IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 15, 2018, accepted July 17, 2018, date of publication July 23, 2018, date of current version August 15, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2858858

An Improved Image Camouflage Technique Using Color Difference Channel Transformation and Optimal Prediction-Error Expansion

HENG YAO[1,2], (Member, IEEE), XIAOKAI LIU[1], ZHENJUN TANG[2], (Member, IEEE), YU-CHEN HU[3], (Senior Member, IEEE), AND CHUAN QIN[1], (Member, IEEE)

[1]School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China
[2]Guangxi Key Lab of Multi-source Information Mining & Security, Guangxi Normal University, Guilin 541004, China
[3]Department of Computer Science and Information Management, Providence University, Taichung 43301, Taiwan

Corresponding author: Chuan Qin (qin@usst.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61702332, Grant 61672354, Grant 61562007, in part by the Research Fund of the Guangxi Key Lab of Multi-source Information Mining & Security under Grant MIMS16-03, and in part by the Guangxi Natural Science Foundation under Grant 2017GXNSFAA198222.

ABSTRACT With the development of the ability to crack encrypted images, conventional image encryption techniques are no longer safe enough. Disguising a to-be-encrypted image into another visually-different image that is similar to the prepared target image is a solution that can be used to transmit an image securely. Inspired by the existing reversible image transformation technique, in this paper, we propose an improved method for camouflaging images that further decrease the distortion between the final camouflaged image and the target image. First, the G channel of the secret image is transformed and further refined to create a tentative camouflaged G channel with the reference of the G channel of the target image. Then, the color difference channels of the secret image are transformed with the reference of subtraction of the R channel (or B channel) and the tentatively camouflaged G channel. After shifting the color difference channels back to the R channel (or B channel), the sub-blocks are refined by a 16-candidate-pattern optimization strategy to generate the tentative camouflaged R channel (or B channel). After the combination of the RGB channels to generate the tentative camouflaged image, the final camouflaged version is generated by embedding all of the auxiliary information, which is collected for lossless recovery of the secret image, into the tentative image in a reversible manner. The experimental results demonstrated the efficacy of the proposed method, and our average gain in the color image peak signal-to-noise ratio (CPSNR) was more than 0.35 dB, whereas the state-of-the-art method is around 32.28 dB.

INDEX TERMS Image camouflage, reversible image transformation, color difference channel, image encryption, reversible data hiding.

I. INTRODUCTION

With the development of Internet technology, the sharing and dissemination of multimedia information has quite easy to do. Due to the wide range in the types of information and the surge in the volume of data, the risk of information leakage and the risk of malicious alteration of content have been increased significantly. Thus, if inadequate attention is paid to protecting information, personal privacy, business developments, and even national security will be seriously threatened. Clearly, the importance of the security of information is increasing with the development of information storage and transmission.

Now, we turn to the issue of transmitting secret images. Due to their vivid and intuitive features, digital images are used extensively every day. In many circumstances, it is important to encrypt the digital images to ensure their confidentiality. For instance, both the private photos that are uploaded to the cloud and confidential military images require reliable encryption techniques to prevent potential attackers from gaining access to important personal or military information. Numerous conventional encryption techniques can be used to encrypt images, such as the RSA cryptosystem [1], the AES cryptosystem [2], and the homomorphic Paillier encryption algorithm [3]. However, the

TABLE 1. Categories of the existing methods.

Categories	Methods	Size ratio of secret image and target image	Recovery of secret image	Consideration of robustness	Processing domain
#1 Watermark-like frequency domain methods	[12], [13]	1:4	Reversible (lossless)	Yes	Frequency
#2 Nearly reversible image transformation methods	[14], [15]	1:1	Near reversible (slight distortion)	No	Spatial
#3 Reversible image transformation methods	[16], [17], [18], [19]	1:1	Reversible (lossless)	No	Spatial

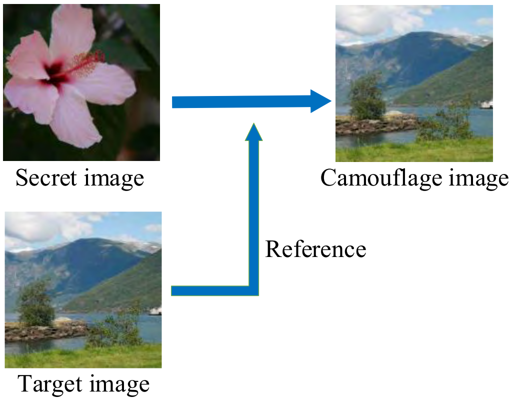


FIGURE 1. Schematic diagram of image camouflage.

large volume of image data and the strong correlation of neighboring pixels limit the efficiency of traditional encryption techniques. In recent years, many encryption algorithms have been proposed specifically for the encryption of images, such as chaotic system-based methods [4]–[6], the wave perturbations-based method [7], the fractional Fourier transform-based method [8], the discrete wavelet transform-based method [9], the DNA encoding-based method [10], and the compressive sensing-based method [11]. Note that all of the image encryption methods mentioned above essentially are based on specific mathematical transformation rules, and the aim of image encryption is to transform the original, meaningful plaintext images into out-of-order, meaningless images. Without knowing the key and transformation rules, it is difficult for person who receives the meaningless image to discern the content of the original image. However, there is a fatal flaw associated with image encryption, i.e., encrypted, garbled images obviously indicate that the original image probably contained some important information, thereby attracting the attention of attackers. Thus, the conventional image encryption no longer provides adequate protection, and the image camouflage technique was developed to overcome this shortcoming. Different from image encryption, image camouflage transforms the original plaintext image into another meaningful plaintext image by a specific rule, which reduces the attackers' suspicion and ensures the security of the original image. Fig. 1 shows a schematic diagram of image camouflage in which some transformation rules or frequency substitution rules have been used to camouflage the secret image so that is looks like the target image. To date, various image camouflage algorithms have been proposed [12]–[19]. According to the quality of the recovered secret image and the size requirements of the secret image and the target image, the existing methods can be grouped roughly into the three categories shown in Table 1. Specifically, for the first category (i.e., watermark-like frequency domain methods), motivated by the data hiding technique [20], Bao and Zhou [12] proposed an algorithm to directly encrypt an original image into a visually-meaningful encrypted image based on the discrete wavelet transform (DWT) and a substitution strategy in the DWT sub-bands. In order to minimize the distortion of the camouflage image, Kanso and Ghebleh [13] improved [12] by embedding the secret image into the sub-bands of the host image that were decomposed via the two-dimensional lifting wavelet transform. However, since the target image is four times the size of the secret image, this approach is not feasible in many applications.

For the second category (i.e., nearly reversible image transformation methods), Lama *et al.* [14] proposed an image transformation method based on the color-transfer concept [21]. The basis of their method was to decompose the covariance of the color space of the secret image and the target image using the singular value decomposition (SVD) algorithm and then to disguise the secret image as a stego image by geometrical transformation. Inspired by another color-transfer method [22], Lee and Tsai [15] created a camouflage image by dividing the secret image into fragments and transforming their color characteristics to be the color characteristics of the matching tiles of the target image. However, this did not provide an authentic lossless recovery for this category of methods, and, in some circumstances, e.g., medical images and military images, the reversibility of the secret image is a critical requirement. Thus, the reversible image transformation technique was developed to overcome this issue.

For the last category (i.e., reversible image transformation methods), Lai and Tsai [16] proposed a method to create secret-fragment-visible mosaic images as camouflage images. In [16], the secret image was divided into tiny blocks before a target image with a similar, one-dimensional color scale feature was selected from a database. Each tile of the secret image, which was analogous to the tile of target image, was then assembled into a camouflage image.

Zhang *et al.* [17] proposed a novel framework to achieve reversible data hiding in encrypted images (RDH-EI); in their framework, the visually-meaningful stego image is used as the encrypted image of RDH-EI. During the reversible image transformation method presented in [17], the original image and the target image are classified into fixed quantiles according to the standard deviation of the image blocks, and, then, the blocks of the original image are paired with the blocks of the target image, which makes lossless recovery of the secret image possible and reduces the amount of auxiliary information required for restoration. Recently, in [18], the K-means clustering algorithm was used to improve the classification of image blocks that was used in [17] in order to achieve adaptive classification of different original images and improve the visual quality of the camouflage images. More details of the content of reference [18] will be interpreted in Section II of previous arts. In [19], Hou *et al.* improved the visual quality of camouflage image by exploring the correlations among color channels and reducing the amount of the accessorial information for secret image recovery.

In this paper, we focused on improving the reversible image camouflage method [18] by using color difference channel transformation and the optimal prediction-error expansion (PEE) parameter selection strategy. First, The G channel of the secret image is transformed and further refined to a tentative camouflage G channel with the reference of the G channel of the target image. Next, the color difference channels (i.e., (R − G) or (B − G) channels) of the secret image are transformed with the reference of the difference between the R channel (or B channel) and the tentative camouflage G channel. After shifting the color difference channels back to the R channel (or B channel), the sub-blocks are refined by a 16-candidate pattern optimization to generate a tentative camouflage R channel (or B channel). Then, the RGB channels are combined as a tentative camouflage image, and the final camouflage version is generated by embedding the entire auxiliary information, which is for the recovery of the secret image, into the tentative image in a reversible manner.

The innovations of this paper are specified below:

1) Apply the algorithm on the G, (R − G), and (B − G) channels of a color image to replace the separation of the RGB channels. In this way, the concentrations of the standard deviation distribution of the sub-blocks in both the secret and target images are improved, and the correlation of the RGB color space is used effectively in our method. Although there are many existing color space transformation methods to convert RGB channels to opponent-color channels, such as YUV and YCbCr, the decimal fractions are inevitable during the space transformation. In this paper, to overcome this issue, we exploit an effective image transformation method based on the new-designed color difference channels.
2) For each channel, after the image transformation, the transformed sub-blocks are converted to 16 candidate patterns, and the optimal pattern is sought by applying a minimum error criterion. It has good effect on reducing the abrupt block effect to bring in more candidate patterns.
3) During the last phase, the auxiliary information is embedded into the tentative camouflage image with an improved RDH manner, i.e., the target image is involved in the redesigned strategy for selecting parameters. The new proposed optimal parameters selection strategy is not merely limited to some specific PEE based reversible data hiding (RDH) methods.

The rest of the paper is organized as follows. Section II briefly reviews the previous arts. Section III presents the potential improvements to the existing reversible image camouflage methods. Section IV provides a detailed description of the improved algorithms. Section V presents and discusses the experimental results for the proposed method. Section VI discusses the concern why do not apply the classical opponent-color space to the proposed method. Section VII concludes the paper.

