Journal of Information Hiding and Multimedia Signal Processing ©2015 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **4**, July **2015**

High-Capacity Steganographic Method for Color Images Using Progressive Pixel-Alignment

Ching-Yu Yang

Department of Computer Science and Information Engineering
National Penghu University of Science and Technology
300, Liuhe Rd., Magong, Penghu 880, Taiwan
chingyu@npu.edu.tw

Wen-Fong Wang

Department of Computer Science and Information Engineering
National Yunlin University of Science and Technology
123 University Rd., Sec. 3, Douliou, Yunlin 640, Taiwan
wwf@yuntech.edu.tw

Received November, 2014; revised March, 2015

Abstract. *By adjusting the pixel-value of a host block, we design an effective steganographic method for color images. More specifically, based on a progressive pixel-alignment approach with two averages of the given block, a secret message can be embedded in a host image without apparent visual distortion. Our experiments indicate that the perceived quality generated by our proposed method is quite good, and the payload is larger than most existing techniques. Moreover, our proposed method maintains a certain degree of robustness; the marked images generated by our method are tolerant of manipulations such as color quantization, equalization, edge sharpening, inversion, JPEG, JPEG2000, noise addition, pixel truncation, winding, and zigzagging. This robustness is rarely found in the traditional techniques for color image steganography.*
Keywords: Data hiding; Color image steganography; Progressive pixel-alignment

1. **Introduction.** Thanks to the rapid evolution of fast broadband services and applications available on intelligent mobile devices, people can easily share and exchange data on the Internet; however, such data can be eavesdropped, falsified, and tampered with during transmission. Data hiding techniques are gradually attracting interest and are being used to ad-dress the above issues. Several applications of data hiding can be found in protecting intellectual property rights, content authentication, and copyright protection [1]–[4]. In general, data hiding consists of two categories: steganography and digital watermarking.

The key advantage of watermarking approaches [5]–[8] is robustness performance. More specifically, most watermarked images are tolerant of manipulations, such as compression, cropping, noise-addition, and quantization attacks; however, most conventional watermarked methods introduce a limited payload size. Conversely, a key advantage of steganographic methods [9]–[11] is providing large hidden storage space while maintaining good perceived quality for covert communication between or among multiple parties.

Further, as color images are more attractive than grayscale images and are commonly circulated around the world, several researchers have presented data hiding techniques for color images [12]–[15]. In [12], Yang used the radius-weighted mean (RWM) and presented

a steganographic method for color images. Based on the RWM-decision pol-icy with the least-significant bit (LSB) substitution technique, data bits are effectively embedded in host color images. Simulations showed that the resultant payload was larger than existing techniques while the perceived quality was not too bad. In [13], based on edge detection and an efficient hiding technique, Ioannidou et al. proposed a novel image steganography. Experimental results indicated that their peak-to-signal ratio (PSNR) performance was good with a limited payload size. Moreover, the overhead required for this technique was significant; i.e., two auxiliary files must be sent to the receiver to extract the secret bits.

In [14], based on the pixel-value differencing (PVD) scheme, Mandal and Das suggested a color image steganography in the spatial domain. To further promote security and avoid the overflow issue, their proposed scheme embedded different number of data bits in different pixel components. Experiments demonstrated that the resultant payload size was not bad while perceived quality was good. In [15], based on a mix column transform (MCT) with irreducible polynomial mathematics, Abduallah et al. presented a novel color image steganography. Simulations showed that the average hiding capacity of the scheme was about 198 Kb with a PSNR of approximately 38 dB when one of the RGB planes was used.

In this paper, we propose a steganographic method for color images based on a progressive pixel-alignment approach with two averages of the given block. In addition to this introductory section, the remainder of this paper is organized as follows. Our pro-posed bit-embedding and bit-extraction techniques are described in Section 2. Experimental results are presented in Section 3, and our conclusions are summarized in Section 4.

2. **The Proposed Robust Watermarking Scheme.** For our proposed method, an RGB host image is first extracted into its individual RGB planes. Each plane is then divided into a series of non-overlapping $n \times n$ blocks. A secret message is subsequently embedded in the host blocks of each plane. As our proposed method uses the same approach to embed data bits in the blocks of each of the RGB planes, for clarity, only data hiding in the R-plane is presented here. In the following subsections, we describe the details of our proposed bit-embedding and bit-extraction techniques in the R-plane.

