Reversible Color Image Steganographic Scheme based on Shape-specific point
(植基於圖型特徵點之可逆式彩色影像隱寫術)

Ching-Yu Yang
Dept. of Comp. Sci. and Inform. Eng., National Penghu University of Science and Technology, Taiwan
No 300, Liu-Ho Rd., Magong, 880 Penghu, Taiwan
chingyu@npu.edu.tw

Wen-Fong Wang
Dept. of Comp. Sci. and Inform. Eng., National Yunlin University of Science and Technology, Taiwan
No 123, University Rd., Section 3, Douliou, 64002 Yunlin, Taiwan
wwf@yuntech.edu.tw

楊慶裕
國立澎湖科技大學資工系
880 澎湖縣馬公市六合路 300 號
chingyu@npu.edu.tw

王文楓
國立雲林科技大學資工系
64002 雲林縣斗六市大學路 3 段 123 號
wwf@yuntech.edu.tw

摘要

植基於兩個圖型特徵點:半徑加權均值(RWM)和中心值(Centroid),本文使用 RWM 模設計出一個可逆式彩色影像隱寫技巧。換言之，我們使用區塊 RWM 模辨別策略，可有效的將祕密位元嵌入主體影像，並於接收端從標示影像無失真取出；而且可完全回復主體影像內容。值得一提的是本法也具備某種程度之強韌性質 (此特性是大多數傳統影像隱寫術所無法達到的)。實驗結果顯示本法產生的視覺品質不錯且具中等隱藏容量。使用本法產生的標示影像可抵抗彩色量化、(邊緣)銳化、高斯/均勻雜訊添加、像素反向、JPEG、JPEG 2000 和風阻等攻擊。也就是說，我們從被攻擊過的標示影像中所取出的版權圖像(或標誌)仍可識別。

關鍵字: 資料隱藏、可逆式彩色影像隱寫術、RWM 模、秘密通訊

Abstract

A reversible steganographic method for color images using two shape-specific points, namely, radius-weighted mean (RWM) and centroid is proposed. To embed data bits in a host block, the decision policy of the Euclidean norm of RWM (RWM-norm) is employed in the proposed method. The proposed method can restore host images after bit extraction with a certain degree of robustness. Simulations confirmed that the resultant perceived quality was

good, while hiding capacity was moderate. Marked images generated by the proposed method could resist various attacks such as color quantization, (edge) sharpening, Gaussian/uniform noise addition, inversion, JPEG and JPEG 2000 compression, and winding attacks.

Keyword: Data Hiding, Reversible Color Image Steganography, RWM-norm, Covert Communications

I. Introduction

Because of the ubiquitous nature of computer networks, economic use of broadband services, and the maturity of Internet Protocol version 6 smart devices, information appliances, surveillance devices, and mobile devices can be connected via internetworking techniques. People can easily share resources or monitor controlled devices over the Internet. However, there is significant risk that data may be eavesdropped, falsified, or tampered with during transmission. In this context, data hiding has recently come to play a pivotal role in securing important (or private) data. In general, data-hiding methods can be divided into two categories: steganography or digital watermarking [1][2][3]. Steganographic methods [4][5][6] emphasize high capacity while maintaining good perceived quality. In contrast to these advantages, robustness against versatile manipulations from attackers is a key performance criterion for watermarking approaches [7][8][9]. Because certain host media such as medical, satellite, and geophysical images are highly confidential, several reversible data-hiding techniques have been proposed [10]–[16]. The proposed method is a reversible data-hiding technique; only studies directly related to this technique are surveyed here.

Ni et al. [10] developed a robust lossless data-hiding technique based on the patchwork theory, the distribution features of pixel groups, error codes, and the permutation scheme. Although the payload size of this technique does not exceed 1,024 bits, the resulting images contain no salt-and-pepper noise and the resulting peak signal-to-noise ratio (PSNR) exceeds 38 dB. Zeng et al. [11] designed a lossless and robust data-hiding method that embedded data bits into blocks by shifting the mathematical difference values of a block. Based on k-means clustering and histogram shifting techniques, Tseng and Ding [12] proposed a reversible data-hiding scheme for color images. By exploiting the histogram of the difference between a pixel and its group center (or the palette), a secret message could effectively be embedded in a host image. Yang et al. [13] used prediction errors of the color difference domain and designed an effective lossless data-hiding algorithm for mosaic images. Simulations showed that this type of algorithm could provide a high payload and good image quality for several types of mosaic images. However, the algorithm is not feasible for real color images.

Boato et al. [14] combined difference expansion and prediction techniques in the spatial and S-transform domains and presented a high-capacity reversible data-hiding scheme. Simulations showed that this approach allows for a high resultant payload and good perceived quality. Efimushkina et al. [15] utilized the rate-distortion theory and Lagrangian formulation to process a reversible watermarking approach for JPEG images. Experimental results

indicated that their method enables hiding performance that is effective and comparatively better than existing reversible data-hiding methods for JPEG images. Based on prediction-error expansion and channel-correlation, Li et al. [16] presented a reversible data-hiding scheme for color images. Their method outperforms traditional reversible data-hiding techniques by improving prediction accuracy and considering overflow/underflow issues.

The remainder of this paper is organized as follows. Section II briefly reviews the radius-weighted mean (RWM) and centroid, as well as their distributions in RGB color space. Section III describes the bit embedding and bit extraction procedures. Section IV presents simulation results, and conclusions are given in Section V.

II. Review of Shape-specific Points

The RWM is a special type of point originally introduced by Mitiche and Aggarwal for shape matching [17] and has thereafter been used to detect rotationally symmetric shape orientations [18]. From Refs. [17][18], it can be seen that both the centroid and RWM are shape-specific points (SSP) of the systems. Note that the position of an SSP of a set is relatively unchanged (relative to the given point) if the set is translated, rotated, and scaled. In other words, the positions of the centroid and RWM are both relatively unchanged when the coordinates axes are translated, rotated, and scaled. Since the RWM of a set is less affected by an unbalanced population and a fast way for bisection, the RWM was subsequently employed to generate block truncation coding for real-time compression [19]. Furthermore, using SSPs for quantization of color images enables generation of a suitable color palette [20], and an effective steganographic method for color images based on SSPs has been proposed [21]. In this study, we have applied the notion of SSPs to our proposed reversible steganographic scheme.

