

A Simple Watermarking Scheme with High Perceptual Quality for Still Color Images Based on RWM and Centroid

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

Yih-Fuh Wang

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

Ran-Zan Wang

Department of Computer Science and Information Engineering
Yuan Ze University
135 Yuan-Tung Rd., Chung-Li, Taiwan 320
rzwang@saturn.yzu.edu.tw

Received May, 2014; revised September, 2014

ABSTRACT. *This study presents a robust watermarking scheme with high perceived quality for still color images. More specifically, based on spatial domain, the proposed watermarking scheme employed the idea of the Euclidean distance of radius-weighted mean (RWM) and centroid that can effectively embed data bits in host images. Simulations demonstrate that the marked images generated by the proposed watermarking scheme are tolerant of versatile attacks such as color reduction, compression, cropping, lens-blurring, noise addition, and so on. Above all, the extracted watermarks are recognized when the marked images are compressed by JPEG2000 with a CR of 517. Moreover, the proposed scheme can resist from 27% Uniform-noise and 17% Gaussian-noise addition attacks. Due to the resultant perceived quality is good, the third parties may not aware of existence of secret message hidden in the marked images.*

Keywords: Robust color image watermarking scheme, RWM, Centroid, Euclidean distance of RWM and centroid

1. Introduction. The fast growth of information technology and development of communication protocols allows individuals and organizations to exchange and share resources through the Internet at a low cost. Examples of these applications are cloud computing, multimedia communications, and transactions for electronic commerce. Because of out-of-date platforms or lack of maintenance, information systems become vulnerable and prone to being compromised by third parties (or hackers). Furthermore, data could be eavesdropped, tampered with, and falsified during transmission. Therefore, the protection and security of private messages during an inter-exchange is vital. In addition to data encryption/decryption systems, data hiding provides an alternative but economic way to secure data. Data hiding can be classified into two categories: steganography and digital watermarking [1]–[3]. A major application of the steganographic approaches can be found in covert communications between two parties or among the anonymous organizations. As for the popular usages of watermarking schemes are copyright protection, proof of ownership, and content authentication.

Steganographic approaches often exhibit high capacity and high perceived quality. The main advantage of digital watermarking is its robustness against manipulations. Because color images are commonly used and are popularly circulated worldwide, several authors have presented data hiding schemes for color images [4]–[12]. Among them, certain researchers have developed steganographic methods to hide numerous data bits in the host images, while maintaining high perceived quality [4, 5, 10].

Based on linear discriminant analysis, Fu and Shen [6] suggested a watermarking scheme for color images. Both the true watermark and the reference watermark were embedded simultaneously into a RGB color image. Simulations confirmed that the scheme was capable of resisting several attacks. Findik et al. [7] used particle swarm optimization and the k-nearest neighbor algorithm to suggest a novel color image watermarking scheme. Their experimental results showed that the marked images were tolerant to various image processing attacks when the payload was 4,096 bits. With the same payload size, Findik et al. [8] further applied the notion of the artificial immune recognition system to develop an effective watermarking technique. They embedded a watermark and a predetermined k-bit binary stream into the B-component of a RGB color space. The extracted watermarks survived attacks such as noise additions, blurring, and sharpening. To further promote robust performance, Niu et al. [9] developed a new color image watermarking scheme based on super vector regression (SVR) and nonsubsampled contourlet transform (NSCT). Simulations indicated that the scheme is robust against geometric distortions and certain image processing operations. However, the time complexity of the scheme is high during SVR training and NSCT process. Based on state coding and an integer wavelet transform (IWT) domain, Su et al. [11] presented a robust watermarking scheme for color images. First, a host image with an RGB color space is converted to the YCbCr system. Three components are then transformed by the level 1 IWT. Subsequently, data bits are embedded into the low-frequency coefficients of the IWT domain. A watermark is hidden in the low-low, low-high, and high-low sub-subbands of the three transformed components. Based on the spatial domain, Yang [12] integrated the RWM and feature-embedding technique, and presented a novel watermarking scheme and a steganographic scheme for color images. Simulations demonstrated that the marked images generated by the watermarking scheme are robust against a variety of manipulations.