2.1. **Data Embedding.** Without loss of generality, let $H_k = \{(r_{i-1,j-1}, r_{i-1,j}, r_{i,j-1}, r_{i,j})\}$ be the kth host block divided from the R-plane of an RGB color space, as shown in Fig. 1 (with $n = 2$); also let $H_k = \hat{H} \cup \tilde{H}$, with $\hat{H} = \{(r_{i-1,j-1}, r_{i,j})\}$ and $\tilde{H} = \{(r_{i-1,j}, r_{i,j-1})\}$. Let $M_{\hat{H}} = \lfloor (r_{i-1,j-1} + r_{i,j})/2 \rfloor$ and $M_{\tilde{H}} = \lfloor (r_{i-1,j} + r_{i,j-1})/2 \rfloor$ be the two average values of the block. Our proposed bit-embedding technique is described by the following algorithm.

$(r_{i-1,j-1})$	$(r_{i-1,j})$
$(r_{i,j-1})$	$(r_{i,j})$

FIGURE 1. A 2×2 host block of the R-plane.

Algorithm 1. Hiding data bits in the R-plane of a color image.
Input: R-plane image S_R, secret message T, and two control parameters τ_r and λ.
Output: Marked image S'_R.
Method:

Step 1: Input block H_k, which is derived from S_R. If the end of input is encountered, then proceed to Step 6.

Step 2: Compute offset φ of the block, i.e., $\varphi = M_{\hat{H}} - M_{\tilde{H}}$.
Step 3: Obtain one data bit δ from T, and perform the following sub-steps:
Step 4: If $\delta = 1$, then perform the following sub-steps:
- **Step 4.1:** If $\varphi < 0$ and $\varphi \geq -\tau_r$ are satisfied, then do nothing, meaning the block "carries" data bit 1 without altering the pixel's value; proceed to Step 1.
- **Step 4.2:** If $\varphi < -\tau_r$, repeatedly increase the pixel-value in $\hat{H}$ and decrease the pixel-value in $\tilde{H}$ by λ, until either conditions $\varphi < 0$ and $\varphi \geq -\tau_r$ are satisfied, or we attempt this τ_r times.
- **Step 4.3:** If $\varphi < 0$ and $\varphi \geq -\tau_r$, proceed to Step 1; otherwise, undo the above pixel-value adjustments, mark the block as a skipped block, and proceed to Step 1.
- **Step 4.4:** If $\varphi > \tau_r$, repeatedly increase the pixel-value in $\tilde{H}$ and decrease the pixel-value in $\hat{H}$ by λ, until either conditions $\varphi < 0$ and $\varphi \geq -\tau_r$ are satisfied, or we attempt this τ_r times.
- **Step 4.5:** If $\varphi < 0$ and $\varphi \geq -\tau_r$, proceed to Step 1; otherwise, undo the above pixel-value adjustments, mark the block as a skipped block, and proceed to Step 1.

Step 5: If $\delta = 0$, then perform the following sub-steps:
- **Step 5.1:** If $\varphi \leq \tau_r$ and $\varphi \geq 0$ are satisfied, then do nothing, meaning the block "carries" data bit 0 without altering the pixel's value; proceed to Step 1.
- **Step 5.2:** If $\varphi > \tau_r$, repeatedly increase the pixel-value in $\tilde{H}$ and decrease the pixel-value in $\hat{H}$ by λ until either conditions $\varphi \leq \tau_r$ and $\varphi \geq 0$ are satisfied, or we attempt this τ_r times.
- **Step 5.3:** If $\varphi \leq \tau_r$ and $\varphi \geq 0$, then proceed to Step 1; otherwise, undo the above pixel-value adjustments, mark the block as a skipped block, and proceed to Step 1.
- **Step 5.4:** If $\varphi < 0$, repeatedly increase the pixel-value in $\hat{H}$ and decrease the pixel-value in $\tilde{H}$ by λ until either conditions $\varphi \leq \tau_r$ and $\varphi \geq 0$ are satisfied, or we attempt this τ_r times.
- **Step 5.5:** If $\varphi \leq \tau_r$ and $\varphi \geq 0$, then proceed to Step 1; otherwise, undo the above pixel-value adjustments, mark the block as a skipped block, and proceed to Step 1.