II. PREVIOUS ARTS

As introduced in the previous section, in the conventional image camouflage methods [14], [15], the secret image restored from the camouflage image is nearly reversible whereas previous methods actually do not have the advantage of reversibility. Recently, the authors of references [17] and [18] proposed a completely reversible image transformation technique, i.e., a technique that transforms a secret image to a target image that has the same size and losslessly restores the original secret image without any external information during the recovery phase. Note that the method presented in [18] was designed for image camouflage, while the work in [17] was for the application of reversible data hiding in the encrypted domain in which reversible transformation of the image is a significant intermediate phase. Since the application in our paper is for image camouflage, as was the case in [18], and, according to our simulation the method in [18] performs better for image camouflage than the method in [17], we mainly regard [18] as a representative of the state-of-the-art approach in this section. An entire framework for reversible image transformation roughly includes the following three steps, i.e., 1) transforming the image, 2) refining the sub-blocks, and 3) embedding the auxiliary information. In this section, we briefly review the image camouflage method [18], and since the image transformation proposed in [18] was conducted independently on RGB color channels, we use a single channel as an example. Fig. 2 shows the flow diagram of image camouflage in a single channel as presented in [18].

A. IMAGE TRANSFORMATION

Assume that I and J are the secret image and target image, respectively, and that they are the same size, i.e., $H \times V$. First, both I and J are divided separately into non-overlapping sub-blocks with the size of $S \times S$, so the total number of sub-blocks in I and J is $T = (H \times V) / (S \times S)$. Then, the mean value

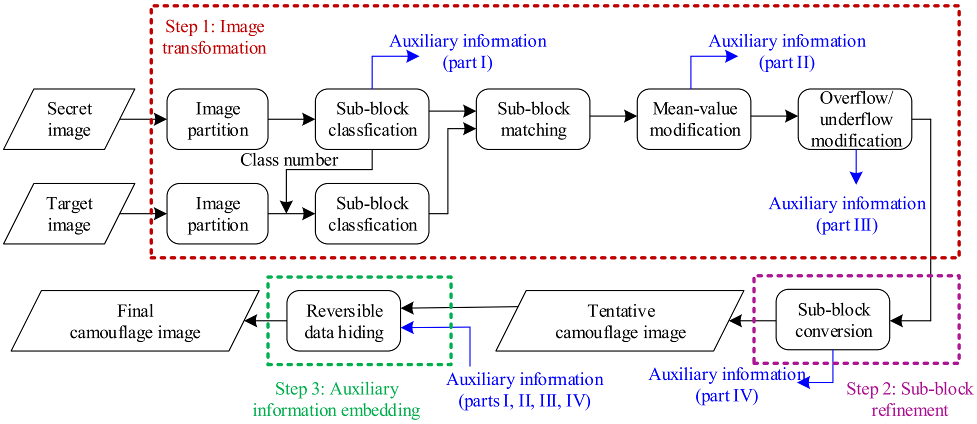

Step 1: Image transformation
Auxiliary information (part I)
Auxiliary information (part II)
Secret image
Image partition
Sub-block classfication
Sub-block matching
Mean-value modification
Overflow/ underflow modification
Class number
Target image
Image partition
Sub-block classfication
Auxiliary information (part III)
Final camouflage image
Reversible data hiding
Tentative camouflage image
Sub-block conversion
Step 3: Auxiliary information embedding
Auxiliary information (parts I, II, III, IV)
Auxiliary information (part IV)
Step 2: Sub-block refinement

FIGURE 2. **Flow diagram of the image camouflage algorithm on a single channel (proposed by Hou *et al.* [18]).**

and standard deviation (SD) of each sub-block in I and J can be computed, respectively, as:

$$\begin{cases} \mu_i = \dfrac{\sum_{k=1}^{S\times S} I_k^i}{S\times S}, \sigma_i = \sqrt{\dfrac{\sum_{k=1}^{S\times S}\left(I_k^i-\mu_i\right)^2}{S\times S}}, \\ \qquad\qquad\qquad\qquad i=1,2,\ldots,T \\ \mu_j^* = \dfrac{\sum_{k=1}^{S\times S} J_k^j}{S\times S}, \sigma_j^* = \sqrt{\dfrac{\sum_{k=1}^{S\times S}\left(J_k^j-\mu_j^*\right)^2}{S\times S}}, \\ \qquad\qquad\qquad\qquad j=1,2,\ldots,T \end{cases} \tag{1}$$

where μ_i and σ_i are the mean value and SD of the i^{th} sub-block of I, respectively, and I_k^i is the k^{th} pixel in the i^{th} sub-block of I. The terms μ_j^* and σ_j^* are the mean value and SD of the j^{th} sub-block of J, and J_k^j is the k^{th} pixel in the j^{th} sub-block of J.

After the image is partitioned, the next step is to rearrange the sub-blocks in I according to a sub-block matching strategy. First, all sub-blocks in I are grouped into K classes according to their corresponding SDs using the K-means clustering method and the number of pixels in each class is recorded. Then, all of the sub-blocks of J are separated into K classes according to their corresponding SDs, but note that the number of pixels in each class of J is mandatorily in accord with that of I, which was recorded in advance. Thus, each of the sub-blocks from I and J can be one-to-one matched following a fixed raster-scanning order (i.e., from left to right and from top to bottom). By this block matching operation, the sub-blocks in I can be rearranged to the new positions in accordance with the corresponding matched sub-blocks in J. To restore the order of the secret sub-blocks, the index table of each sub-block of I is recorded and regarded as the first part of the auxiliary information. Fig. 3 shows a simplified example of sub-block classification and matching, where both S and K are equal to 3.

Note that the directly rearranged sub-blocks of I are visually different from the corresponding matched sub-blocks of J. To achieve the aim of image camouflage, all pixels in each secret sub-block are modified by subtracting the difference between the mean value of the current sub-block and that of its corresponding matched target sub-block. If we assume that the i^{th} sub-block in I is matched with the j^{th} sub-block in J, each pixel, I_k^i, is modified to:

$$I_k^{i\prime} = I_k^i - \boldsymbol{Q}_{\boldsymbol{\lambda}}\left(\Delta\mu\right) \tag{2}$$

where $I_k^{i\prime}$ is the modified value of I_k^i, $\Delta\mu = \mu_i - \mu_j^*$, and function $\boldsymbol{Q}_{\boldsymbol{\lambda}}$ (•) indicates the quantization operation with the quantization step λ to reduce the amount of information that must be recorded in order to recover the secret image. The quantization coefficients are recorded as the second part of the auxiliary information.

It is worth noticing that for better visual quality, it is better to save the un-quantized mean difference $\Delta\mu$ between the secret sub-block and its corresponding target sub-block. However, it takes a lot of storage space to save the decimal $\Delta\mu$. Hence, to make a trade-off between visual quality and auxiliary information amount, we use (2) to transform the original pixel I_k^i to the camouflage pixel which is visually similar to its corresponding matched target pixel. As its reverse process, the recovery process can be conducted as $I_k^i = I_k^{i\prime} + \boldsymbol{Q}_{\boldsymbol{\lambda}}\left(\Delta\mu\right)$. Since the quantized mean value has been transmitted as the second part of the auxiliary information, the value of $\boldsymbol{Q}_{\boldsymbol{\lambda}}\left(\Delta\mu\right)$ can be losslessly recovered by the RDH extraction method proposed in Section III.C. In a word, the quantization process in (2) merely decrease the visual similarity to the target image, and do not change the one-to-one mapping between each pair of secret and target sub-blocks. Therefore, for the proposed method, it has no effect on the lossless recovery of original secret image.

Of course, the overflow/underflow issue is inevitable, so the overflow/underflow residuals are recorded as the third part of the auxiliary information.

B. SUB-BLOCK REFINEMENT

To further narrow the gap between the camouflage image and the target image, most existing image camouflage methods [15], [17], [18] used a sub-block isometric conversion strategy. When the elements of each sub-block have been

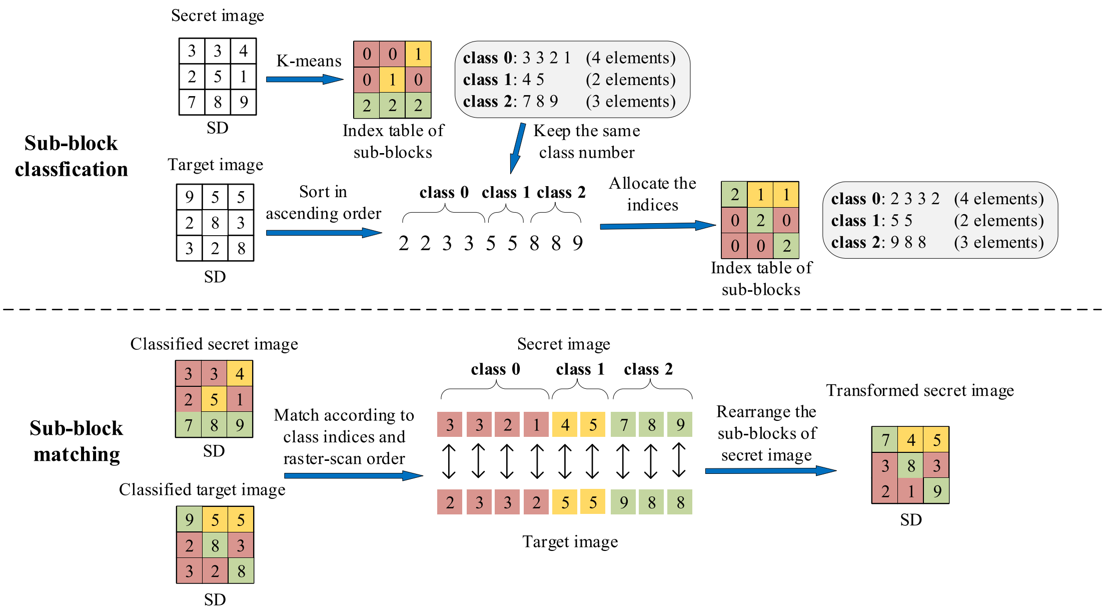


FIGURE 3. Simplified example of sub-block classification and matching.

modified according to (2), the sub-blocks are rotated at angles of 0, 90, 180, and 270 degrees, respectively, to generate four candidate isometric sub-blocks. Then, the optimal isometric sub-block is selected with the criterion that the minimum distortion between the camouflage sub-block and the target sub-block corresponds to the optimal rotation angle; also the optimal rotation angle for each sub-block is recoded as the fourth part of auxiliary information. To this point, the tentative camouflage image and auxiliary information for restoring the secret image have been generated.

C. EMBEDDING THE AUXILIARY INFORMATION

The last procedure for reversible image camouflage is embedding the auxiliary information by using the existing RDH technique. It has been suggested that the PEE method proposed by Sachnev *et al.* [23] be used to implement this embedding. In this step, note that the embedding strategy is not tied to a particular RDH method, and, actually, any high capacity RDH method can be used, such as [24]–[26]. Also, some color image RDH methods (e.g., [27], [28]) also can be used to decrease the distortion further during the phase of embedding the auxiliary information. In this paper, to facilitate the description, we take [23] as an example. Auxiliary information (AI) and tentative camouflage are regarded as the message and the cover image, respectively, and the image that is eventually marked in the PEE framework corresponds to the final camouflage image in the entire reversible image camouflage phase.

III. IMPROVEMENTS TO THE EXISTING METHODS

In this section, we elaborate on our improvements to the state-of-the-art reversible image transformation method [18] from the following three aspects.