Here, $S = \{(r_i, g_i, b_i) \mid i = 1,2,..., MN\}$ is the 3D data set, which is used to hide a secret message in a color (host) image of size $M \times N$. Two SSPs, the RWM $R = (r', g', b')$ and the centroid $O = (\bar{r}, \bar{g}, \bar{b})$ of the RGB color system are defined as follows:

$$r' = \left[\sum_{i=1}^{MN} \mu_i r_i\right] \Big/ \left[\sum_{i=1}^{MN} \mu_i\right], \tag{1}$$

$$g' = \left[\sum_{i=1}^{MN} \mu_i g_i\right] \Big/ \left[\sum_{i=1}^{MN} \mu_i\right], \tag{2}$$

$$b' = \left[\sum_{i=1}^{MN} \mu_i b_i\right] \Big/ \left[\sum_{i=1}^{MN} \mu_i\right], \tag{3}$$

Where

$$\mu_i = \sqrt{\left[(r_i - \bar{r})^2 + (g_i - \bar{g})^2 + (b_i - \bar{b})^2\right]}, \tag{4}$$

$$\bar{r} = \left[\sum_{i=1}^{MN} r_i\right] \Big/ MN, \tag{5}$$

$$\bar{g} = \left[\sum_{i=1}^{MN} g_i\right] \Big/ MN, \tag{6}$$

and

$$\bar{b} = \left[\sum_{i=1}^{MN} b_i\right] \Big/ MN. \tag{7}$$

The 3D distributions of the “Lena” and “Baboon” images with their compressed 3D versions are shown in Figs. 1 and 2, respectively. The centroid and the RWM are marked by “+” and “×,” respectively. Their corresponding 3D coordinates are also shown at the bottom of Figs. 1 and 2. Figure 1(b) shows the 3D distribution of the “Lena” image compressed by JPEG 2000 with a compression ratio (CR) of 101. Figure 1(b) shows a distribution similar to that shown in Fig. 1(a). Figure 2(b) indicates the 3D distribution of the “Baboon” image compressed by JPEG with a CR of 48. As can be seen, Figs. 2(a) and (b) also share similar characteristics. From the above description, we therefore employed the RWM in this study.

III. Proposed Method

The important details regarding bit embedding and bit extraction for the proposed method using RWM norm are presented in the following subsections.

1. Bit Embedding

As shown in Fig. 3, with $n = 3$, let $H_j = \{(r_{kj}, g_{kj}, b_{kj})\}_{k=0}^{n^2-1}$ be the j-th block of size $n \times n$ taken from a host image. In addition, let $H_j = \hat{I} \cup \tilde{I}$ with

$$\hat{I} = \{(r_{ij}, g_{ij}, b_{ij}) \mid i = 0,2,4,6,8\} \tag{8}$$

and

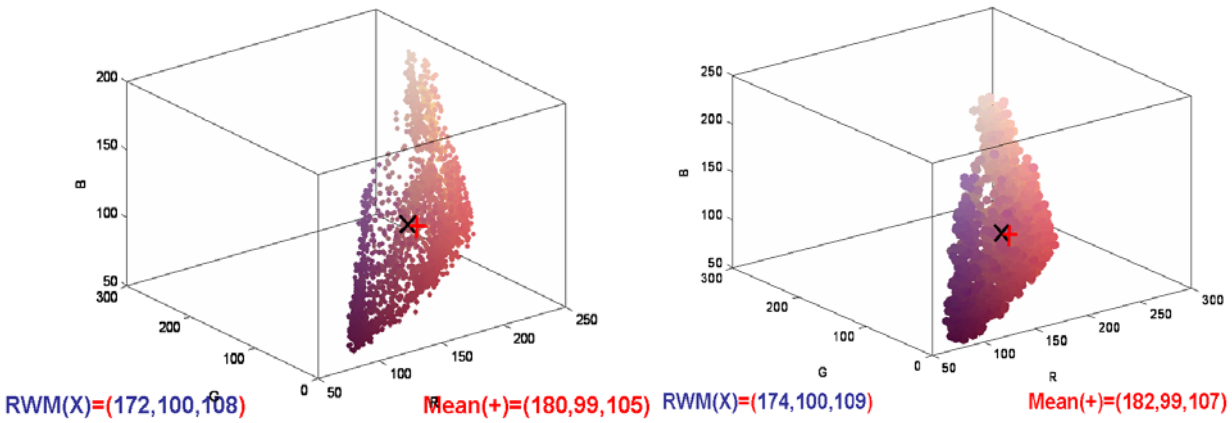
$$\tilde{I} = \{(r_{tj}, g_{tj}, b_{tj}) \mid t = 1,3,5,7\}. \tag{9}$$

Let $RWM_x = (\hat{r}', \hat{g}', \hat{b}')$ and $RWM_d = (\tilde{r}', \tilde{g}', \tilde{b}')$ be the RWM computed from $\hat{I}$ and $\tilde{I}$, respectively. The Euclidean norm of RWM_x and RWM_d are defined by