Step 6: Stop.

To avoid overflow during pixel adjustment, the increment operation bypasses pixels with values greater than $(255 - \tau_r)$. Similarly, to avoid underflow, the decrement operation bypasses pixels with values less than or equal to τ_r. Flowcharts of our proposed bit-embedding scheme are shown in Fig. 2.

2.2. **Data Extraction.** Let $H'_k = \{(r'_{i-1,j-1}, r'_{i-1,j}, r'_{i,j-1}, r'_{i,j})\}$ be the kth hidden block extracted from the R-plane of marked image $H'_k = \hat{H}' \cup \tilde{H}'$ with $\hat{H}' = \{(r'_{i-1,j-1}, r'_{i,j})\}$ and $\tilde{H}' = \{(r'_{i-1,j}, r'_{i,j-1})\}$. Also let $M_{\hat{H}'}$ and $M_{\tilde{H}'}$ be the two average values of the given block. The bit-extraction procedure is simpler than that of bit-embedding; the algorithm is specified in the following steps.

Input: Marked image S'_R, and control parameter τ_r.
Output: Secret message T.
Method:

Step 1: Input hidden block H'_k, derived from S'_R If end of the input is encountered, then proceed to Step 4.
Step 2: Compute block offset $\varphi = M_{\hat{H}'} - M_{\tilde{H}'}$.