The remainder of this paper is organized as follows. Section 2 reviews Yang's scheme [12]. Section 3 describes the proposed robust watermarking scheme and overhead analysis. Section 4 presents the simulation results and the comparisons of performance, and Section 5 provides the conclusion.

2. Related Work. Yang [12] presents a robust watermarking scheme based on the radius-weighted mean (RWM) decision policy with X-/directional-sampling. Two data bits can be embedded into a host block if both X-/directional-samplings were employed together. A host block may contain only one data bit if either X-sampling or directional-sampling was used. However, if none of the samplings are utilized, the block contains no data bits. For clarity, only the bit embedding stage is presented here, while the bit extraction one is omitted.

$(r_{0j}g_{0j}b_{0j})$	$(r_{1j}g_{1j}b_{1j})$	$(r_{2j}g_{2j}b_{2j})$	$(r_{3j}g_{3j}b_{3j})$
$(r_{4j}g_{4j}b_{4j})$	$(r_{5j}g_{5j}b_{5j})$	$(r_{6j}g_{6j}b_{6j})$	$(r_{7j}g_{7j}b_{7j})$
$(r_{8j}g_{8j}b_{8j})$	$(r_{9j}g_{9j}b_{9j})$	$(r_{10j}g_{10j}b_{10j})$	$(r_{11j}g_{11j}b_{11j})$
$(r_{12j}g_{12j}b_{12j})$	$(r_{13j}g_{13j}b_{13j})$	$(r_{14j}g_{14j}b_{14j})$	$(r_{15j}g_{15j}b_{15j})$

FIGURE 1. A 4×4 block taken from the RGB color image.

First, a host color image is divided into non-overlapping $n \times n$ blocks. Then, to embed data bits into a host block, the RWM decision policy with X-/directional-sampling is employed. Both samplings consist of one half $n \times n$ pixels in a block. Let $C_j = \{(r_{kj}, g_{kj}, b_{kj})\}_{k=0}^{n^2-1}$ be the j th host block, as shown in Fig. 1 (when $n = 4$), and $C_j = \hat{C} \cup \tilde{C}$ with $\hat{C} = \{(r_{ij}, g_{ij}, b_{ij}) \mid i = 0, 3, 5, 6, 9, 10, 12, 15\}$, and $\tilde{C} = \{(r_{tj}, g_{tj}, b_{tj}) \mid t = 1, 2, 4, 7, 8, 11, 13, 14\}$. Also let $\|OR\|$ and $\|c_{kj}O\|$ represent the Euclidean distance between the centroid O and the RWM R , as well as the pixels c_{kj} and O with $c_{kj} \in C_j$. The RWM decision policy with X-sampling can be represented by the two formulas: $\hat{\Omega}_1 = \{\hat{c}_{lj} \mid \|\hat{c}_{lj}O\| \leq h \|OR\|, \hat{c}_{lj} \in \hat{C}\}$ and $\hat{\Omega}_2 = \{\hat{c}_{mj} \mid \|\hat{c}_{mj}O\| > h \|OR\|, \hat{c}_{mj} \in \hat{C}\}$ with $\hat{C} = \hat{\Omega}_1 \cup \hat{\Omega}_2$. Note that h is a control parameter. Similarly, the RWM decision policy with directional-sampling is calculated by $\tilde{\Omega}_1 = \{\tilde{c}_{lj} \mid \|\tilde{c}_{lj}O\| \leq h \|OR\|, \tilde{c}_{lj} \in \tilde{C}\}$ and $\tilde{\Omega}_2 = \{\tilde{c}_{mj} \mid \|\tilde{c}_{mj}O\| > h \|OR\|, \tilde{c}_{mj} \in \tilde{C}\}$ with $\tilde{C} = \tilde{\Omega}_1 \cup \tilde{\Omega}_2$. Bit embedding of Yang's scheme is described in the following algorithm.