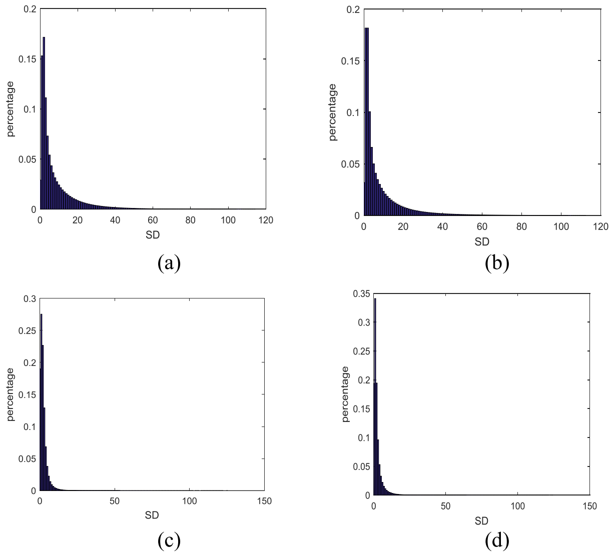


FIGURE 4. The comparing distribution of the average SDs of 4×4 blocks from 1000 test images downloaded from database [29]. (a) Distribution of the average SDs from R channel. (b) Distribution of the average SDs from B channel. (c) Distribution of the average SDs from (R − G) channel. (d) Distribution of the average SDs from (B − G) channel.

A. COLOR DIFFERENCE CHANNEL TRANSFORMATION

For image transformation, in principle, to perceive an optimal visual quality, all sub-blocks should be one-to-one exactly matched according to a SD value sorting with an ascending order. However, in doing so, if the sorting had been executed, the mapping indices would be saved as extra auxiliary information to recover the original secret image. To make a trade-off, the proposed method use K-means clustering strategy to separate all sub-blocks into different classifications such

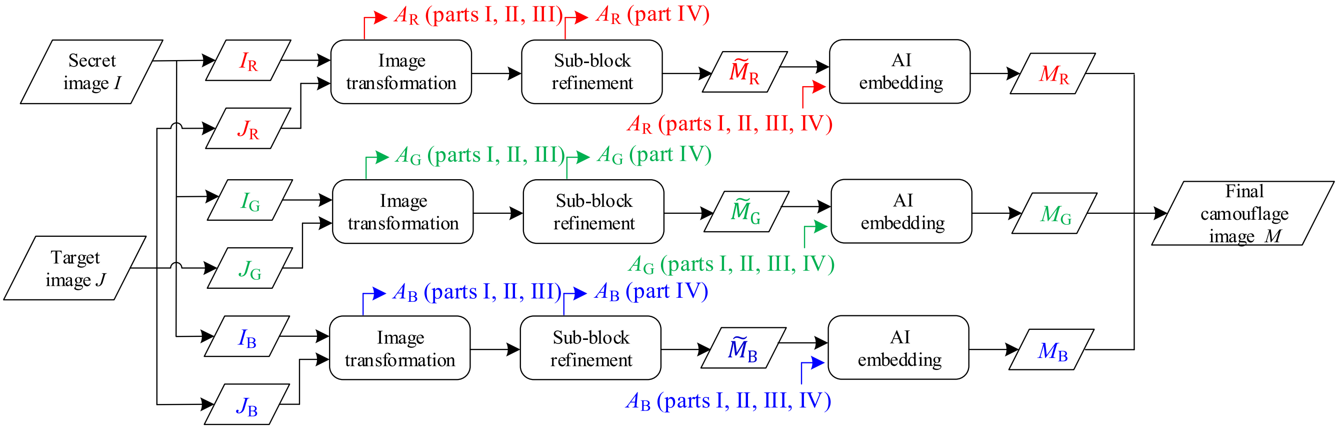


FIGURE 5. Flow chart of image camouflage conducted on independent channels proposed by Hou *et al.* [18].

that each classification has the similar SD properties.For the sub-blocks belonging to each classification, we no longer distinguish the size of these values, i.e., the sub-blocks are roughly matched by a raster-scanning order. In this way, the accuracy of K-means classification is crucial to the final matching result. As indicated in [18], the image transformation is conducted independently on the RGB channels, and the efficacy of transformation is based on the circumstance that the SD values of most sub-blocks concentrate in a small range close to zero, and the frequency decreases quickly as the value of SD increases. In other words, the concentrations of the SD values of the sub-blocks are critical for the transformation. To further improve this type of concentration, we analyzed the distribution of SDs of 4×4 sub-blocks on 1000 collected images, all of which were downloaded from the Boss-Base image database [29] on independent color channels and color difference channels, respectively. Fig. 4 shows the results of the comparison, i.e., for the analysis of the color differences of the channels, the G channel components are subtracted from the R channel and the B channel, respectively, and they are denoted as the (R − G) channel and the (B − G) channel, respectively. For the independent color channel, the R channel and B channel are selected. As shown in Figure 4. The SD distributions of (R − G) and (B − G) channels are more concentrated and steeper than those of independent R and B channels. This discrepancy was probably caused by the strong correlation between color channels. According to the characteristics of K-means classification, the more concentrated the distribution of variable features, the better the effect of adaptive clustering, which makes the matching between secret sub-blocks and target sub-blocks more accurately.

In general, human eyes are more sensitive to green than red and blue. In this paper, on the premise of ensuring the reversibility, the algorithm addresses the G channel, the (R − G) channel, and the (B − G) channel instead of using the RGB channel independently for image transformation, so we are able to take advantage of the correlation of the RGB components of the color image. During the phase in which the secret image is recovered, the G channel image is recovered first, and then the (R − G) (or the (B − G)) channel is recovered. For ease of comprehension, Figs. 5 and 6 show the flow charts of the previous image camouflage strategy of using the independent color channel and the proposed strategy of image camouflage using the color difference channel, respectively, where I, J, and M are supposed to be the secret image, the target image, and the final camouflage image, respectively, and their RGB channels are denoted as $\{I_R, I_G, I_B\}$, $\{J_R, J_G, J_B\}$, and $\{M_R, M_G, M_B\}$, respectively. In addition, Figs. 5 and 6, the RGB channels of auxiliary information are denoted as A_R, A_G, and A_B, respectively, and the tentative camouflage image and its corresponding RGB components are denoted as $\widetilde{M}$ and $\left\{\widetilde{M}_R, \widetilde{M}_G, \widetilde{M}_B\right\}$, respectively. Fig. 6 shows that, by using the color difference channel transformation, the G channel is transformed first, and, then, the (R − G) (or the (B − G)) channel is transformed by means of the tentative camouflage G channel component that was generated. There are two important points we should mark here, i.e., 1) the process of image transformation can be treated as a function with double-ended inputs, as shown in Fig. 7, and the output depends only on the corresponding inputs without other parameters being involved. In other words, the detailed processes for image transformation are exactly the same except the inputs are different. 2) Due to the absence of a target image in the secret image recovery phase, we cannot directly use $(J_R - J_G)$ (or $(J_B - J_G)$) as the target image; instead, we use $(J_R - \widetilde{M}_G)$ (or $(J_B - \widetilde{M}_G)$) as a substitute. Table 2 lists the three different input combinations in the previous strategy and in our designed strategy.

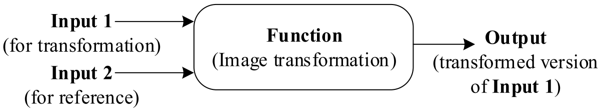


FIGURE 7. Double-ended inputs function model for image transformation.

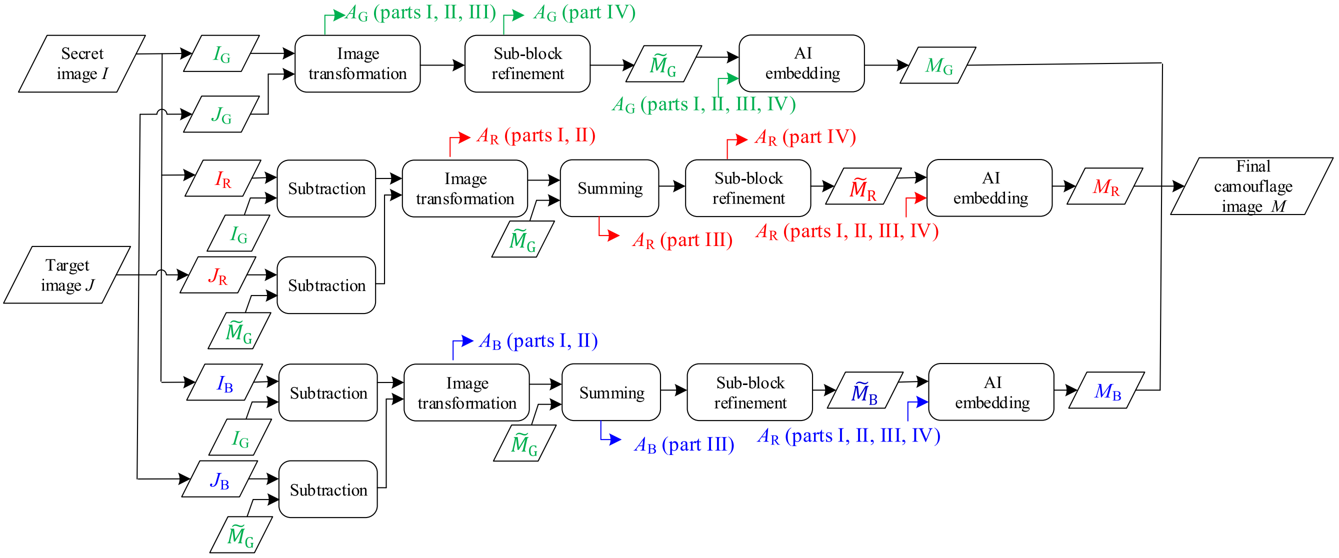


FIGURE 6. Flow chart of image camouflage conducted on G channel and color difference channels.

TABLE 2. Three different combinations of double-ended inputs adopted in previous and the proposed method.