$$\| RWM_x \| = \sqrt{(\hat{r}')^2 + (\hat{g}')^2 + (\hat{b}')^2} \tag{10}$$

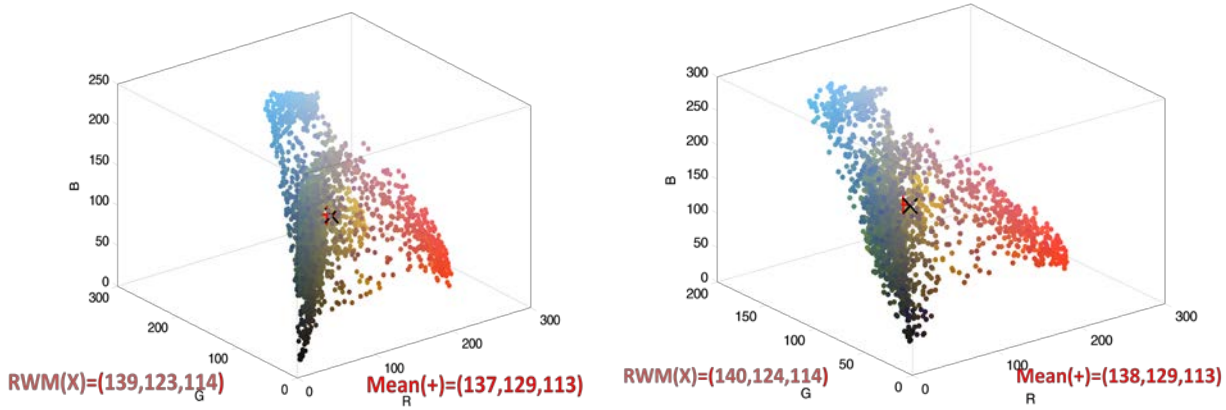
and

$$\| RWM_d \| = \sqrt{(\tilde{r}')^2 + (\tilde{g}')^2 + (\tilde{b}')^2}. \tag{11}$$



(a) (b)

Figure 1: 3D distribution of the "Lena" image: (a) original and (b) compressed by JPEG 2000 with CR = 101



(a) (b)

Figure 2: 3D distribution of the "Baboon" image: (a) original and (b) compressed by JPEG with CR = 48

$(r_{0j}g_{0j}b_{0j})$	$(r_{1j}g_{1j}b_{1j})$	$(r_{2j}g_{2j}b_{2j})$
$(r_{3j}g_{3j}b_{3j})$	$(r_{4j}g_{4j}b_{4j})$	$(r_{5j}g_{5j}b_{5j})$
$(r_{6j}g_{6j}b_{6j})$	$(r_{7j}g_{7j}b_{7j})$	$(r_{8j}g_{8j}b_{8j})$

Figure 3: A 3 × 3 block taken from a host image

In addition, let the block map $B = \{\beta_{ij} \mid i < \lfloor M/n \rfloor, j < \lfloor N/n \rfloor\}$ with $\beta_{ij} \in \{'0','10','11'\}$. The major steps of bit embedding are described as follows.

Step 1. Input a block H_j derived from the j-th non-overlapping block of a host image. If the end of the input is encountered, proceed to Step 4.

Step 2. If an input bit $\phi_r = 1$, perform the following sub-steps.

Step 2.1. If $\| RWM_x \| > | RWM_d \|$ is satisfied, set bit "0" to the corresponding mark β_{ij} of the block map *B* and repeat from Step 1; otherwise, increase (r_{ij}, g_{ij}, b_{ij}) in $\hat{I}$ by the δ value and compute $\| RWM_x \|$ again.

Step 2.2. If $\| RWM_x \| > | RWM_d \|$ is satisfied, set bits "10" to β_{ij} and repeat from Step 1; otherwise, undo the above increment, set bits "11" to β_{ij} (i.e., the skipped blocks) and repeat from Step 1.

Step 3. If an input bit $\phi_r = 0,$ perform the following sub-steps.

Step 3.1. If $\| RWM_x \| < \| RWM_d \|$ is satisfied, set bit "0" to β_{ij} and return to Step 1; otherwise, increase (r_{tj}, g_{tj}, b_{tj}) in $\tilde{I}$ by the δ value and compute $\| RWM_d \|$ again.

Step 3.2. If $\| RWM_x \| < \| RWM_d \|$ is satisfied, set bits "10" to β_{ij} and repeat from Step 1; otherwise, undo the above increment, set bits "11" to β_{ij}, and proceed to Step 1.

Step 4. Stop.

The term δ is a control integer. To avoid overflow, an input host block is immediately skipped if there is a pixel within a block whose value is greater than $255 - \delta$.

Two 1D numeric examples (Figs. 4 and 5) illustrate the proposed bit embedding. Here, the value of the control paramter δ was 2. Each example has three different host blocks, i.e., H1, H2, and H3. Figure 4(a) shows that host block H1 that requires no adjustment, which means that the block carries data bit "1" when an input data bit $\phi_r = 1$. According to Step 2.1, the target pixels (with shadow) in Fig. 4(b) of the host block H2 must be adjusted because $\phi_r = 1$ and $\| RWM_x \| < \| RWM_d \|$. The target pixels (with border line) resulting from successful pixel adjustment are shown in Fig. 4(c), i.e., the hidden block (of H2). The mean square error (MSE) computed between Figs. 4(b) and (c) was 4. However, a failed adjustment was encountered in Fig. 4(d) of the host block H3, which is a skipped block. Note that the pixels in the block remain intact. A similar example with three host blocks (H4, H5, and H6) is shown in Fig. 5, assuming that an input data bit $\phi_r = 0$.

1	1	2
2	3	1
4	2	5

(a)

1	4	2
5	3	4
4	5	5

(b)

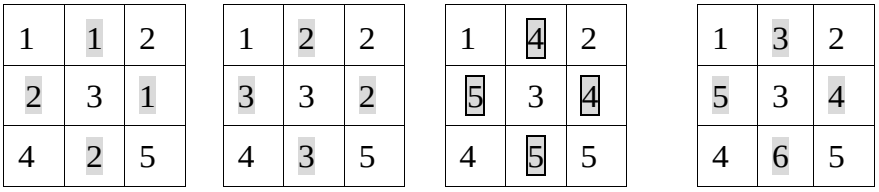
3	4	4
5	5	4
6	5	7

(c)

1	6	2
7	3	6
4	7	5

(d)

Figure 4: Examples of three host blocks when the input data bit is "1": (a) $\| RWM_x \| = 4 > \| RWM_d \| = 1.5,$ no adjustment is required for the block H1; (b) the host block H2 with $\| RWM_x \| = 4 < \| RWM_d \| = 4.5,$ target pixels (with shadow) must be increased by 2; (c) the hidden block successfully generated from (b), i.e., $\| RWM_x \| = 6 > \| RWM_d \| = 4.5,$ MSE = 4; and (d) the host block H3 is a skipped block (due to adjustment failure)