Algorithm 1. Hiding data bits in a RGB color image.

Input: A host color image $S = \{(r_i, g_i, b_i) \mid i = 1, 2, \dots, MN\}$, an input watermark W , and three integers h, η and λ .

Output: A marked image, the RWM R , the centroid O , and a block map B .

- Step 0:** Compute O and R of S , and the Euclidean distance $\|OR\|$ of O and R , respectively.
- Step 1:** Input a block C_j , which derived from S . If the end of input is encountered, then proceed to Step 5.
- Step 2:** Obtain one data bit δ' from W , and perform the following sub-steps:
- Step 2.1:** If $\delta' = 1$ and $|\hat{\Omega}_2| > |\hat{\Omega}_1|$, then do nothing—data bit 1 can be carried by X-sampling without altering the pixels' value, and proceed to Step 3.
- Step 2.2:** If $\delta' = 1$ and $|\hat{\Omega}_2| \leq |\hat{\Omega}_1|$, then increase the value of color pixels in $\hat{\Omega}_1$ repeatedly by λ value until either $|\hat{\Omega}_2| > |\hat{\Omega}_1|$ or times η is encountered.
- Step 2.3:** If times η is encountered, then undo the above pixel-value-increment, and proceed to Step 3.
- Step 2.4:** If $\delta' = 0$ and $|\hat{\Omega}_2| \leq |\hat{\Omega}_1|$, then do nothing—data bit 0 can be carried by X-sampling without altering the pixels' value, and proceed to Step 3.
- Step 2.5:** If $\delta' = 0$ and $|\hat{\Omega}_2| > |\hat{\Omega}_1|$, then reduce the value of color pixels in $\hat{\Omega}_2$ repeatedly by λ value until either $|\hat{\Omega}_2| \leq |\hat{\Omega}_1|$ or η times is encountered.
- Step 2.6:** If times η is encountered, then undo the above pixel-value-decrement.
- Step 3:** Obtain the next data bit δ'' from W , and perform the following sub-steps:
- Step 3.1:** If $\delta'' = 1$ and $|\tilde{\Omega}_2| > |\tilde{\Omega}_1|$, then do nothing—data bit 1 can be carried by X-sampling without altering the pixels' value, and proceed to Step 4.
- Step 3.2:** If $\delta'' = 1$ and $|\tilde{\Omega}_2| \leq |\tilde{\Omega}_1|$, then increase the value of color pixels in $\tilde{\Omega}_1$ repeatedly by λ value until either $|\tilde{\Omega}_2| > |\tilde{\Omega}_1|$ or times η is encountered.
- Step 3.3:** If times η is encountered, then undo the above pixel-value-increment, and proceed to Step 4.
- Step 3.4:** If $\delta'' = 0$ and $|\tilde{\Omega}_2| \leq |\tilde{\Omega}_1|$, then do nothing—data bit 0 can be carried by X-sampling without altering the pixels' value, and proceed to Step 3.
- Step 3.5:** If $\delta'' = 0$ and $|\tilde{\Omega}_2| > |\tilde{\Omega}_1|$, then reduce the value of color pixels in $\tilde{\Omega}_2$ repeatedly by λ value until either $|\tilde{\Omega}_2| \leq |\tilde{\Omega}_1|$ or η times is encountered.
- Step 3.6:** If times η is encountered, then undo the above pixel-value-decrement.
- Step 4:** Set a mark 0 to the corresponding position of block map B if only X-sampling is used; set 1 to that of B if only directional-sampling is used; set 2 to that of B if both samplings are used; and set 3 to that of B if neither X-sampling nor directional-sampling were used, and return to Step 1.
- Step 5:** Stop.

3. The Proposed Robust Watermarking Scheme. The procedures of bit embedding and bit extraction for the proposed method are specified in the following subsections.