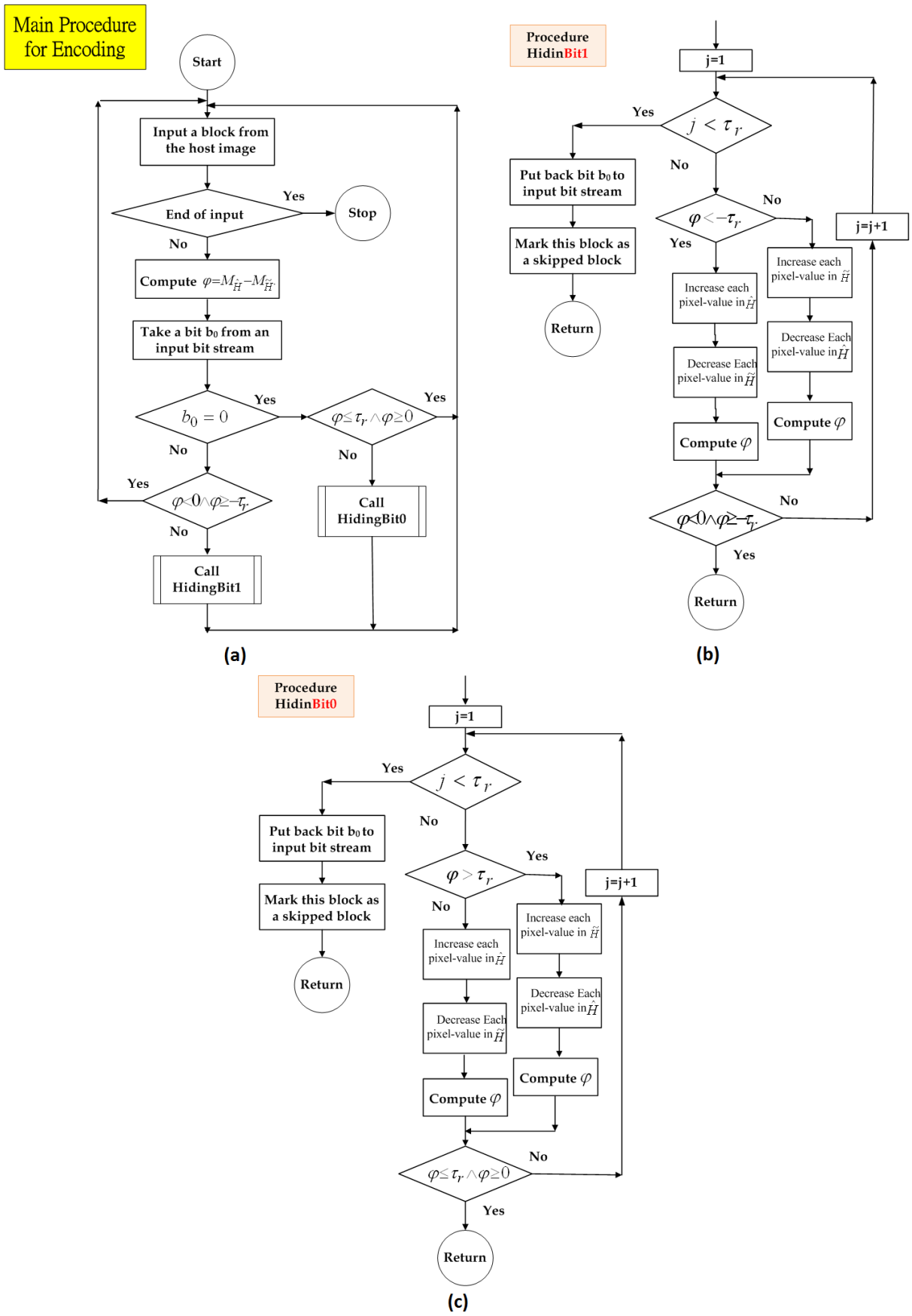


FIGURE 2. Flowcharts of our proposed bit-embedding algorithm: (a) main procedure, (b) HidingBit1 procedure, and (c) HidingBit0 procedure.

TABLE 1. PSNR and payload comparison between our proposed method using different block sizes: 2×2 and 3×3.

Images	Block size	
	2×2	3×3
Lena	41.58/196,608	43.65/86,700
Jet	43.73/196,608	43.10/86,700
Peppers	39.43/196,608	40.20/86,700
Tiffany	40.57/196,608	42.84/86,700
Splash	44.86/196,608	45.36/86,700
House	49.17/196,608	47.10/86,700
Couple	49.54/196,608	47.96/86,700
CarHouse	41.34/196,608	42.04/86,700
Average	43.78/196,608	44.03/86,700

Step 3: If conditions $\varphi < 0$ and $\varphi \geq -\tau_r$ are satisfied, then data bit 1 is extracted; otherwise, data bit 0 is extracted, and proceed to Step 1.
Step 4: Assemble the extracted data bits to form secret message T.
Step 5: Stop.

As mentioned above, a secret message is embedded separately in the three planes of a host color image. More specifically, the bit-embedding sequence follows the order of R-plane, G-plane, and B-plane.

3. **Experimental Results.** Several 512×512 color images were used as host images. Each RGB pixel of the host images is represented by 24 bits, 8 bits per component. The size of the test binary watermark was 444×444, and the block size was 2×2. Integer λ was set to 1. The marked images generated by our proposed method are shown in Fig. 3. From the figure, we observe that each host image has a variety of control parameters, i.e., τ_r, τ_g, and τ_b, in the RGB plane. For example, control parameters $\tau_r = 19$, $\tau_g = 32$, and $\tau_b = 27$ were used for the image Lena. No skipped blocks were generated.

The optimal number of hidden bits for each marked image is $(512 \times 512)/2 \times 2 \times 2 = 196,608$ bits. From the figure, we observe that the perceived quality is rather good. No false colors appeared in the figures. Their corresponding PSNR is given in Table 1. Further, performance of our proposed method using a host block of size 3×3 is included. From Table 1, we observe that the payload for a block of size 2×2 is larger than that of 3×3 blocks, while the average PSNR of the former is slightly smaller than that of the latter. Similarly, there were no skipped blocks when a 3×3 block size was used. More specifically, no overhead (such as a bitmap) was required by our proposed method. The PSNR is defined by

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \tag{1}$$

with $MSE = \frac{1}{3MN} \sum_{i=1}^{MN} \left[(r_i - \widehat{r}_i)^2 + (g_i - \widehat{g}_i)^2 + (b_i - \widehat{b}_i)^2 \right]$. Here (r_i, g_i, b_i) and $\left(\widehat{r}_i, \widehat{g}_i, \widehat{b}_i \right)$ denote the RGB pixel values of the host image and the marked image, respectively.