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

Figure 5: Examples of three host blocks while the input data bit is "0": (a) due to adjustment failure, the host block H4 was marked as a skipped block; (b) the host block H5 with $\| RWM_x \| = 4 > \| RWM_d \| = 2.5$, target pixels (with shadow) must be increased by 2; (c) the hidden block successfully generated from (b), i.e., $\| RWM_x \| = 4 < \| RWM_d \| = 4.5$, MSE = 4; and (d) $\| RWM \|_x = 4 < \| RWM \|_d = 4.5$, no adjustment is required for the host block H6

2. Bit Extraction

Let $H'_j = \{(r_{kj}, g_{kj}, b_{kj})\}_{k=0}^{n^2-1}$ be the *j*-th hidden block taken from a marked image. In addition, let $H'_j = \hat{I}' \cup \tilde{I}'$ with $\hat{I}' = \{(r_{ij}, g_{ij}, b_{ij}) \mid i = 0,2,4,6,8\}$ and $\tilde{I}' = \{(r_{tj}, g_{tj}, b_{tj}) \mid t = 1,3,5,7\}$. Let $\| RWM_{x'} \|$ and $\| RWM_{d'} \|$ be the Euclidean norm of the RWM computed from $\hat{I}'$ and $\tilde{I}'$, respectively. The bit extraction procedure is described in the following.

Step 0. Read in parameter δ and block map $B = \{\beta_{ij} \mid i < \lfloor M/n \rfloor, j < \lfloor N/n \rfloor\}$.

Step 1. Input a hidden block from a marked image. If the end of the input is encountered, proceed to Step 5.

Step 2. If the corresponding mark $\beta_{ij} =$'11', return to Step 1 (the skipped blocks).

Step 3. If $\| RWM_{x'} \| > \| RWM_{d'} \|$ is satisfied, data bit "1" is extracted, and the following sub-step is performed.

Step 3.1. If $\beta_{ij} =$'0,' return to Step 1; otherwise, decrease pixels (r_{ij}, g_{ij}, b_{ij}) in $\hat{I}'$ by the δ value and return to Step 1.

Step 4. If $\| RWM_{x'} \| < \| RWM_{d'} \|$ is satisfied, data bit "0" is extracted, and the following sub-step is performed.

Step 4.1. If $\beta_{ij} =$'0,' return to Step 1; otherwise, decrease pixels (r_{tj}, g_{tj}, b_{tj}) in $\tilde{I}'$ by the δ value and return to Step 1.

Step 5. Assemble all extracted bits, form the watermark, and restore the original image.

Step 6. Stop.

Flow charts of the proposed method are shown in Fig. 6. In the proposed method, bits "0," "10," and "11" are required to mark hidden blocks without offset adjustment, hidden blocks