	Previous strategy adopted in [18]		Proposed strategy	
channel	**Input 1**	**Input 2**	**Input 1**	**Input 2**
G channel	I_G	J_G	I_G	J_G
R channel	I_R	J_R	$I_R - I_G$	$J_R - \widetilde{M}_G$
B channel	I_B	J_B	$I_B - I_G$	$J_B - \widetilde{M}_G$

Next, we investigated the detailed operation in the function of image transformation. As shown in Fig. 3 and discussed in Section II.A, the sub-blocks in I_G (or $(I_R - I_G)$, $(I_B - I_G)$) can be rearranged according to an SD-value based clustering. Then, all the pixel values in each sub-block of I_G (or $(I_R - I_G)$, $(I_B - I_G)$) are shifted by (2). Note that there is some probability that some shifted pixel values could result in some issues of overflow/underflow, i.e., $I_k^{i'} > 255$ or $I_k^{i'} < 0$ in the case of the G channel, and $I_k^{i'} > 255$ or $I_k^{i'} < -255$ in the case of the (R – G) (or (B – G)) channel. Thus, following [18], a modification on Eq. (2) was processed as

$$I_k^{i'} = I_k^i - \boldsymbol{Q}_\lambda\left(\Delta\mu'\right) \tag{3}$$

where,

$$\Delta\mu' = \begin{cases} \boldsymbol{max}\left(\left[\boldsymbol{max}\left(I_k^i\right) - \ell_H\right], \Delta\mu\right), & \text{if } \Delta\mu < 0 \\ \boldsymbol{min}\left(\left[\boldsymbol{min}\left(I_k^i\right) - \ell_L\right], \Delta\mu\right), & \text{if } \Delta\mu \geq 0 \end{cases}, \quad k = 1, 2, \ldots, S \times S \tag{4}$$

where $\boldsymbol{max}(\cdot)$ and $\boldsymbol{min}(\cdot)$ indicate the operation to seek the maximum and minimum values from the inputs, respectively, and ℓ_H and ℓ_L stand for the permitted upper bound and lower bound, respectively, to avoid overflow/underflow; specifically, $\ell_H = 255$ and $\ell_L = 0$ for the R channel, and $\ell_H = 255$ and $\ell_L = -255$ for the (R – G) (or (B – G)) channel. In addition, to further reduce the quantization coefficients, a specially designed quantization can be conducted, i.e.,:

$$\boldsymbol{Q}_\lambda\left(\Delta\mu'\right) = \begin{cases} \lambda \times \boldsymbol{round}\left(\dfrac{\Delta\mu'}{\lambda}\right), & \text{if } \Delta\mu' \geq 0 \\ \lambda \times \boldsymbol{floor}\left(\dfrac{\Delta\mu'}{\lambda}\right) + \lambda/2, & \text{if } \Delta\mu' < 0 \end{cases} \tag{5}$$

where the functions $\boldsymbol{round}(\cdot)$ and $\boldsymbol{floor}(\cdot)$ represent an ordinary rounding operation and a rounding operation towards minus infinity, respectively, and λ is suggested to be set at 8 in both [18] and the proposed method. Therefore, we only need to record the value of $2\left|\Delta\mu'\right|/\lambda$ as the quantized mean difference coefficients for losslessly restoring $\Delta\mu'$ in the secret image recovery phase.

Although the overflow/underflow issue was considered in (4), the possibility still exists that $I_k^{i'}$ will be beyond the allowable range due to the process of quantization, thus, the shifted value of $I_k^{i'}$ is then modified to ℓ_H or ℓ_L if overflow or underflow occurs. In order to restore the unmodified $I_k^{i'}$, the residual r for each overflow/underflow pixel is recorded as:

$$r = \begin{cases} I_k^{i'} - \ell_H, & \text{if } I_k^{i'} \geq \ell_H \\ \ell_L - I_k^{i'}, & \text{if } I_k^{i'} \leq \ell_L \end{cases} \tag{6}$$

For the entire channel, we collected all of the overflow/underflow residuals as a part of AI. By this point, we have introduced the process of image transformation.

During the transformation of the (R – G) (or (B – G)) channel, since the subsequent step after image transformation is the summing by the G channel, and this step also bring the issue of overflow/underflow. Therefore, in our practical execution, we changed the order of two steps of overflow/underflow modification and summing by $\widetilde{M}_G$, and,

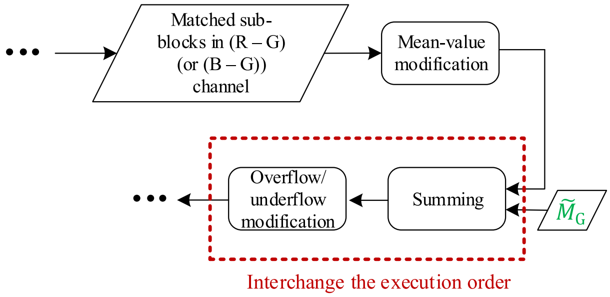

Matched sub-blocks in (R – G) (or (B – G)) channel
Mean-value modification
Overflow/ underflow modification
Summing
$\widetilde{M}_G$
Interchange the execution order

FIGURE 8. Practical order of the steps in the proposed method during the process of (R – G) (or (B – G)) channel transformation and summing.

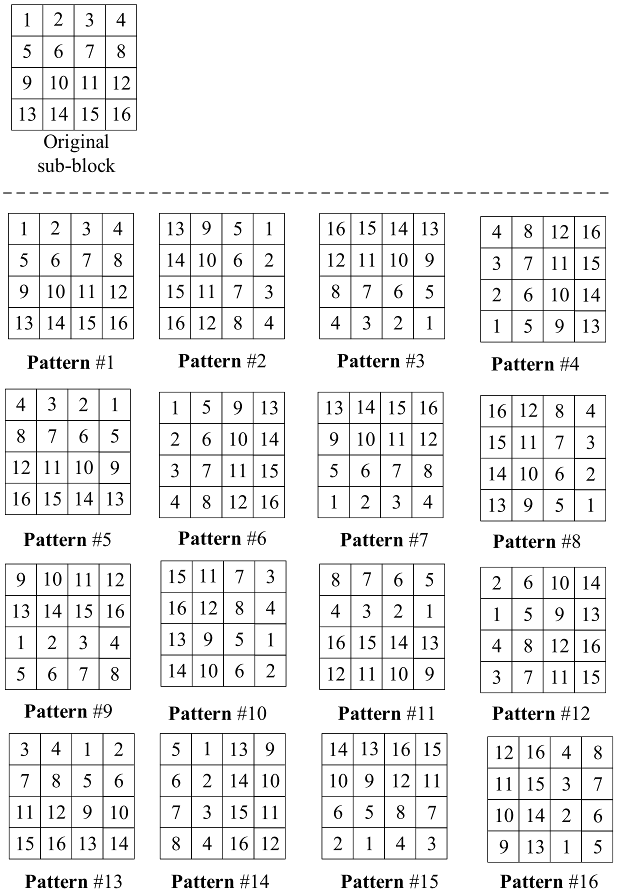
due to this change, we only need to record residuals once. Fig. 8 shows the detailed procedures that were used during the process of (R – G) (or (B – G)) channel transformation and summing.

B. FURTHER REFINEMENT OF BLOCK CONVERSION OPERATION

As indicated in most image transformation methods [15], [17], [18], during the sub-block refinement process, each sub-block is rotated by 0, 90, 180, and 270 degrees, and, then, an optimal rotation angle is selected according to the criterion that the conversed sub-block and its corresponding target block have the minimum MSE, i.e., the selected rotated sub-block is most similar to the target block. Based on the four different degree conversions, a 2-bit AI is needed to preserve the information related to the selected degree. Based on our experiments on many images, there are more potential ways to improve the similarity between the converted sub-blocks and their corresponding target sub-blocks. Note that more possible conversions inevitably require that more bits be added in AI, so we must make a trade-off between the number of possible conversions and the amount of auxiliary information. According to our experiments, 16 different possible conversion patterns can be designed, as shown in Fig. 9. Specifically, Patterns #1 – 4 correspond to the clockwise rotation of the original sub-block at 0, 90, 180, and 270 degrees, respectively. Patterns #5 – 8 are the horizontal flip versions of Patterns #1 – 4, respectively, and Patterns #9 – 12 and Patterns #13 – 16 are the vertical and horizontal cyclic shift versions of Patterns #1 – 4, respectively. Due to the 16 patterns, we arranged four bits to represent the selection patterns. The demonstration of the advantage of the proposed sub-block refinement strategy, i.e., the use of 16 patterns to substitute for the original four patterns, is presented in Section V.

C. NEW OPTIMIZATION TARGET FOR PEE BASED RDH METHOD

The conventional PEE-based RDH method was used in [18] to embed AI into the tentative camouflage image, $\widetilde{M}_G$, in a reversible manner. Considering the circumstance in our application, the cover image is the tentative camouflage image, and the to-be-embedded message is auxiliary information, so the goal of the conventional RDH method is to minimize the distortion between the cover image and the marked image, i.e., the final camouflage image. However, note that the goal of our application is to minimize the distortion between the original target image and the marked image, so it certainly results in a new optimization problem. Fig. 10 compares the conventional RDH target and the new target in our application. Although the target image J will not appear in the secret image recovery phase, we can seek the optimal parameters in the data hiding phase. The proposed optimization for the PEE-based RDH method is presented below.



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Original sub-block

Pattern #1

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Pattern #2

13	9	5	1
14	10	6	2
15	11	7	3
16	12	8	4

Pattern #3

16	15	14	13
12	11	10	9
8	7	6	5
4	3	2	1

Pattern #4

4	8	12	16
3	7	11	15
2	6	10	14
1	5	9	13

Pattern #5

4	3	2	1
8	7	6	5
12	11	10	9
16	15	14	13

Pattern #6

1	5	9	13
2	6	10	14
3	7	11	15
4	8	12	16

Pattern #7

13	14	15	16
9	10	11	12
5	6	7	8
1	2	3	4

Pattern #8

16	12	8	4
15	11	7	3
14	10	6	2
13	9	5	1

Pattern #9

9	10	11	12
13	14	15	16
1	2	3	4
5	6	7	8

Pattern #10

15	11	7	3
16	12	8	4
13	9	5	1
14	10	6	2

Pattern #11

8	7	6	5
4	3	2	1
16	15	14	13
12	11	10	9

Pattern #12

2	6	10	14
1	5	9	13
4	8	12	16
3	7	11	15

Pattern #13

3	4	1	2
7	8	5	6
11	12	9	10
15	16	13	14

Pattern #14

5	1	13	9
6	2	14	10
7	3	15	11
8	4	16	12

Pattern #15

14	13	16	15
10	9	12	11
6	5	8	7
2	1	4	3

Pattern #16

12	16	4	8
11	15	3	7
10	14	2	6
9	13	1	5

FIGURE 9. Schematic diagram of the proposed 16 candidate patterns for sub-block conversion.

The RDH algorithm can be conducted on the RGB channels independently, and, here, we take the G channel as an example, and the R and B channels can be processed in the same manner. First, all pixels in $\widetilde{M}_G$ are allocated into two types, i.e., dotted pixels and crossed pixels, as shown in Fig. 11. To increase the embedding capacity, a two-round embedding strategy was conducted during our practical execution, and, during the embedding phase, A_G was first embedded into crossed pixels, and then it was embedded into dotted pixels. In the extraction phase, the auxiliary information was extracted in reverse order.

