Colour image steganography method based on sparse representation," *IET Image Process.*, vol. 9, no. 6, pp. 496–505, 2015.

[25] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, "CISSKA-LSB: Color image steganography using stego key-directed adaptive LSB substitution method," *Multimedia Tools Appl.*, vol. 76, no. 6, pp. 8597–8626, 2017.

[26] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "Image steganography using uncorrelated color space and its application for security of visual contents in online social networks," *Future Gener. Comput. Syst.*, vol. 86, pp. 951–960, Sep. 2018.

[27] W. Tang, B. Li, W. Luo, and J. Huang, "Clustering steganographic modification directions for color components," *IEEE Signal Process. Lett.*, vol. 23, no. 2, pp. 197–201, Feb. 2016.

[28] M. Goljan, J. Fridrich, and R. Cogranne, "Rich model for steganalysis of color images," in *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, Atlanta, GA, USA, Dec. 2014, pp. 185–190.

[29] M. Kirchner and R. Böhme, "'Steganalysis in technicolor' boosting WS detection of stego images from CFA-interpolated covers," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Florence, Italy, May 2014, pp. 3982–3986.

[30] H. Abdulrahman, M. Chaumont, P. Montesinos, and B. Magnier, "Color images steganalysis using RGB channel geometric transformation measures," *Secur. Commun. Netw.*, vol. 9, no. 15, pp. 2945–2956, 2016.

[31] H. Abdulrahman, M. Chaumont, P. Montesinos, and B. Magnier, "Color image steganalysis based on steerable Gaussian filters bank," in *Proc. ACM Workshop Inf. Hiding Multimedia Secur.*, New York, NY, USA, 2016, pp. 109–114.

[32] R. Böhme, "An epistemological approach to steganography," in *Proc. Int. Workshop Inf. Hiding*, Darmstadt, Germany, 2009, pp. 15–30.

[33] C. Cachin, "An information-theoretic model for steganography," in *Proc. Int. Workshop Inf. Hiding*, Portland, OR, USA, 1998, pp. 306–318.

[34] J. Fridrich and T. Filler, "Practical methods for minimizing embedding impact in steganography," *Proc. SPIE*, vol. 6505, Feb. 2007, Art. no. 650502.

[35] P. Schöttle and R. Böhme, "A game-theoretic approach to content-adaptive steganography," in *Proc. Int. Conf. Inf. Hiding*, Berkeley, CA, USA, 2012, pp. 125–141.

[36] P. Schöttle, S. Korff, and R. Böhme, "Weighted stego-image steganalysis for naive content-adaptive embedding," in *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, Tenerife, Spain, Dec. 2012, pp. 193–198.

[37] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE Multimedia Mag.*, vol. 25, no. 4, pp. 46–56, Oct./Dec. 2018.

[38] 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.

[39] C. C. Chang and C. J. Lin, "LIBSVM: A library for support vector machines," *ACM Trans. Intell. Syst. Technol.*, vol. 2, no. 3, pp. 1–27, 2011.

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

[41] A. Olmos and F. A. Kingdom, "A biologically inspired algorithm for the recovery of shading and reflectance images," *Perception*, vol. 33, no. 12, pp. 1463–1473, 2004.

[42] G. Schaefer and M. Stich, "UCID: An uncompressed color image database," *Proc. SPIE*, vol. 5307, pp. 472–480, Dec. 2003.

[43] G. Xu, H.-Z. Wu, and Y.-Q. Shi, "Structural design of convolutional neural networks for steganalysis," *IEEE Signal Process. Lett.*, vol. 23, no. 5, pp. 708–712, May 2016.

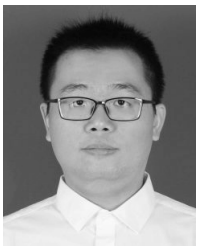
[44] B. Li, W. Wei, A. Ferreira, and S. Tan, "ReST-Net: Diverse activation modules and parallel subnets-based CNN for spatial image steganalysis," *IEEE Signal Process. Lett.*, vol. 25, no. 5, pp. 650–654, May 2018.

[45] Y. Jia *et al.*, "Caffe: Convolutional architecture for fast feature embedding," in *Proc. ACM Int. Conf. Multimedia*, Orlando, FL, USA, 2014, pp. 675–678.

Xin Liao (M'16) received the B.E. and Ph.D. degrees in information security from the Beijing University of Posts and Telecommunications, Beijing, China, in 2007 and 2012, respectively. In 2012, he joined Hunan University, Changsha, China, where he is currently an Associate Professor. He was a Visiting Scholar with the University of Maryland at College Park, College Park, MD, USA, from 2016 to 2017. His current research interests include image steganography, watermarking, and multimedia forensics.

Yingbo Yu received the B.E. degree in computer science from the Hunan Institute of Technology, Hengyang, China, in 2015, and the M.S. degree in computer science from Hunan University, Changsha, China, in 2018. His current research interests include image steganography and watermarking.

Bin Li (S'07–M'09–SM'17) 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. In 2009, he joined Shenzhen University, Shenzhen, China, where he is currently an Associate Professor. He is currently the Director of the Shenzhen Key Laboratory of Media Security. He is also a Scholar with the Peng Cheng Laboratory. His current research interests include image processing, multimedia forensics, and pattern recognition. He is currently a member of the IEEE Information Forensic and Security Technical Committee.



Zhongpeng Li received the B.E. degree in electronic information engineering and the M.S. degree in information and communication engineering from Shenzhen University, Shenzhen, China, in 2013 and 2017, respectively. His current research interests include image processing and machine learning.

Zheng Qin received the Ph.D. degree in computer software and theory from Chongqing University, 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 as the Vice Director of the Hunan Engineering Laboratory of Authentication and Data Security. His main interests are network and data security, privacy, data analytics and applications, machine learning, and applied cryptography.