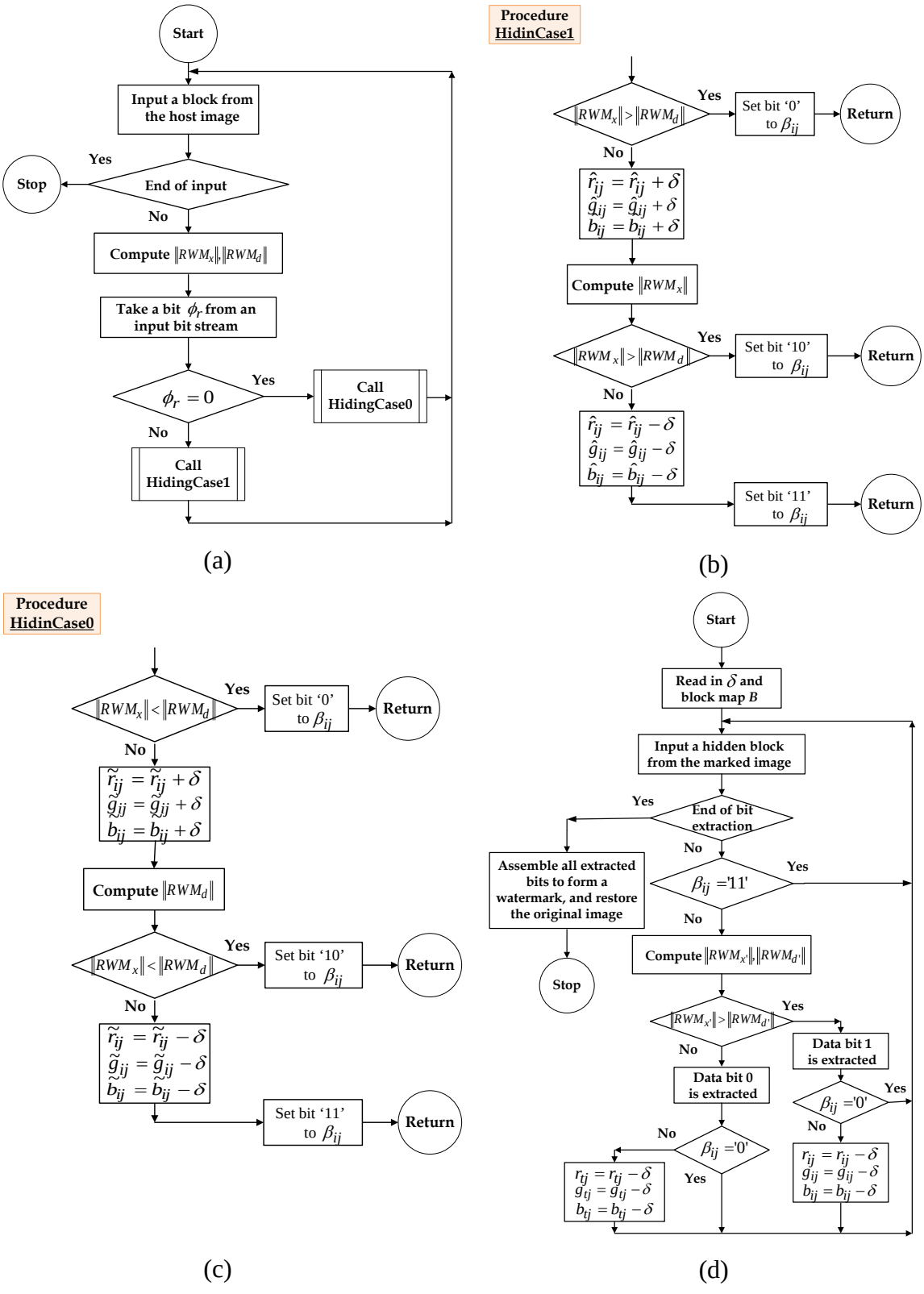


Figure 6: Flow charts: (a) main bit embedding procedure, (b) HidingBit1 procedure, (c) HidingBit0 procedure, and (d) main bit extraction procedure

with offset adjustment, and skipped blocks in bit embedding, respectively. This leads to the total number of overhead bits N_k+2(N_p+N_s), where N_k, N_p, and N_s are the number of hidden blocks without offset adjustment, the number of hidden blocks with offset

adjustment, and the skipped blocks, respectively. At the receiver, bit extraction would fail without overhead information. To help the receiver extract the hidden message, auxiliary information can be sent to the receiver by an out-of-band transmission. However, to save transmission time, overhead bits can be compressed by JBIG2 [22] prior to transmission.

IV. Experimental Results

n our experiments, several 512 × 512 color images were used as host images. Each RGB pixel of the host images is represented by 24 bits with 8 bits per component. A 180 × 180 binary watermark was used as test data. Several marked images generated by the proposed scheme are shown in Fig. 7. In addition, the resultant PSNR/payload and the control offset for the test images are given in Table 1. The PSNR is defined as follows:

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE}, \tag{12}$$

where $MSE = \frac{1}{3MN} \sum_{i=1}^{MN} \left[(r_i - \hat{r}_i)^2 + (g_i - \hat{g}_i)^2 + (b_i - \hat{b}_i)^2 \right]$ Here, (r_i, g_i, b_i) and $(\hat{r}_i, \hat{g}_i, \hat{b}_i)$ denote the RGB pixel values of the host images and the marked image, respectively. From Table 1 and Fig. 7, it is evident that although the resultant PSNR is moderate, the perceived quality is good. The “Tiffany” image comprises many “bright” blocks, i.e., a large number of pixel values on the R-/G-channel are close to 255. Therefore, to minimize distortion and increase hiding capacity, only the B-channel of the “Tiffany” image was employed in offset adjustment. The tradeoff between PSNR and payload for the test images is depicted in Fig. 8, which shows that the proposed method can hide data bits with a larger payload in the “House,” “Splash,” and “Couple” images and with the lowest hiding capacity in the “Baboon” image. The rest of the images provide a payload of approximately 27 Kb with a PSNR of approximately 35 dB. Furthermore, the optimal payload for the “Tiffany” image is approximately 14 Kb. This image demonstrates the largest PSNR among the images used.

For comparison, several lossless data-hiding approaches are compared with the proposed method. Table 2 shows that the PSNR performance of the method proposed by Tseng et al. [12] is the best among the compared methods. The scheme proposed by Boato et al. [14] demonstrates the greatest payload and the smallest average PSNR. In general, marked images with poor quality tend to attract hackers (or adversaries). The average payload of the proposed method is greater than that obtained by the method proposed by Efimushkina et al. [15], and the PSNR is comparable. Although the three compared approaches [12][13][16] provided good perceptual quality with high payload, their data-hiding approaches are fragile. Extraction of the hidden messages failed even if only a slight alteration was imposed on the marked images. In addition, avoidance of underflow/overflow (U/O) issues is not considered

by two of the methods [12][13]. Consequently, severe distortion in the resulting perceived quality was generated when U/O issues occurred during bit embedding. In contrast, the host images were fully recovered by the proposed method after bit extraction if the marked images remained intact. If the marked images are attacked by third parties (or hackers), it is not possible for the proposed method to restore the host images; however, it can extract hidden watermarks. Furthermore, the proposed method is free of U/O issues.

Table 1: PSNR, payload, control offset, and auxiliary information

Images	PSNR	Payload†	Offset	Overhead
Lena	33.58	28,110	7	45,310
Jet	35.26	28,011	8	46,377
Peppers	34.88	27,919	9	44,177
Baboon	35.93	24,836	9	44,189
House	34.62	28,761	8	48,300
Tiffany	34.98	27,023	15	45,846
Scene	35.03	27,301	9	44,309
Splash	34.95	28,695	8	46,960
Couple	35.74	28,768	7	48,529
Garden	35.35	27,602	8	46,361
Average	35.03	27,703	-	46,036

†Payload contains no auxiliary information.

Table 2: Payload and PSNR comparison of existing reversible steganographic techniques

Images	Payload/ PSNR			
	Ref. [12]*	Ref. [14]	Ref. [15]†	Our method!
Lena	57,862/49.64	382,730/27.54	14,048/36.20	28,110/33.58
Baboon	41,973/49.64	285,737/18.80	N/A	24,836/35.93
Peppers	75,996/49.81	343,409/25.71	15,079/34.60	27,919/34.88
Jet	89,597/50.37	N/A+	N/A	28,011/35.26
Average	66,357/49.87	337,292/24.02	14,564/35.40	27,219/34.91

*Block size is 32 × 32.
†Simulations were employed with optimization.
+Not available.
!Overhead information was not included in the payload.