Taking the embedding of the crossed pixel $\widetilde{M}_G\,(p, q)$ as an example, first, predict $\widetilde{M}_G\,(p, q)$ by averaging its nearest

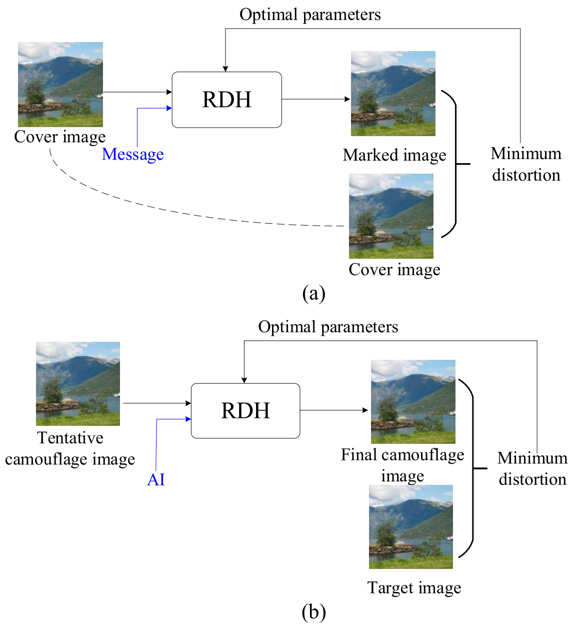


FIGURE 10. The comparison of targets of conventional RDH methods and our new application. (a) A sketch of conventional optimal parameters selection. (b) A sketch of new optimal parameters selection in our method.

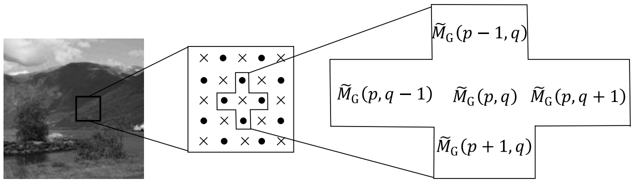


FIGURE 11. The rhombus prediction pattern of $\widetilde{M}_G(p,q)$.

surrounding dotted pixels (i.e., $\widetilde{M}_G(p-1,q)$, $\widetilde{M}_G(p+1,q)$, $\widetilde{M}_G(p,q-1)$, and $\widetilde{M}_G(p,q+1)$) before rounding it towards minus infinity, and denote the rounded prediction value as $\hat{M}_G(p,q)$. Then, calculate the prediction error by $e(p,q) = \widetilde{M}_G(p,q) - \hat{M}_G(p,q)$. Next, the prediction error histogram (PEH), Ψ, is generated by counting the frequencies of prediction errors, and the auxiliary information is embedded through PEH expansion. Specifically, the prediction error $e(p,q)$ is shifted and expanded as:

$$e(p,q) = \begin{cases} 2e(p,q) + \omega_G, & if\ e(p,q) \in [T_n, T_p] \\ e(p,q) + T_p + 1, & if\ e(p,q) > T_p \\ e(p,q) + T_n, & if\ e(p,q) < T_n \end{cases} \qquad (7)$$

where T_p and T_n are integer upper and lower bound parameters, respectively, to make a trade-off between capacity and distortion, and ω_G is the to-be-embedded auxiliary information bit. Note that T_p is set to be greater than or equal to zero, and T_n is less than zero. Here, different from conventional methods, as shown in Fig. 10, the optimal embedding parameters, i.e., T_p, T_n, are sought by a new minimization problem as:

$$\begin{cases} \boldsymbol{Minimize} \sum_{p,q} (M_G(p,q) - J_G(p,q))^2 \\ \boldsymbol{Subject\ to} \sum_{\psi=T_n}^{T_p} \Psi(\psi) \le \ell_{AG}, \\ \qquad\qquad (p,q) \in crossed\ pixels \end{cases} \qquad (8)$$

where $\Psi(\psi)$ corresponds to the cardinal number of prediction error ψ during the generation of PEH, and ℓ_{AG} stands for the length of the first round to-be-embedded, A_G. Through PEH expansion, the message is embedded into the bins of $[T_n, T_p]$. Finally, $\widetilde{M}_G(p,q)$ is modified to the camouflage pixel $M_G(p,q)$ through:

$$M_G(p,q) = e'(p,q) + \widetilde{M}_G(p,q) \qquad (9)$$

In the recovery phase, the auxiliary information bit, ω_G, and the tentative camouflage pixel, $\widetilde{M}_G(p,q)$, can be restored as:

$$\widetilde{M}_G(p,q) = \begin{cases} \boldsymbol{floor}\left(\frac{e'(p,q)}{2}\right) + \hat{M}_G(p,q), & if\ e'(p,q) \in [2T_n, 2T_p+1] \\ e'(p,q) - T_p - 1 + \hat{M}_G(p,q), & if\ e'(p,q) > (2T_p+1) \\ e'(p,q) - T_n + \hat{M}_G(p,q), & if\ e'(p,q) < 2T_n \end{cases} \qquad (10)$$

and

$$\omega_G = e'(p,q)\,\boldsymbol{mod} 2, \quad if\ e'(p,q) \in [2T_n, 2T_p+1] \qquad (11)$$

IV. ALGORITHMS OF THE PROPOSED METHOD

Based on the discussion in Section III, a scheme to produce an improved image camouflage has been presented. To provide a clearer understanding the detailed steps involved, Algorithm 1 lists the detailed procedures of the proposed image camouflage method. Of course, the recovery of the original secret image can be done be reversing the steps in the image camouflage procedures. Fig. 12 shows the flow diagram of the recovery phase for the secret image, and, similarly, Algorithm 2 presents the procedures required to recover the secret image.

V. EXPERIMENTAL RESULTS

In this section, we conduct the proposed method on many secret and target images, and the common quality metrics of root mean square error (RMSE) and color image peak signal to noise ratio (CPSNR) are both used to demonstrate the comparability of the target image and the camouflage image, where the values of RMSE and CPSNR are computed as

$$\begin{cases} RMSE(M,J) = \sqrt{\frac{\sum_{C\in\{R,G,B\}} \sum_{x=1}^{H\times V} (M_C(x) - J_C(x))^2}{3\times H\times V}} \\ CPSNR(M,J) = 10\log_{10} \\ \qquad \times \frac{255^2 \times 3 \times H \times V}{\sum_{C\in\{R,G,B\}} \sum_{x=1}^{H\times V} (M_C(x) - J_C(x))^2} \end{cases} \qquad (12)$$

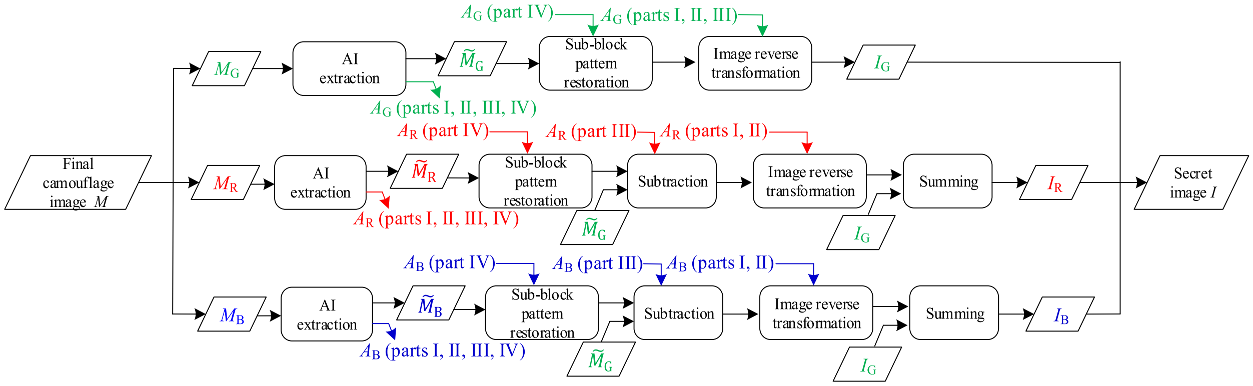


FIGURE 12. Flow diagram of secret image recovery phase.

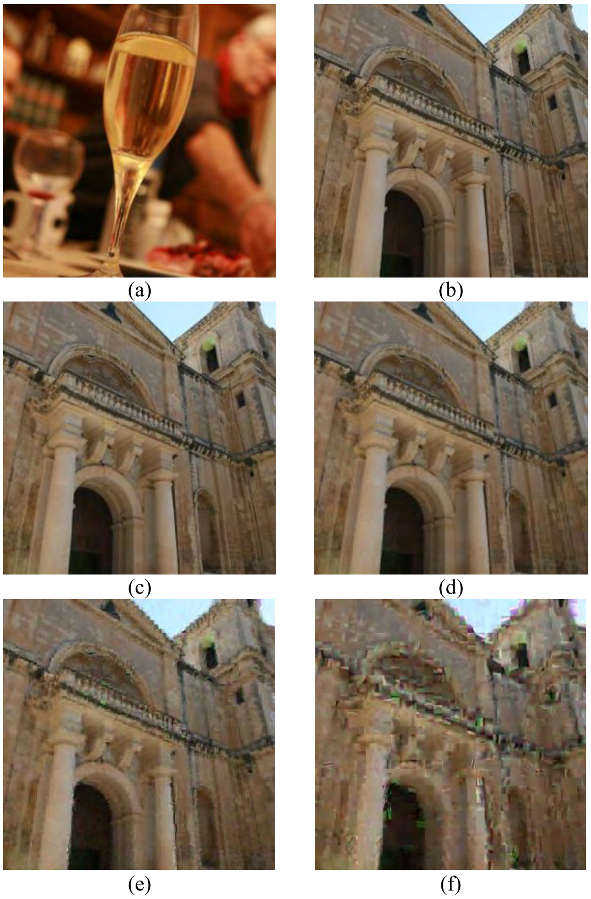


FIGURE 13. (a) Secret image. (b) Target image. (c) Camouflage image by setting 4×4 sub-block. (d) Camouflage image by setting 8×8 sub-block. (e) Camouflage image by setting 16×16 sub-block. (f) Camouflage image by setting 32×32 sub-block.

where all pixels in each channel of both M and J are arranged in a one-dimensional sequence with the lengh of $H \times V$, and $M_C(x)$ and $J_C(x)$ are the x^{th} pixel value in the C channel of M and J, respectively. In addition, we also compared the results with the state-of-the art method to demonstrate the superiority of the proposed method. All test images were downloaded from the Boss-Base image database [29], and all images were resized to the size of 1024×1024. First, we determined the parameters in our algorithm, including the K-means classification number K, the quantification step λ, and sub-block size, S. As indicated in [18], K and λ were suggested to be set at 6 - 10 and 8, respectively. Thus, we set $K = 6$ and $\lambda = 8$ in our experiments. Fig. 13 shows an example of the visual comparison results of the final camouflage images by setting different S values, i.e., 4, 8, 16, and 32 in (c), (d), (e), and (f), respectively. Fig. 13 shows that, with the increase of S, its corresponding blocking artifacts are more noticeable. Moreover, Table 3 lists the CPSNR and amount of AI of Figs. 13 (c) – (f), where Fig. 13 (c) (i.e., $S = 4$) presents the best quality image. Therefore, from Fig. 13 and Table 3, to achieve a satisfactory visual quality, we set $S = 4$ in our experiments.

TABLE 3. The results by setting the different sub-block size parameter.

Figure	S	CPSNR [a] (dB)	Amount of AI (bpp)	CPSNR [b] (dB)
Fig. 13 (c)	4	36.2237	0.6459	35.0234
Fig. 13 (d)	8	33.8430	0.1771	33.6777
Fig. 13 (e)	16	32.1448	0.0620	32.0957
Fig. 13 (f)	32	30.6974	0.0401	30.6753

[a] for tentative camouflage image.
[b] for final camouflage image.