Table 2 summarizes a comparison of performance of our proposed method with the following existing schemes: Yang's scheme [12]; Ioannidou et al.'s approach [13]; Mandal and Das's technique [14]; and Abduallah et al.'s algorithm [15]. We observe that the payload provided by our method is larger than that provided by methods in [12]–[14], while

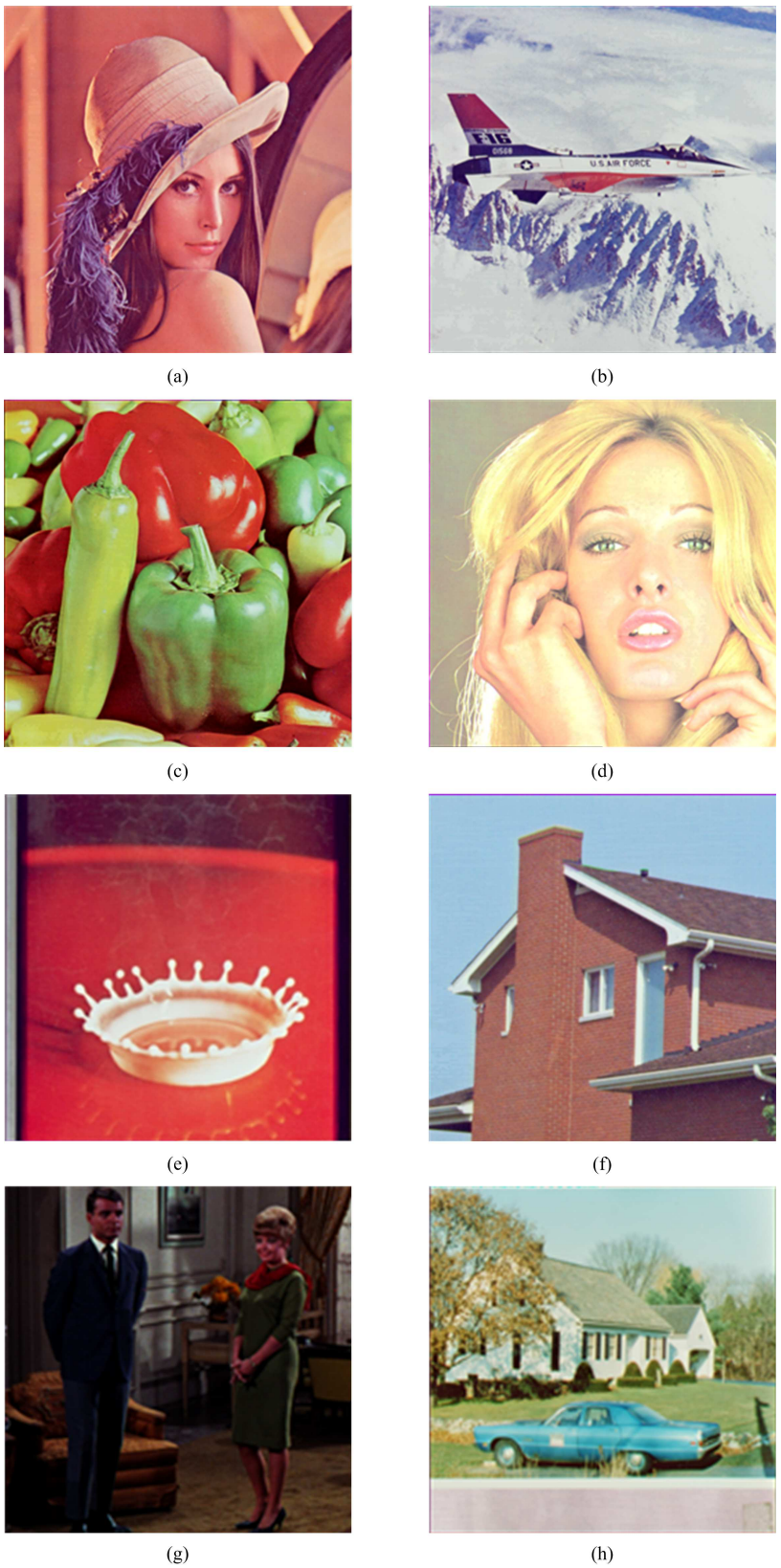


FIGURE 3. Marked images generated by our proposed method using various control parameters ($\tau_r/\tau_g/\tau_b$) in the host images: (a) Lena (19/32/27); (b) Jet (20/37/23); (c) Peppers (28/39/33); (d) Tiffany (40/77/69); (e) Splash (14/66/34); (f) House (5/6/7); (g) Couple (9/10/9); and (h) Car-House (86/40/24).