A comparison of the proposed method and existing watermarking techniques is shown in Table 3. The proposed method clearly provides the greatest payload and achieves better PSNR than the existing techniques [8][10][11]. The scheme proposed by Yang et al. [9] has the best PSNR among the compared methods; however, its payload size is only approximately half

that of the proposed method. Both the proposed method and the method proposed by Yang et al. [9] employ SSPs in data hiding; however, they differ in two major aspects. (1) Yang et al. focused on achieving (lossy) digital watermarking with high-perceptual quality, whereas, the proposed approach is a (lossless) steganographic method with moderate hiding capacity. As mentioned in the Introduction the design goals in steganography and digital watermarking are very distinct. (2) To promote robustness, Yang et al. used the Euclidean distance between the centroid and RWM with the Euclidean distance between the target pixels and the centroid of the block as their decision policy during bit embedding. It is obvious that the kernel component of bit embedding and bit extraction in the scheme proposed by Yang et al. is quite different from the proposed method.

Table 3: Payload/ PSNR comparison of various methods

Images	Payload/ SNR				
	Ni et al. [10]	Zeng et al. [11]	Yang [8]*!	Yang et al. [9]!	Our method!
Lena	24,576/42.20	16,384/38.07	24,576/42.18	14,803/58.23	25,565/44.78
Zelda	24,576/43.50	16,384/38.09	24,576/42.20	11,238/58.20	27,854/43.43
Goldhill	24,576/42.63	16,384/38.10	24,576/43.50	12,275/57.43	27,162/47.14
Average	5,717/40.28	16,384/38.09	24,576/42.63	12,772/57.95	26,861/45.12

*With Yang's robust watermarking approach.
!Overhead information was not included in the payload.

To validate the robustness of the proposed method (Tables 4 and 5), a binary watermark of size 167 × 167 was used as test data. The extracted watermarks and their bit correct ratio (BCR) were included. The tested marked images were generated by the proposed method using $\delta = 7$ for the "Lena" image. The BCR is defined as follows:

$$BCR = \left(\sum_{i=0}^{ab-1} \overline{w_i \oplus \tilde{w}_i} \Big/ a \times b \right) \times 100\%, \tag{13}$$

where w_i and $\tilde{w}_i$ are the values of the original watermark and the extracted watermark, respectively, and where the size of a watermark is $a \times b$. Table 4 shows that the marked images generated by the proposed method can resist various attacks, and the extracted watermarks can still be recognized. Note that the BCR for the extracted watermark (manipulated by inversion) is only 4.78% and is recognizable. Moreover, to show that the proposed method is tolerant to versatile manipulations, a demonstration with a different binary watermark of size 167 × 167 is given in Table 5. As can be seen, all extracted watermarks are recognizable.

V. Conclusion

Based on the decision policy of the RWM-norm in the host blocks, we have presented a simple reversible steganographic scheme for color images. Typically, a hidden watermark can be extracted in a lossless manner from a marked image, and the host image can be completely restored. If the marked images are attacked by third parties (or hackers), the host images are not recoverable. However, the extracted watermarks can be recognized using the proposed method. Our experimental results show that the perceptual quality of the proposed method is good and the hiding capacity is moderate. Furthermore, marked images generated by the proposed method are robust against several attacks such as blurring, brightness, color quantization, contrast, (edge) sharpening, cropping, equalization, Gaussian/uniform noise addition, inversion, JPEG and JPEG 2000 compression, plastic-wrap, posterization, rough pastels, surface blurring, and winding attacks. Note that a reversible steganographic method equipped with a certain degree of robustness is not common among traditional reversible data-hiding techniques.

References

[1] Cox, I.J., Miller, M.L., Bloom, J.A., Fridrich, J. and Kalker, T., D*igital watermarking and steganography*, 2nd Ed., Morgan Kaufmann., MA, 2008.

[2] Phadikar, A. *Data hiding techniques and applications specific designs*, LAP LAMBERT Academic Publishing, Saarbrucken, 2012.

[3] Raggo, M. and Hosmer, C. *Data hiding: exposing concealed data in multimedia, operating systems, mobile devices and network protocols*, *Elsevier*, MA, 2013.

[4] Qu, Z.G., Chen, X.B., Zhou, X.J., Niu, X.X. and Yang, Y.X., "Novel quantum steganography with large payload", *Optics Communications* (283:13), 2010: pp. 4782-4786.

[5] Wang, S., Yang, B. and Niu, X., "A secure steganography method based on genetic algorithm", *Journal of Information Hiding and Multimedia Signal Processing* (1:1), 2010: pp. 28-35.

[6] Eielinska, E., Mazurczyk, W. and Szczypiorski, K., "Trends in steganography", *Communications of the ACM* (57:3), 2014: pp. 86-95.

[7] Niu, P.P., Wang, X.Y., Yang, Y.P. and Lu, M.Y., "A novel color image watermarking scheme in nonsampled contourlet-domain", *Expert Systems with Applications* (38:3), 2011: pp. 2081-2098.

[8] Yang, C.Y., "Robust watermarking scheme based on radius weight mean and feature-embedding technique", *ETRI Journal* (35:3), 2013: pp. 512-522.

[9] Yang, C.Y., Wang, W.F., Wang, Y.F. and Wang, R.Z., "A simple watermarking scheme with high perceptual quality for still color imaged based on RWM and centroid", *Journal of Information Hiding and Multimedia Signal Processing* (6:3), 2015: pp. 577-90.

[10] Ni, Z., Shi, Y.Q., Ansari, N., Su, W., Sun, Q. and Lin, X., "Robust lossless image data hiding designed for semi-fragile image authentication", *IEEE T. Circuits and Systems for Video Technology* (18:4), 2008: pp. 497-509.

[11] Zeng, X.T., Ping, L.D. and Pan, X.Z., "A lossless robust data hiding scheme", *Pattern Recognition* (43:4), 2010: pp. 1656-67.

[12] Tseng, H.W. and Ding, W.B., "Reversible data hiding scheme for color images based on pixel clustering and histogram shifting", *The Imaging Science Journal* (60:1) 2012: pp. 47-53.

[13] Yang, W.J., Chung, K.L. and Liao, H.Y.M., "Efficient reversible data hiding for color filter array images", *Information Science* (190:1), 2012: pp. 208-26.