3.1. Data Embedding. Without loss of generality, let $P_j = \{(r_{kj}, g_{kj}, b_{kj})\}_{k=0}^{n^2-1}$ be the j th block of size $n \times n$ taken from a host image. $\|OR\|$ represents the Euclidean distance between the centroid O and the RWM R , and $\|p_{kj}O\|$ represents the Euclidean distance between the pixel p_{kj} and O with $p_{kj} \in P_j$. In addition, let

$$\Omega_1 = \{p_{lj} \mid \|p_{lj}O\| < \tau \|OR\|, p_{lj} \in P_j\} \quad (1)$$

and

$$\Omega_2 = \{p_{mj} \mid \|p_{mj}O\| \geq \tau \|OR\|, p_{mj} \in P_j\} \quad (2)$$

be the two subsets of P_j with $P_j = \Omega_1 \cup \Omega_2$, where τ is a control parameter. The major steps for data embedding are summarized as follows:

- Step 1:** Input a block P_j , which is the j th non-overlapping block derived from a host image. If the end of input is encountered, proceed to Step 4.
- Step 2:** If an input bit $\phi_l = 1$, perform the following sub-steps:
- Step 2.1:** If $|\Omega_1| > |\Omega_2|$ is satisfied, nothing is done (which meaning the block carries data bit 1); set 1 to the corresponding position of the block map B , and repeat from Step 1.
- Step 2.2:** Decrease repeatedly the three components in p_{mj} by the λ value each time until either $|\Omega_1| > |\Omega_2|$ or the number of times η is encountered.
- Step 2.3:** If $|\Omega_1| > |\Omega_2|$ is satisfied, set 1 to the corresponding position of B , otherwise, set 0 to the corresponding position of B , and repeat from Step 1.
- Step 3:** If an input bit $\phi_l = 0$, perform the following sub-steps:
- Step 3.1:** If $|\Omega_1| \leq |\Omega_2|$ is satisfied, nothing is done (which meaning the block carries data bit 0); set 1 to the corresponding position of B , and repeat from Step 1.
- Step 3.2:** Increase repeatedly the three components in p_{lj} by the λ value each time until either $|\Omega_1| \leq |\Omega_2|$ or the number of times η is encountered.
- Step 3.3:** If $|\Omega_1| \leq |\Omega_2|$ is satisfied, set 1 to the corresponding position of B , otherwise, set 0 to the corresponding position of B , and repeat from Step 1.
- Step 4:** Stop.

In Steps 2 and 3, both η and λ are two control integers. Note that if a block fails to hide a data bit, the block is skipped. The skipped blocks, which are marked by 0 in the corresponding position of B , contain no data bits.

3.2. Data Extraction. Data extraction for the proposed robust watermarking scheme is much simpler than data embedding. Let $Q_j = \{(r_{kj}, g_{kj}, b_{kj})\}_{k=0}^{n^2-1}$ be the j th hidden block taken from a marked image. Also let $\Omega'_1 = \{q_{lj} \mid \|q_{lj}O\| < \tau \|OR\|, q_{lj} \in Q_j\}$ and $\Omega'_2 = \{q_{mj} \mid \|q_{mj}O\| \geq \tau \|OR\|, q_{mj} \in Q_j\}$ be the two subsets of Q_j with $Q_j = \Omega'_1 \cup \Omega'_2$. The major steps of data extraction are specified as follows:

- Step 0:** Read in the RWM, centroid, λ , η , and the 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 input is encountered, proceed to Step 3.
- Step 2:** If the corresponding mark β_{ij} , i.e., the block contains no data bit return to Step 1; otherwise, perform the following sub-steps:
- Step 2.1:** If $|\Omega'_1| > |\Omega'_2|$ is satisfied, data bit 1 is extracted, and return to Step 1.
- Step 2.2:** If $|\Omega'_1| \leq |\Omega'_2|$ is satisfied, data bit 0 is extracted, and return to Step 1.
- Step 3:** Assemble all the extracted bits and form the watermark.
- Step 4:** Stop.