Next, we demonstrate the advantage of the 16 candidate conversion patterns that were used in our sub-block refinement strategy. Fig. 14 shows three examples of the proposed method, and Table 4 lists their corresponding CPSNR and AI values. For comparison, we continued to conduct the experiments in Fig. 14 by using the same proposed method except for different sub-block refinement strategies, as shown in Table 4. Table 4 indicates that, although AI was larger and more patterns had to be considered during the sub-block refinement stage, the final camouflage images still had better image quality.

To evaluate the efficacy of improved RDH method, Table 5 lists their corresponding RMSE and CPSNR values using conventional RDH method and our proposed RDH method. Note that the other settings and strategies in

Algorithm 1 Camouflage Image Generation

```
Input: secret color image $I$, target color image $J$, secret key $\rho$
Output: camouflage image $M$
Stage 1: Tentative camouflage of the G channel image
1) Select G channel of $I$ and $J$, i.e., $I_{\mathrm{G}}$ and $J_{\mathrm{G}}$, and divide them into non-overlapping $S \times S$ sized sub-blocks.
2) Calculate the standard deviation of each of the sub-blocks and define them as secret sub-block SDs and target sub-block SDs.
3) Cluster the secret sub-blocks into $K$ classes according to the secret sub-block SDs alone. Then, cluster the target sub-blocks into the same $K$ classes according to a comprehensive combination of the target sub-block SDs, the number of each clustering class of $I$, and the raster-scanning order. Match the corresponding sub-blocks of $I$ and $J$ in each class, as shown in Fig.3, and record the index table of the secret image.
4) Calculate the difference between the mean values of each of the matched sub-blocks and modify the difference to overcome the overflow/underflow problem according to (4). Quantify the modified mean difference using a preset quantization step, and shift each value of the secret sub-blocks by subtracting the quantized mean difference according to (5). Then, record the quantization parameters.
5) Thoroughly eliminate the overflow/underflow and record the overflow/underflow residuals according to (6).
6) Rearrange the secret sub-blocks according to the index table.
7) Refine the image transformation result using 16-pattern conversion strategy as described in Section III.B, and record the optimal pattern numbers. Generate the tentatively-transformed G channel image, $\widetilde{M}_{\mathrm{G}}$.
Stage 2: Tentative camouflage of the R channel (or B channel) image
8) Select the R channel (or B channel) of $I$ and $J$, i.e., $I_{\mathrm{R}}$ (or $I_{\mathrm{B}}$) and $J_{\mathrm{R}}$ (or $J_{\mathrm{B}}$). Calculate the color difference channel of $I_{\mathrm{R}}$ (or $I_{\mathrm{B}}$) and $I_{\mathrm{G}}$, denoted as $I_{\mathrm{R-G}}$ (or $I_{\mathrm{B-G}}$). Calculate the approximate color difference channel of $J_{\mathrm{R}}$ (or $J_{\mathrm{B}}$) and $\widetilde{M}_{\mathrm{G}}$, denoted as $J_{\mathrm{R-G}}$ (or $J_{\mathrm{B-G}}$).
9) Divide both $I_{\mathrm{R-G}}$ (or $I_{\mathrm{B-G}}$) and $J_{\mathrm{R-G}}$ (or $J_{\mathrm{B-G}}$) into non-overlapping $S \times S$ sized sub-blocks.
10) Repeat Steps 2) - 5), to generate rearranged secret sub-blocks of $I_{\mathrm{R-G}}$ (or $I_{\mathrm{B-G}}$). Restore the R channel (or B channel) by adding $\widetilde{M}_{\mathrm{G}}$.
11) Repeat Steps 6) - 7) to generate the tentatively transformed R channel (or B channel) image $\widetilde{M}_{\mathrm{R}}$ (or $\widetilde{M}_{\mathrm{B}}$).
12) Combine three-color channels (i.e., $\widetilde{M}_{\mathrm{R}}$, $\widetilde{M}_{\mathrm{G}}$ and $\widetilde{M}_{\mathrm{B}}$) to generate the tentative camouflage image $\widetilde{M}$.
```

Algorithm 1 *(Continued.)* Camouflage Image Generation

```
Stage 3: Embedding of the auxiliary information
13) Combine the quantized mean difference coefficients, clustering index tables, sub-block refinement pattern numbers, and overflow/underflow residuals as auxiliary information and then compress and encrypt it using entropy coding and key $\rho$, respectively.
14) Process the embedding in each channel independently, and take $J$ as the reference image to determine the optimal prediction error histogram shifting parameters $T_n$ and $T_p$.
15) Embed auxiliary information into the tentative camouflage image using the high-capacity PEE method as described in III.C and generate the final camouflage image $M$.
```

TABLE 4. The comparison results among CPSNR of tentative and final camouflage images, and amount of AI by setting different sub-block refinement strategies.

Figure	Strategy	CPSNR [a] (dB)	Amount of AI (bpp)	CPSNR [b] (dB)
Fig. 14 (a)	4 patterns (**Patterns** #1 - 4)	35.5970	0.4546	35.1634
	8 patterns (**Patterns** #1 - 8)	35.6674	0.5106	35.2003
	16 patterns (**Patterns** #1 - 16)	35.8407	0.5650	35.2832
Fig. 14 (b)	4 patterns (**Patterns** #1 - 4)	31.1227	0.4835	30.9034
	8 patterns (**Patterns** #1 - 8)	31.1602	0.5391	30.9172
	16 patterns (**Patterns** #1 - 16)	31.2438	0.5889	30.9514
Fig. 14 (c)	4 patterns (**Patterns** #1 - 4)	33.5111	0.4801	32.8907
	8 patterns (**Patterns** #1 - 8)	33.6717	0.5425	32.9236
	16 patterns (**Patterns** #1 - 16)	34.0155	0.6050	33.0821

[a] for tentative camouflage image.
[b] for final camouflage image.

the table are the same except for the different RDH methods. Table 6 indicates that the distortion of some camouflage image, i.e., Fig. 14 (c) has been significantly decreased by using the proposed RDH method to embed the auxiliary information.

Then, we compared the proposed method with Hou *et al.*'s method [18]. We also take Fig. 14 as an example, and Table 6 lists the comparison results with respect to CPSNR and amount of AI. For our simulation, the classification parameter K in [18] was set at 6. In addition, to be fair, the same PEE-based RDH scheme [23] was used to embed the AI. Table 6 indicates that the proposed method presented better image quality than [18]. To compare the visual effect of the proposed method further, Fig. 15 shows an example of the

```
Algorithm 2 Secret Image Recovery
  Input: camouflage image $M$, secret key $\rho$
  Output: secret color image $I$
  Stage 1: Extraction of the auxiliary information and restoration of the tentatively camouflage image
  1) Extract the compressed and encrypted auxiliary information from the camouflage image, $M$, directly, and obtain the tentative transformed image, $\widetilde{M}$.
  2) Decompress and decrypt the auxiliary information using key $\rho$, and obtain the quantized mean difference coefficients, clustering index tables, sub-block refinement pattern numbers, and overflow/underflow residuals of channels of G, (R − G), and (B − G), respectively.
  Stage 2: Recovery of the G channel secret image
  3) Select G channel of $\widetilde{M}$, i.e., $\widetilde{M}_{\mathrm{G}}$, and divide it into non-overlapping $S \times S$ sized sub-blocks.
  4) Convert each sub-block back to its original pattern using the reverse direction of the sub-block conversion pattern.
  5) Restore the value with overflow/underflow according to the overflow/underflow residuals.
  6) Add the corresponding quantized mean difference to each pixel of each sub-block.
  7) Calculate the SD of each sub-block. Then, cluster the sub-blocks into $K$ classes according to the SDs and the clustering index table.
  8) Rearrange the sub-blocks according to the clustering results and the clustering index tables. Recover the G channel secret image $I_{\mathrm{G}}$.
  Stage 3: Recovery of the R channel (or B channel) secret image
  9) Select the R channel (or B channel) of $\widetilde{M}$, i.e., $\widetilde{M}_{\mathrm{R}}$ (or $\widetilde{M}_{\mathrm{B}}$), and repeat steps 4) and 5) to restore the pixels values with overflow/underflow.
  10) Calculate the color difference channel of $\widetilde{M}_{\mathrm{R}}$ (or $\widetilde{M}_{\mathrm{B}}$) and $\widetilde{M}_{\mathrm{G}}$, denoted $\widetilde{M}_{\mathrm{R-G}}$ (or $\widetilde{M}_{\mathrm{B-G}}$).
  11) Repeat steps 6) – 8) to restore the original difference channel $I_{\mathrm{R-G}}$ (or $I_{\mathrm{B-G}}$).
  12) Recover the R channel (or the B channel) of secret image $I_{\mathrm{R}}$ (or $I_{\mathrm{B}}$) by adding $I_{\mathrm{G}}$.
  13) Combine three-color channels (i.e., $I_{\mathrm{R}}$, $I_{\mathrm{G}}$, and $I_{\mathrm{B}}$) to recover the secret image, $I$.
```

comparison of the visual quality of the proposed method and those of [18]. As shown in Fig. 15, our method had the best visual quality, i.e., the lightest saw-toothed block effect, and the possible reasons for this promotion include sub-block transformation on color difference channel, more precise candidate pattern conversion in the sub-block refinement phase, and the redesigned parametric optimization during AI embedding phase.

To demonstrate the universality of the proposed method, we also compared our method and [18] using 100 pairs of images that were chosen randomly from the selected database [29]. Fig. 16 shows the comparison of the CPSNR values between the proposed method and [18]. In addition, the average results of the proposed method and [18] are listed in Table 7. From Fig. 16 and Table 7, the experimental results once again verified the improvement provided by the proposed method; compared with [18], our average gain in CPSNR was 0.3546 dB.

TABLE 5. The results by using conventional RDH method [23] and proposed RDH method among RMSE and CPSNR of final camouflage images.

Figure	Strategy	RMSE	CPSNR (dB)
Fig. 14 (a)	RDH method [23]	8.1192	35.1637
	Proposed RDH method	8.0734	35.2888
Fig. 14 (b)	RDH method [23]	20.8746	30.9639
	Proposed RDH method	20.8552	30.9732
Fig. 14 (c)	RDH method [23]	10.4156	32.7004
	Proposed RDH method	10.1914	33.0708

TABLE 6. The comparison results of [18] and the proposed method.

Figure	Method	CPSNR [a] (dB)	Amount of AI (bpp)	CPSNR [b] (dB)
Fig. 14 (a)	Hou et al. [18]	35.4337	0.5514	34.7936
	Proposed	35.8407	0.5650	35.2832
Fig. 14 (b)	Hou et al. [18]	31.0550	0.5754	30.7632
	Proposed	31.2438	0.5889	30.9514
Fig. 14 (c)	Hou et al. [18]	33.2364	0.5753	32.3860
	Proposed	34.0155	0.6050	33.0821

[a] for tentative camouflage image.
[b] for final camouflage image.