[14] Boato, G., Carli, M., Battisti, F., Azzoni, M. and Egiazarian, K., "Difference expansion and prediction for high bit-rate reversible data hiding", *Journal of Electronic Imaging* (21:3), 2012: doi: 033013-1-9.

[15] Efimushkina, T., Egiazarian, K. and Gabbouj, M., "Rate-distortion based reversible watermarking for JPEG images with quality factors selection", *European Workshop on Visual Information Processing* (EUVIP 2013), Paris, France, June 10-12, 2013: pp. 94-99.

[16] Li, J., Li, X. and Yang, B., "Reversible data hiding scheme for color image based on prediction-error and cross-channel correlation", *Signal Processing* (93:9), 2013: pp. 2748-58.

[17] Mitiche, A. and Aggarwal, J.K., "Contour registration by shape-specific point for shape matching", *Computer Vision, Graphics Image Processing* (22:3), 1983: pp. 396-408.

[18] Lin, J.C., Chou, S.L. and Tsai, W.H., "Detection of rotationally symmetric shape orientations by fold-invariant shape-specific points", *Pattern Recognition* (25:5), 1992: pp. 473-82.

[19] Yang, C.Y. and Lin, J.C., "EBTC: An economical method for searching the threshold of BTC compression", *Electronics Letters* (32:20), 1996: pp. 1870-1.

[20] Yang, C.Y. and Lin, J.C., "RWM-cut for color image quantization", *Computer & Graphics* (20:4), 1996: pp. 577-88.

[21] Yang, C.Y., "Use of radius weighted mean to hide data in colour images", *The 5th IET Int. Conf. on U-Media Comp*., August 16-18, Xining, China, 2012: pp. 248-52.

[22] Howard, P.G., Kossentini, F., Martins, B., Forchhammer, S. and Rucklidge, W.J., "The emerging JBIG2 standard", *IEEE T. Circuits and Systems for Video Technology* (8:7), 1998: pp. 838–848.

[23] Cox, I.J., Miller, M.L., Bloom, J.A., Fridrich, J. and Kalker, T., D*igital watermarking and steganography*, 2nd Ed., Morgan Kaufmann., MA, 2008.

[24] Phadikar, A. *Data hiding techniques and applications specific designs*, LAP LAMBERT Academic Publishing, Saarbrucken, 2012.

[25] Raggo, M. and Hosmer, C. *Data hiding: exposing concealed data in multimedia, operating systems, mobile devices and network protocols*, *Elsevier*, MA, 2013.

[26] Qu, Z.G., Chen, X.B., Zhou, X.J., Niu, X.X. and Yang, Y.X., "Novel quantum steganography with large payload", *Optics Communications* (283:13), 2010: pp. 4782-4786.

[27] Wang, S., Yang, B. and Niu, X., "A secure steganography method based on genetic algorithm", *Journal of Information Hiding and Multimedia Signal Processing* (1:1), 2010: pp. 28-35.

[28] Eielinska, E., Mazurczyk, W. and Szczypiorski, K., "Trends in steganography", *Communications of the ACM* (57:3), 2014: pp. 86-95.

[29] Niu, P.P., Wang, X.Y., Yang, Y.P. and Lu, M.Y., "A novel color image watermarking scheme in nonsampled contourlet-domain", *Expert Systems with Applications* (38:3), 2011: pp. 2081-2098.

[30] Yang, C.Y., "Robust watermarking scheme based on radius weight mean and feature-embedding technique", *ETRI Journal* (35:3), 2013: pp. 512-522.

[31] Yang, C.Y., Wang, W.F., Wang, Y.F. and Wang, R.Z., "A simple watermarking scheme with high perceptual quality for still color imaged based on RWM and centroid", *Journal of Information Hiding and Multimedia Signal Processing* (6:3), 2015: pp. 577-90.

[32] Ni, Z., Shi, Y.Q., Ansari, N., Su, W., Sun, Q. and Lin, X., "Robust lossless image data hiding designed for semi-fragile image authentication", *IEEE T. Circuits and Systems for Video Technology* (18:4), 2008: pp. 497-509.

[33] Zeng, X.T., Ping, L.D. and Pan, X.Z., "A lossless robust data hiding scheme", *Pattern Recognition* (43:4), 2010: pp. 1656-67.

[34] Tseng, H.W. and Ding, W.B., "Reversible data hiding scheme for color images based on pixel clustering and histogram shifting", *The Imaging Science Journal* (60:1) 2012: pp. 47-53.

[35] Yang, W.J., Chung, K.L. and Liao, H.Y.M., "Efficient reversible data hiding for color filter array

images", *Information Science* (190:1), 2012: pp. 208-26.

[36] Boato, G., Carli, M., Battisti, F., Azzoni, M. and Egiazarian, K., "Difference expansion and prediction for high bit-rate reversible data hiding", *Journal of Electronic Imaging* (21:3), 2012: doi: 033013-1-9.

[37] Efimushkina, T., Egiazarian, K. and Gabbouj, M., "Rate-distortion based reversible watermarking for JPEG images with quality factors selection", *European Workshop on Visual Information Processing* (EUVIP 2013), Paris, France, June 10-12, 2013: pp. 94-99.

[38] Li, J., Li, X. and Yang, B., "Reversible data hiding scheme for color image based on prediction-error and cross-channel correlation", *Signal Processing* (93:9), 2013: pp. 2748-58.

[39] Mitiche, A. and Aggarwal, J.K., "Contour registration by shape-specific point for shape matching", *Computer Vision, Graphics Image Processing* (22:3), 1983: pp. 396-408.

[40] Lin, J.C., Chou, S.L. and Tsai, W.H., "Detection of rotationally symmetric shape orientations by fold-invariant shape-specific points", *Pattern Recognition* (25:5), 1992: pp. 473-82.

[41] Yang, C.Y. and Lin, J.C., "EBTC: An economical method for searching the threshold of BTC compression", *Electronics Letters* (32:20), 1996: pp. 1870-1.

[42] Yang, C.Y. and Lin, J.C., "RWM-cut for color image quantization", *Computer & Graphics* (20:4), 1996: pp. 577-88.