3.3. Overhead Analysis. The number of overhead bit for the proposed robust watermarking scheme is $\lfloor MN/n^2 \rfloor$, where the size of the block and host image are $n \times n$ and $N \times N$, respectively. Although the overhead is larger than the payload, both robustness and security can be obtained by the proposed scheme. Because a marked image and its overhead can be separately transmitted to the receiver. If the marked image is seized by third parties (or hackers), it is very hard for them to extract the hidden message (or watermark) without having the overhead information. Compared with conventional watermarking techniques, which embed a secret message with overhead into a host image, our method provides a better way to secure data. To save space and transmission time, the overhead information can be losslessly compressed using run-length coding or JBIG2 [13] algorithms before transmission.

4. 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 block size is 3×3 . Theoretically, the maximum payload for the proposed two methods is $\lfloor \frac{512}{3} \rfloor \times \lfloor \frac{512}{3} \rfloor \leq 28,900$ bits. To demonstrate the performance of the proposed robust watermarking scheme, a binary watermark with size 120×120 is used as the test data. The marked images generated by the proposed scheme using various τ and η are depicted in Figs. 2 and 3. The value of parameter λ is set to 1. Figure 2 indicates tradeoff between the PSNR and payload (in bits) for the proposed scheme. Except ‘Baboon,’ most of images provide above 16 Kb with the PSNR around 44 dB. However, the PSNR for ‘Tiffany’ is around 49 dB. In addition, Fig. 3 shows that the perceived quality is good. No apparent color distortion is observed in the marked images. Further, the resultant PSNR is high. The PSNR (dB) are 48.84 for ‘Lena,’ 44.30 for ‘Jet,’ 48.73 for ‘Peppers,’ 39.28 for ‘Baboon,’ 48.04 for ‘House,’ and 47.36 for ‘Tiffany,’ respectively. All of the marked images provide payload of size 14,400 bits. The PSNR is defined by

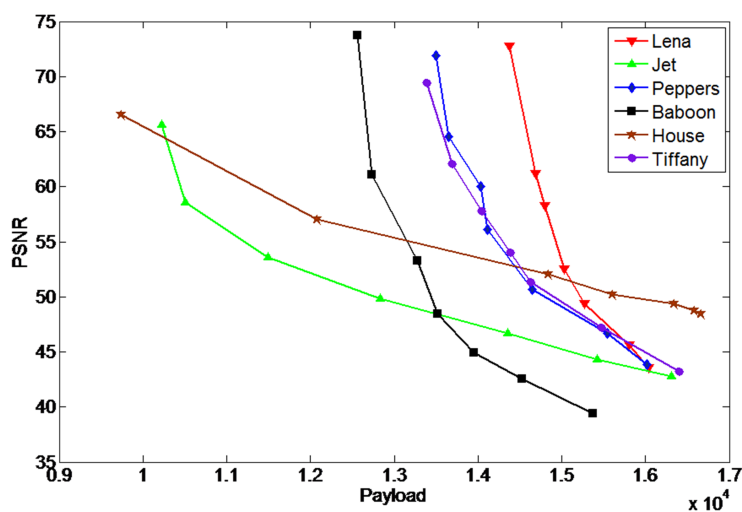


FIGURE 2. Tradeoff between the PSNR and payload for the proposed robust watermarking scheme on the test images.

TABLE 1. Demonstrations of survived watermarks.