TABLE 2. PSNR and payload comparison between our proposed method and other existing methods.

Images	Method				
	Ref. [12]	*Ref.*[13]$^{+}$	Ref. [14]	*Ref.*[15]†	*Our method**
Lena	45.32/171,200	45.12/30,987	42.26/145,787	37.58/203,043	41.58/196,608
Baboon	46.44/160,300		38.44/144,916	37.72/203,043	33.29/196,608
Jet	44.90/199,500		42.60/145,648	37.87/203,043	43.73/196,608
Peppers	46.20/181,300	44.45/∼31kb	42.28/145,995	37.73/203,043	39.43/196,608
Car-House	47.61/110,870		41.41/145,374		41.34/196,608
Splash	45.24/145,900		42.86/146,732		44.86/196,608
Sailboat	46.61/166,780	40.66/143,278		47.41/196,608	
Tiffany	42.12/165,720	43.87/∼31kb			40.57/196,608
House	45.48/175,440	45.12/∼31kb			49.17/196,608
Average	45.55/164,112	44.64/∼31kb	41.50/145,390	37.73/203,043	43.80/196,608

$^{+}$ The method uses the Laplacian or fuzzy edge detector without using a random number generator.
† Secret bits are only embedded in the R-plane of a color image.
* The block size is 2×2.

the average PSNR of our method is still larger than that of Mandal and Das's technique [14]. The average PSNR for our proposed method is slightly less than that of Yang's scheme [12] and Ioannidou et al.'s approach [13]; however, the hiding capacity provided by our method is approximately six times larger than that provided by Ioannidou et al.'s approach [13]. In addition, the average PSNR for our proposed method is approximately 6 dB larger than that of Abduallah et al.'s algorithm [15] with a competitive payload size.

To demonstrate that our proposed steganographic method shares a certain degree of robustness performance, the marked images were tested by various attacks. Extracted watermarks and their bit correct ratio (BCR) are shown in Table 3. The size of an input watermark is 443×443. The tested marked image is generated by using our proposed method with $\tau_r = 19$, $\tau_g = 32$, and $\tau_b = 27$, and $\lambda = 1$ on the *Lena* image.

The BCR is defined by

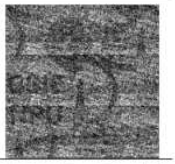
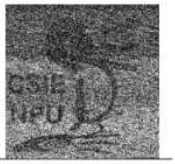
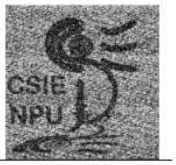
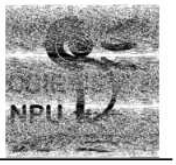
$$BCR = \left(\frac{\sum_{i=0}^{ab-1} \overline{w_i \oplus \widetilde{w_i}}}{a \times b}\right) \times 100\% \tag{2}$$

where w_i and $\widetilde{w_i}$ represent the values of the original and extracted watermarks, respectively; furthermore, the size of the watermark is $a \times b$. The BCR for an extracted watermark is 100% if the marked image is not manipulated.

Table 3 shows that most extracted watermarks were recognized. Note that the BCR of the survived watermark extracted from a marked image, which had undergone inversion attack, was only 7.51%, and it was still recognizable. In addition, the extracted watermarks were recognized when the marked images were compressed by JPEG2000/JPEG with a compression ratio (CR) of approximately ten and four, respectively. Similar performance can be found in the marked images manipulated by color quantization, pixel truncation, winding, and zigzagging. Moreover, the survived watermarks were identified after the marked images had undergone uniform and Gaussian-noise addition attacks.

4. **Conclusion.** In this paper, we proposed a straightforward color image steganography approach. Using a progressive pixel-alignment strategy with the two average values of the given block, we showed that data bits can be effectively embedded in a host image with

TABLE 3. The survived watermarks extracted from the marked images that have undergone various manipulations.