[43] Yang, C.Y., "Use of radius weighted mean to hide data in colour images", *The 5th IET Int. Conf. on U-Media Comp*., August 16-18, Xining, China, 2012: pp. 248-52.

[44] Howard, P.G., Kossentini, F., Martins, B., Forchhammer, S. and Rucklidge, W.J., "The emerging JBIG2 standard", *IEEE T. Circuits and Systems for Video Technology* (8:7), 1998: pp. 838–848.

(a)

(b)

(c)

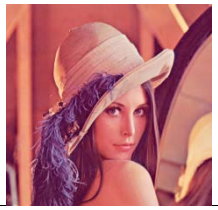
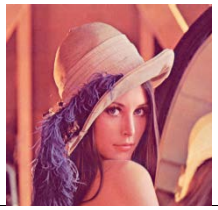
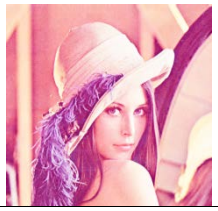
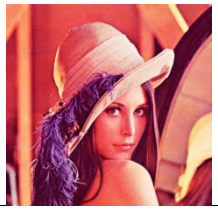
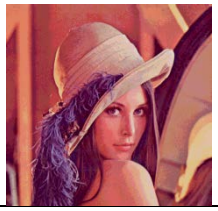
(d)

(e)

(f)

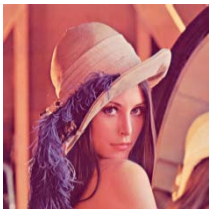
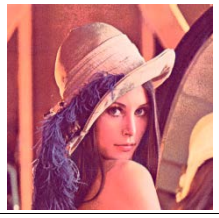
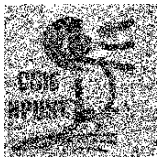
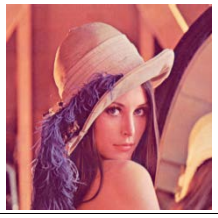
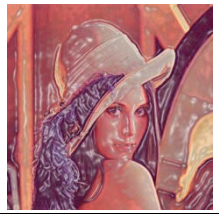
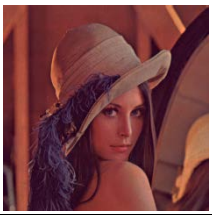
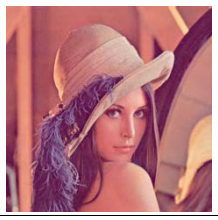
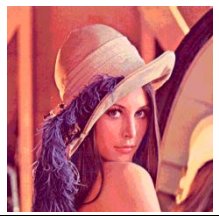
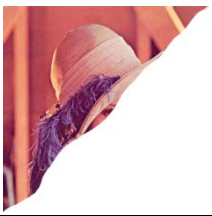
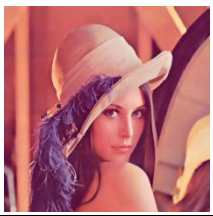
Figure 7: Marked images generated by the proposed reversible watermarking scheme: (a) "Lena," (b) "Jet," (c) "Peppers," (d) "Baboon," (e) "House," and (f) "Tiffany"

Table 4: Examples of watermarks from the proposed reversible watermarking scheme that survived manipulations of the marked “Lena” image

Attacks	Manipulated Stego-images	Survived Watermarks	Attacks	Manipulated Stego-images	Survived Watermarks
Null-attack BCR=100%			Inversion BCR = 4.78%		
JPEG 2000 (CR=17) BCR = 72.09%			Equalized BCR = 95.79 %		
JPEG (CR=5) BCR = 68.27%			Sharpening BCR = 92.07 %		
uniform-noise (10%) BCR = 72.57%			Edge-sharpening BCR = 98.48 %		
Gaussian-noise (7%) BCR = 69.39%			Brightness (100%) BCR= 92.45%		
Poterized (16-palette) BCR = 86.60 %			Contrast (100%) BCR= 96.12%		
Truncation† BCR= 75.55%			Winding BCR= 79.70%		

†The last five bits of the stego-pixel were truncated.

Table 5: Additional examples of extracted watermarks that survived manipulations of the marked “Lena” image

Attacks	Manipulated Stego-images	Survived Watermarks	Attacks	Manipulated Stego-images	Survived Watermarks
Null-attack BCR=100%			Filter-gallery BCR = 71.03%		
Blurring BCR = 85.48%			Plastic-wrap BCR = 87.59 %		
Brightness (-100%) BCR = 91.91%			Rough-pastels BCR = 73.79 %		
Contrast (-50%) BCR = 95.07%			Posterized (8-palette) BCR = 73.81 %		
Cropping (~50% off) BCR = 62.47%			Surface-blur. BCR= 75.26%		

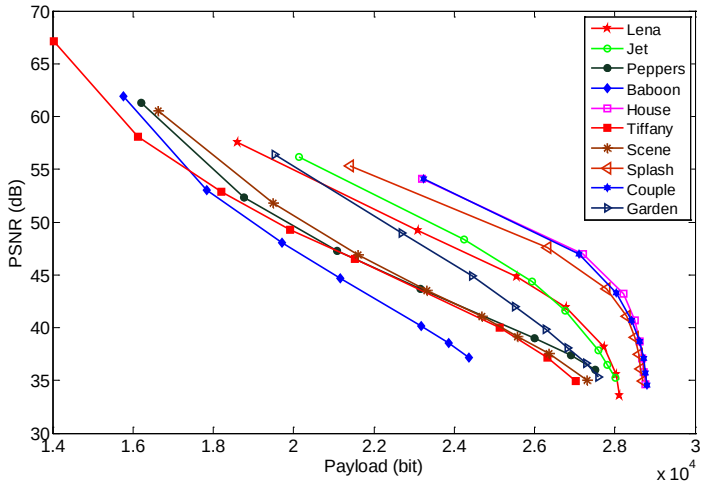


Figure 8: Tradeoff between PSNR and payload

78 Reversible Color Image Steganographic Scheme based on Shape-specific point