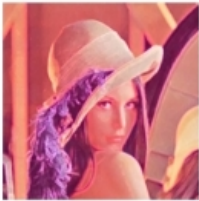



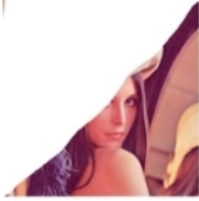



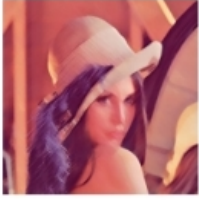



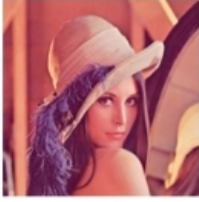



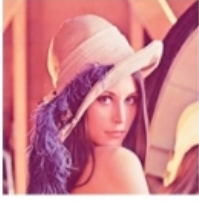



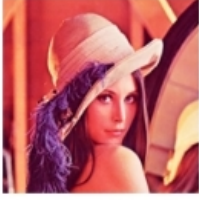



Attacks	Manipulated Images	Survived Watermarks	Attacks	Manipulated Images	Survived Watermarks
Null-attack BCR=100%			Cross-hatch BCR=83.98%		
Accented-edge BCR=74.26%			Crystallized BCR=84.65%		
Anti-diagonal-cropping (50%) BCR=59.56%			Diagonal-cropping (50%) BCR=65.22%		
Angle-stroke BCR=85.42%			Diffusing BCR=92.69%		
Blurring BCR=91.77%			Dry-brush BCR=86.39%		
Brightness (30%) BCR=68.41%			Edge-sharpen. BCR=97.59%		
Contrast (100%) BCR=69.54%			Equalized BCR=65.99%		

Table 1. (continued)








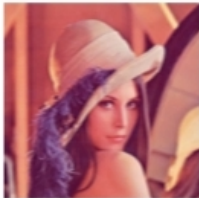



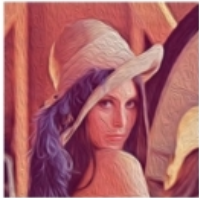























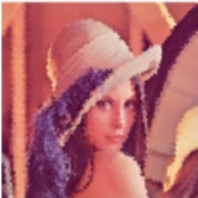




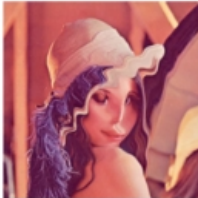

Attacks	Manipulated Images	Survived Watermarks	Attacks	Manipulated Images	Survived Watermarks
Facet BCR=90.80%			Liquify BCR=93.21%		
Film-grain BCR=71.40%			Mosaicking BCR=84.11%		
Gaussian-blurring BCR=89.85%			Motion-blur. BCR=87.87%		
Gaussian-noise (17%) BCR=49.81%			Oil-paint BCR=84.63%		
Grain BCR=76.04%			Ocean-ripple BCR=78.81%		
JPEG2000 (CR=517) BCR=84.57 %			Paint-daubs BCR=82.80%		
JPEG (CR=61) BCR=84.66%			Plastic-wrap BCR=85.79%		

Table 1. (continued)

Attacks	Manipulated Images	Survived Watermarks	Attacks	Manipulated Images	Survived Watermarks
Pointlized BCR=60.58%			Spray-stroke BCR=88.13%		
Posterized (8-palette) BCR=78.28%			Sumi-e BCR=56.63%		
Poster-edge BCR=85.71%			Texturizer BCR=81.10%		
Ripple BCR=89.91%			Truncation [†] BCR=86.96%		
Rough-pastels BCR=80.94%			Uniform-noise (27%) BCR=49.60%		
Spatter BCR=86.01%			Winding BCR=90.51%		
Sharpening BCR=93.80%			Zigzagging BCR=87.51%		