Attacks	Survived watermarks	Attacks	Survived watermarks
Null Attack BCR = 100%		JPEG2000 (CR=9.97) BCR=50.83%	
Color quantization (8-color) BCR=35.68%		JPEG (QF=90) BCR=51.71%	
Edge Sharpening BCR=97.57%		Truncation* BCR=35.88%	
Equalization BCR=90.99%		Uniform noise (6%) BCR =60.45%	
Gaussian noise (3%) BCR =59.01%		Winding BCR =60.69%	
Inversion BCR=7.51%		Zigzagging BCR =66.38%	

* The last five bits of the stego-pixels were purposely truncated.

no apparent color distortion. Simulations confirmed that the visual quality introduced by our proposed method was quite good and that the payload for our proposed method was better than most existing techniques. In addition, our proposed method shares a certain degree of robustness. The marked images generated by our method were tolerant of manipulations such as color quantization, equalization, edge sharpening, inversion, JPEG, JPEG2000, noise additions, pixel truncation, winding, and zigzagging. Most conventional steganographic approaches rarely possess this level of robustness performance.

REFERENCES

[1] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, "Digital Watermarking and Steganography," 2nd Ed., Morgan Kaufmann., MA, 2008.

[2] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: survey and analysis of current methods," *Signal Processing*, vol. 90, pp. 727-752, 2010.

[3] A. Phadikar, Data Hiding Techniques and Applications Specific Designs, LAP LAMBERT Academic Publishing, Saarbrucken, Germany, 2012.

[4] E. Eielinska, W. Mazurczyk, and K. Szczypiorski, "Trends in steganography," *Communications of the ACM*, vol. 57, pp. 86-95, 2014.

[5] R. M. Noriega, M. Nakano, B. Kurkoski, and K. Yamaguchi, "High payload audio watermarking: toward channel characterization of MP3 compression," *Journal of In-fo. Hiding and Multimedia Signal Processing*, vol. 2, no. 2, pp. 91-107, 2011.

[6] P. P., Niu, X. Y. Wang, Y. Yang, and M. Y. Lu, "A novel color image watermarking scheme in nonsampled contourlet-domain," *Expert System with Applications*, vol. 38, pp. 2081-2098, 2011.

[7] A. Latif, "An adaptive digital image watermarking scheme using fuzzy logic and Tabu search," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, pp. 250-271, 2013.

[8] C. C. Lin, C. C. Chang, and Y. H. Chen, "A novel SVD-based watermarking scheme for protecting rightful ownership of digital images," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, pp. 124-143, 2014.

[9] R. Jafari, D. Ziou, and M. Mohammad, "Increasing image compression rate using steganography," *Expert Systems with Applications*, vol. 40, pp. 6918-6927, 2013.

[10] B. J. Mohd, S. Abed, and B. Na'ami, "Hierarchical steganography using novel optimum quantization technique," *Signal Image and Video Processing*, vol. 7, pp.1029-1040, 2013.

[11] J. S. Pan, W. Li, C. S. Yang, and L. Yan, "Image steganography based on subsampling and compressive sensing," *Multimedia Tools and Applications*, DOI 10.10071/s11042-014-2070-1.

[12] C.Y. Yang, "Use of radius weighted mean to hide data in colour images," *The 5th IET Int. Conf. on Ubi-Media Computing*, Xining, China, 16-18 August, pp. 248-252, 2012.

[13] A. Ioannidou, S. T. Halkidis, and G. Stephanides G, "A novel technique for image steganography based on a high payload method and edge detection," *Expert System with Applications*, vol. 39, pp. 11517-11524, 2012.

[14] J. K. Mandal and D. Das, "Colour image steganography based on pixel value differencing in spatial domain," *Int. Journal of Information Science and Techniques*, vol. 2, pp. 83-93, 2012.

[15] W. M. Abduallah, A. M. S. Rahma, and A. S. K. Pathan, "Mix column transform based on irreducible polynomial mathematics for color image steganography: a novel approach," *Computers and Electrical and Engineering*, vol. 40, pp. 1390-1404, 2014.