VI. DISCUSSION

The concept of opponent-color channels have been widely developed in many fields such as YUV, YCbCr, and CIE L * a * b * systems, however, the color channels converted by the existing opponent-color transforms inevitably have fractional parts, thereby generating round-off error after converting the opponent-color channel back to original RGB channels. The aim of the proposed method is to transform the secret image to another same-sized target image, with the capability of lossless recovery of original secret image. Therefore, we are insistent on using the color difference channels (i.e., G, (R - G), and (B - G) channels) to avoid this issue. To clarify the reason why do not directly adopt the existing opponent-color channels more clearly, following we take YCbCr transform as an example.

The process of RGB to YCbCr transformation for a pixel I_k^i can be expressed as

$$\left[I_{k,\mathrm{Y}}^i, I_{k,\mathrm{Cb}}^i, I_{k,\mathrm{Cr}}^i\right] = \boldsymbol{rgb2ycbcr}\left(I_{k,\mathrm{R}}^i, I_{k,\mathrm{G}}^i, I_{k,\mathrm{B}}^i\right) \quad (13)$$

where, $I_{k,\mathrm{R}}^i$, $I_{k,\mathrm{G}}^i$ and $I_{k,\mathrm{B}}^i$ stand for the RGB components of I_k^i, and $I_{k,\mathrm{Y}}^i$, $I_{k,\mathrm{Cb}}^i$, and $I_{k,\mathrm{Cr}}^i$ correspond to the converted YCbCr components, respectively. Specifically, function ***rgb2ycbcr*** denotes the transformation from RGB color space to YCbCr

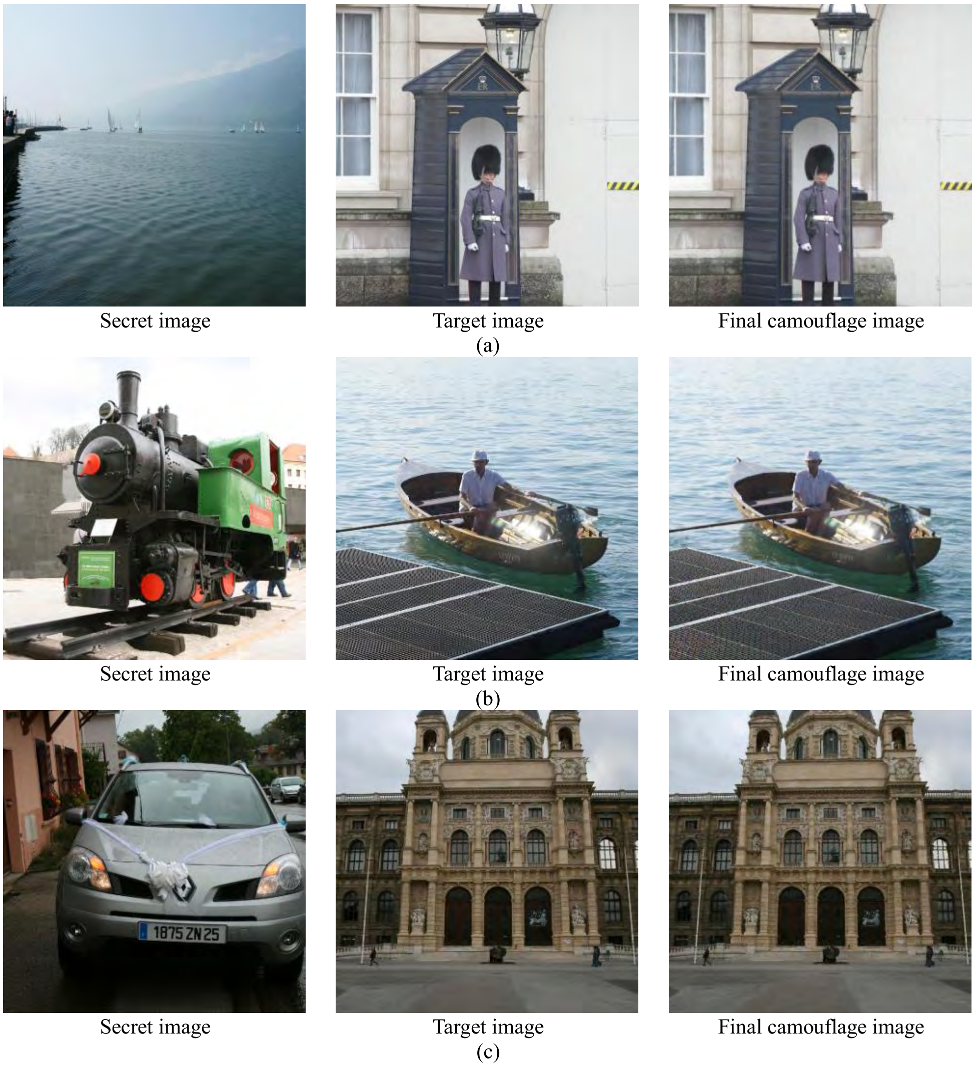

Secret image Target image Final camouflage image
(a)
Secret image Target image Final camouflage image
(b)
Secret image Target image Final camouflage image
(c)

FIGURE 14. Example results of the proposed method. (a) Example 1. (b) Example 2. (c) Example 3.

space, i.e.,

$$\begin{bmatrix} I^i_{k,\mathrm{Y}} \\ I^i_{k,\mathrm{Cb}} \\ I^i_{k,\mathrm{Cr}} \end{bmatrix} = \begin{bmatrix} 0.257 & 0.564 & 0.098 \\ -0.148 & -0.291 & 0.439 \\ 0.439 & -0.368 & -0.071 \end{bmatrix} \begin{bmatrix} I^i_{k,\mathrm{R}} \\ I^i_{k,\mathrm{G}} \\ I^i_{k,\mathrm{B}} \end{bmatrix} + \begin{bmatrix} 16 \\ 128 \\ 128 \end{bmatrix} \tag{14}$$

In this case, the values of $I^i_{k,\mathrm{Y}}$, $I^i_{k,\mathrm{Cb}}$, and $I^i_{k,\mathrm{Cr}}$ are all decimals due to the non-integral mapping. Then we continue conducting the proposed lossless image camouflage algorithm on the YCbCr color space before converting the camouflaged YCbCr values back into RGB values. These two processes can be merged into one equation as

$$\left[I'^i_{k,\mathrm{R}}, I'^i_{k,\mathrm{G}}, I'^i_{k,\mathrm{B}}\right] = \boldsymbol{ycbcr2rgb}\left(I^i_{k,\mathrm{Y}} + \Delta\mu_{\mathrm{Y}}, I^i_{k,\mathrm{Cb}} + \Delta\mu_{\mathrm{Cb}}, I^i_{k,\mathrm{Cr}} + \Delta\mu_{\mathrm{Cr}}\right) \tag{15}$$

where, $I'^i_{k,\mathrm{R}}$, $I'^i_{k,\mathrm{G}}$, and $I'^i_{k,\mathrm{B}}$ stand for the RGB component of the camouflaged pixel, denoted I^i_k, and $\Delta\mu_{\mathrm{Y}}$, $\Delta\mu_{\mathrm{Cb}}$, and $\Delta\mu_{\mathrm{Cr}}$ indicate the quantized sub-block mean difference values between the secret image and the target image for the YCbCr components, respectively. Function ***ycbcr2rgb*** indicates the reverse transformation from YCbCr space to RGB color space. Reversely to (14), Equation (15) can be detailedly represented as

$$\begin{bmatrix} I'^i_{k,\mathrm{R}} \\ I'^i_{k,\mathrm{G}} \\ I'^i_{k,\mathrm{B}} \end{bmatrix} = \begin{bmatrix} 1.164 & 0 & 1.596 \\ 1.164 & -0.392 & -0.813 \\ 1.164 & 2.017 & 0 \end{bmatrix} \times \begin{bmatrix} I^i_{k,\mathrm{Y}} + \Delta\mu_{\mathrm{Y}} - 16 \\ I^i_{k,\mathrm{Cb}} + \Delta\mu_{\mathrm{Cb}} - 128 \\ I^i_{k,\mathrm{Cr}} + \Delta\mu_{\mathrm{Cr}} - 128 \end{bmatrix} \tag{16}$$

Note that the values of $I'^i_{k,\mathrm{R}}$, $I'^i_{k,\mathrm{G}}$, and $I'^i_{k,\mathrm{B}}$ are all decimals. To save the image as uncompressed bitmap format, each values of $I'^i_{k,\mathrm{R}}$, $I'^i_{k,\mathrm{G}}$, and $I'^i_{k,\mathrm{B}}$ deserve to be further rounded and

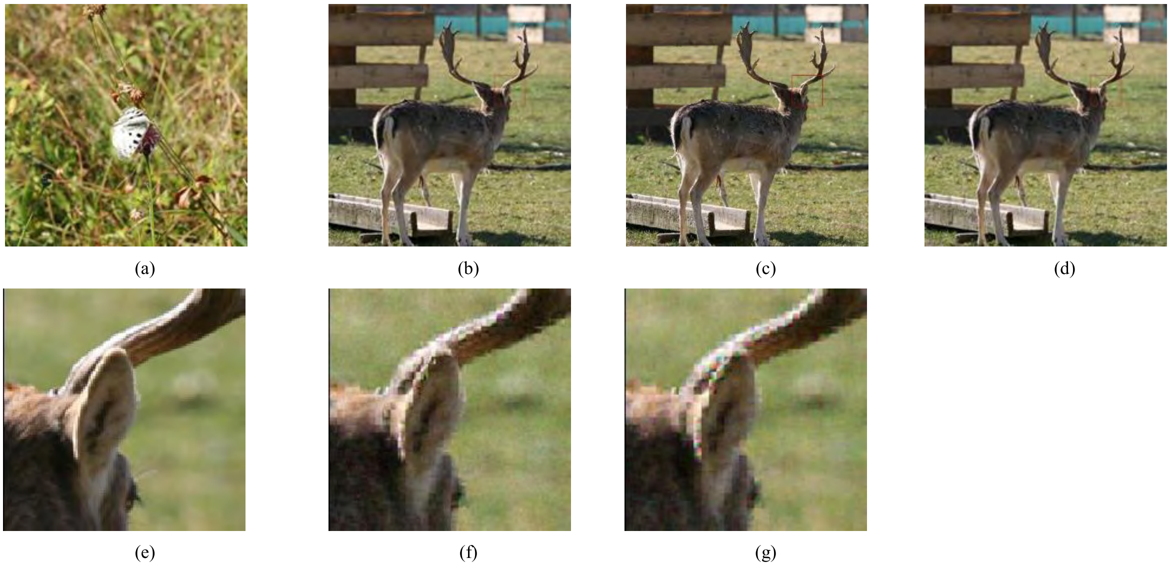


FIGURE 15. An example of visual quality comparison between the proposed method and [18]. (a) Secret image. (b) Target image. (c) Camouflage image generated by the proposed method. (d) Camouflage image generated by Hou *et al.*'s method [18]. (e) Zoom-in image of red square region from image (b). (f) Zoom-in image of red square region from image (c). (g) Zoom-in image of red square region from image (d).

TABLE 7. The average results on 100 pairs of images of database [29] among RMSE of tentative and final camouflage image, CPSNR of tentative and final camouflage image, and amount of AI.