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \quad (3)$$

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

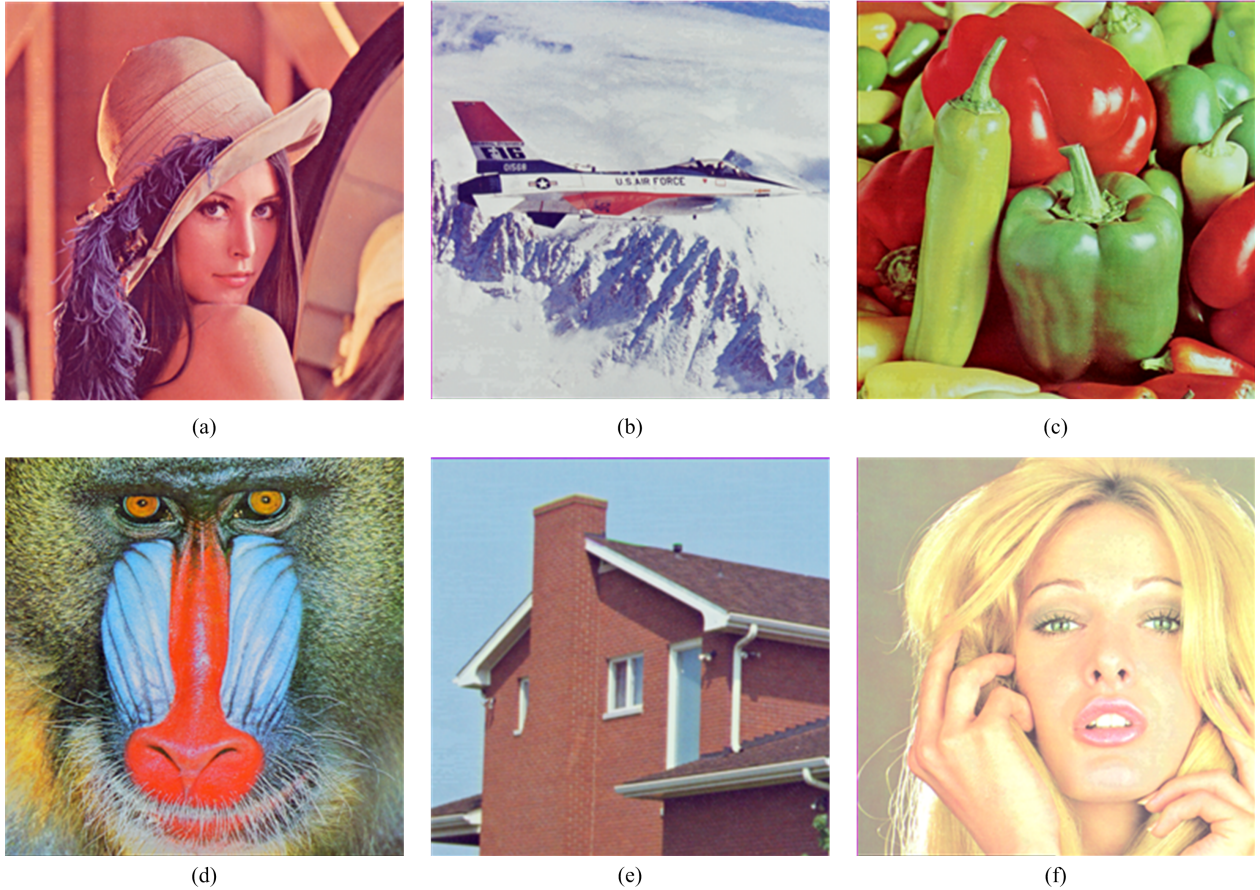


FIGURE 3. Marked images generated by the proposed robust watermarking scheme. (a) 'Lena' using $\tau = 9$ and $\eta = 9$, (b) 'Jet' using $\tau = 1$ and $\eta = 6$, (c) 'Peppers' using $\tau = 17$ and $\eta = 7$, (d) 'Baboon' using $\tau = 22$ and $\eta = 19$, (e) 'House' using $\tau = 13$ and $\eta = 7$, and (f) 'Tiffany' using $\tau = 3$ and $\eta = 7$.