Method	RMSE [a]	CPSNR [a] (dB)	Amount of AI (bpp)	RMSE [b]	CPSNR [b] (dB)
Hou et al. [18]	13.9465	32.9667	0.5845	14.4333	32.2768
Proposed	12.4704	33.4459	0.6349	12.9668	32.6314

[a]for tentative camouflage image.
[b]for final camouflage image.

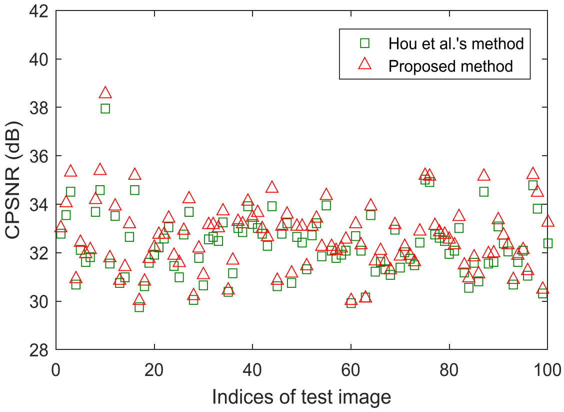


FIGURE 16. Comparison of CPSNR of final camouflage images between the proposed method and [18].

truncated to the integers $I''^{i}_{k,\mathrm{R}}$, $I''^{i}_{k,\mathrm{G}}$, and $I''^{i}_{k,\mathrm{B}}$ with the interval of [0, 255]. In this way, $I''^{i}_{k,\mathrm{R}}$, $I''^{i}_{k,\mathrm{G}}$, and $I''^{i}_{k,\mathrm{B}}$ can be expressed as

$$\begin{bmatrix} I''^{i}_{k,\mathrm{R}} \\ I''^{i}_{k,\mathrm{G}} \\ I''^{i}_{k,\mathrm{B}} \end{bmatrix} = \begin{bmatrix} I'^{i}_{k,\mathrm{R}} \\ I'^{i}_{k,\mathrm{G}} \\ I'^{i}_{k,\mathrm{B}} \end{bmatrix} + \begin{bmatrix} \varepsilon_{\mathrm{R}} \\ \varepsilon_{\mathrm{G}} \\ \varepsilon_{\mathrm{B}} \end{bmatrix} \tag{17}$$

where ε_{R}, ε_{G}, and ε_{B} denote the round-off and truncated errors in RGB components, respectively, and they are all decimals. Since ε_{R}, ε_{G}, and ε_{B} are not saved in the proposed method, the secret image cannot be losslessly recovered. Actually it is not realistic to save ε_{R}, ε_{G}, and ε_{B} owing to the limited auxiliary information space, therefore, we have demonstrated that the existing opponent-color transform cannot applied in the scope of reversible image camouflage.

VII. CONCLUSION

In this paper, we proposed an improved image camouflage algorithm to transform a secret image to another image that is visually similar to the selected target image. The secret image can be restored losslessly in the recovery phase. We improved Hou *et al.*'s work [18] in following three aspects: 1) Giving up the RGB independent transformation strategy, the color difference channels, i.e., the (R – G) and (B – G) channels, were used to transform the secret sub-blocks to their corresponding matched target sub-blocks; 2) After image transformation, 16 candidate patterns were used to replace the previous 4-pattern strategy to further improve the similarity between the tentative camouflage sub-blocks and their corresponding target sub-blocks; 3) Revisited the framework of AI embedding, which actually has a different objective relative to the conventional RDH methods. Based on the above improvements, the experimental results have demonstrated the efficacy and superiority of the proposed method.

Fig. 15 shows that, although our method performs better than the existing reversible image transformation method in [18], obvious block artifacts still can be easily perceived once one applies an enlarged view of some local part of the camouflage image. Thus, our future research direction will be to determine how to suppress the abrupt boundaries between each of the neighboring sub-blocks rather than merely decreasing the distortion between the camouflage image and the target image.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their helpful comments.

REFERENCES

[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[2] National Institute of Standards and Technology. (Nov. 2001). *FIPS PUB 197, Advanced Encryption Standard (AES)*. [Online]. Available: https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf

[3] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, 1999, pp. 223–238.

[4] W. Zhang, H. Yu, Y.-L. Zhao, and Z.-L. Zhu, "Image encryption based on three-dimensional bit matrix permutation," *Signal Process.*, vol. 118, pp. 36–50, Jan. 2016.

[5] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016.

[6] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Inf. Sci.*, vol. 339, pp. 237–253, Apr. 2016.

[7] Y. Wu, Y. Zhou, S. Agaian, and J. P. Noonan, "A symmetric image cipher using wave perturbations," *Signal Process.*, vol. 102, pp. 122–131, Sep. 2014.

[8] J. B. Lima and L. F. G. Novaes, "Image encryption based on the fractional Fourier transform over finite fields," *Signal Process.*, vol. 94, pp. 521–530, Jan. 2014.

[9] S. Tedmori and N. Al-Najdawi, "Image cryptographic algorithm based on the Haar wavelet transform," *Inf. Sci.*, vol. 269, pp. 21–34, Jun. 2014.

[10] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography," *Signal Process.*, vol. 125, pp. 187–202, Aug. 2016.

[11] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Process.*, vol. 134, pp. 35–51, May 2017.

[12] L. Bao and Y. Zhou, "Image encryption: Generating visually meaningful encrypted images," *Inf. Sci.*, vol. 324, pp. 197–207, Dec. 2015.

[13] A. Kanso and M. Ghebleh, "An algorithm for encryption of secret images into meaningful images," *Opt. Laser. Eng.*, vol. 90, pp. 196–208, Mar. 2017.

[14] R. K. Lama, S.-J. Han, and G.-R. Kwon, "SVD based improved secret fragment visible mosaic image generation for information hiding," *Multimedia Tools Appl.*, vol. 73, no. 2, pp. 873–886, Nov. 2014.

[15] Y.-L. Lee and W.-H. Tsai, "A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 24, no. 4, pp. 695–703, Apr. 2014.

[16] I.-J. Lai and W.-H. Tsai, "Secret-fragment-visible mosaic image—A new computer art and its application to information hiding," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 936–945, Sep. 2011.

[17] W. Zhang, H. Wang, D. Hou, and N. Yu, "Reversible data hiding in encrypted images by reversible image transformation," *IEEE Trans. Multimedia*, vol. 18, no. 8, pp. 1469–1479, Aug. 2016.

[18] D. Hou, W. Zhang, and N. Yu, "Image camouflage by reversible image transformation," *J. Vis. Commun. Image Represent.*, vol. 40, pp. 225–236, Oct. 2016.

[19] D. Hou, C. Qin, N. Yu, and W. Zhang, "Reversible visual transformation via exploring the correlations within color images," *J. Vis. Commun. Image Represent.*, vol. 53, pp. 134–145, May 2018.

[20] C. Qin, C.-C. Chang, and Y.-P. Chiu, "A novel joint data-hiding and compression scheme based on SMVQ and image inpainting," *IEEE Trans. Image Process.*, vol. 23, no. 3, pp. 969–978, Mar. 2014.

[21] X. Xiao and L. Ma, "Color transfer in correlated color space," in *Proc. ACM Int. Conf. Virtual Reality Continuum Appl.*, 2006, pp. 305–309.

[22] E. Reinhard, M. Adhikhmin, B. Gooch, and P. Shirley, "Color transfer between images," *IEEE Comput. Graph. Appl.*, vol. 21, no. 5, pp. 34–41, Sep./Oct. 2001.

[23] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009.

[24] W. Zhang, X. Hu, X. Li, and N. Yu, "Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression," *IEEE Trans. Image Process.*, vol. 22, no. 7, pp. 2775–2785, Jul. 2013.

[25] C. Qin, C.-C. Chang, Y.-H. Huang, and L.-T. Liao, "An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 23, no. 7, pp. 1109–1118, Jul. 2013.

[26] I.-C. Dragoi and D. Coltuc, "Local-prediction-based difference expansion reversible watermarking," *IEEE Trans. Image Process.*, vol. 23, no. 4, pp. 1779–1790, Apr. 2014.

[27] B. Ou, X. Li, Y. Zhao, and R. Ni, "Efficient color image reversible data hiding based on channel-dependent payload partition and adaptive embedding," *Signal Process.*, vol. 108, pp. 642–657, Mar. 2015.

[28] H. Yao, C. Qin, Z. Tang, and Y. Tian, "Guided filtering based color image reversible data hiding," *J. Vis. Commun. Image Represent.*, vol. 43, pp. 152–163, Feb. 2017.

[29] *BossBase Image Database*. Accessed: Jul. 24, 2018. [Online]. Available: http://agents.fel.cvut.cz/stegodata/RAWs

HENG YAO (S'11–M'12) received the B.Sc. degree from the Hefei University of Technology, China, in 2004, the M.Eng. degree from Shanghai Normal University, China, in 2008, and the Ph.D. degree in signal and information processing from Shanghai University, China, in 2012. He is currently with the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, China. He has contributed over 15 international journal papers. His research interests include multimedia security, image processing, and pattern recognition.

XIAOKAI LIU received the B.S. degree in power electronics and power drives from the University of Shanghai for Science and Technology, Shanghai, China, in 2016, where he is currently pursuing the master's degree. His current research interests include information hiding and image camouflage.

ZHENJUN TANG (M'15) received the B.S. and M.Eng. degrees from Guangxi Normal University, Guilin, China, in 2003 and 2006, respectively, and the Ph.D. degree from Shanghai University, Shanghai, China, in 2010. He is currently a Professor with the Department of Computer Science, Guangxi Normal University. He has contributed over 50 international journal papers. He holds six China patents. His research interests include image processing and multimedia security. He is a Senior Member of the China Computer Federation and also a reviewer of over 20 SCI-indexed journals, such as IEEE journals, IET journals, Elsevier journals, Springer journals, and Taylor & Francis journals.

YU-CHEN HU (M'03–SM'15) received the Ph.D. degree in computer science and information engineering from the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan, in 1999.He is currently a Professor with the Department of Computer Science and Information Management, Providence University, Sha-Lu, Taiwan. His research interests include image and signal processing, data compression, information hiding, and data engineering. He is a member of ACM. He is also a member of Computer Vision, Graphics, and Image Processing, Chinese Cryptology and Information Security Association. He has been serving as the Editor-in-Chief of the *International Journal of Image Processing* since 2009. In addition, he is the Managing Editor of the *Journal of Information Assurance and Security*.

CHUAN QIN (M'11) received the B.S. degree in electronic engineering and the M.S. degree in signal and information processing from the Hefei University of Technology, Anhui, China, in 2002 and 2005, respectively, and the Ph.D. degree in signal and information processing from Shanghai University, Shanghai, China, in 2008. He was with Feng Chia University, Taiwan, as a Post-Doctoral Researcher and an Adjunct Assistant Professor from 2010 to 2012. Since 2008, he has been with the Faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, where he is currently an Associate Professor. His research interests include image processing and multimedia security. He has published over 90 papers in these research areas.