To test the robustness of the proposed method, a variety of manipulations are performed to the marked images. All of the attacks given in Table 1 are manipulated by using two popular image processing tools: Adobe Photoshop [14] and FastStone Image Viewer [15] to the marked images. In Table 1, one of the attacks such as 'Uniform-noise (27%)' means that the marked image is manipulated by the uniform-distribution-noise addition with the amount of 27% of the size of a marked image. 'Gaussian-blurring' means that the manipulated image is introduced by a blurring operation via Gaussian function (also known as Gaussian smoothing), it is a widely used effect in graphics software, typically to reduce image noise and details. In addition, 'Cropping (50%)' means that the attacked image is introduced by cutting 50% of the original size. Due to space limitation, the specifications

of other attacks are skipped here.

The extracted watermarks and the bit correct ratio (BCR) are given in Table 1. The marked image is introduced by using $\tau = 8$, $\eta = 9$, and $\lambda = 1$, respectively, in ‘Lena’. The BCR is defined by

$$BCR = \left(\frac{\sum_{i=0}^{ab-1} \overline{w_i \oplus \tilde{w}_i}}{a \times b} \right) \times 100\% \quad (4)$$

where w_i and \tilde{w}_i represent the values of the original and extracted watermarks, respectively; the size of the watermark is $a \times b$. The BCR for an extracted watermark is 100% when a marked image is not manipulated. Most extracted watermarks are recognized. Although the BCR for certain watermarks that survived from the attacks such as craquelure, cropping, equalized, Gaussian-noise mosaic-tile, pointilized, sumi-e, and Uniform-noise are below 70%, they are recognizable. In addition, after a color reduction attack (posterized)—the number of colors in a marked image is intentionally reduced to a few representative colors (e.g., eight colors)—the extracted watermark is recognized. The survived watermark, which is compressed by JPEG at a CR of 61, is identified. Above all, the extracted watermark is still recognizable even as the marked image is compressed by JPEG2000 at a CR of 517. Moreover, the proposed scheme is capable of resisting large-scale noise-addition attacks, including 27% of Uniform-noise addition and 17% of Gaussian-noise addition attacks. After the above noise-addition attacks, the BCRs for the extracted watermarks are below 50%, they are recognized. It seems that the word “CSIE NPU” of survived watermarks such as JPEG, JPEG2000, noise-addition attacks, and sumi-e are hard to identified, however, the bird-like logo of extracted watermarks are still recognizable. This logo may play an important role of owner’s watermark and can be used to guard against manipulations from the third parties.

Performance comparison with various methods in terms of payload and PSNR is given in Table 2. Table 2 shows that the average PSNR for the proposed method is the best among these compared methods. Although the payload size for the approach of Su et al. [11] is superior to other schemes, the size of an input watermark is confined to 64×64 . The payload size of the proposed method provides a competitive hiding-capacity compared with that of Yang’s technique [12]. Notice as well our method requires only a half size of overhead used in Yang’s technique. The average hiding capacity for both the technique of Findik et al. [8] and the approach of Niu et al. [9] is only 1,024 bits, while their PSNR values are still less than ours. However, the Niu et al.’s scheme [9] has a good performance in resisting geometric attacks. Moreover, Table 3 presents the robustness of the compared methods in terms of attacks and their corresponding BCR values. Since the Findik et al.’s technique, Niu et al.’s scheme and Su et al.’s approach were capable of resisting limited sorts of attacks, their performance were not appeared in Table 3. Among the 13 given attack-items, the BCRs for Yang’s technique are larger than that for the proposed method on the 4 compared items. However, there are five compared items are not available for Yang’s technique. Other attacks such as accented-edge, angle-stroke, cross-hatch, crystal-lize, facet, liquefy, ocean-ripple, oil-paint, paint-daubs, plastic-wrap, poster-edge, rough-pastels, sumi-e and texturizer are not available for Yang’s technique. Figure 4 illustrates the BCRs of the extracted watermarks, which survive from Uniform-/Gaussian-noise addition attacks that are generated by our method and the Yang’s technique. Obviously,

TABLE 2. Payload (bit) and PSNR (dB) comparison with various methods.

Images	Payload (bit)/ PSNR (dB)				
	Findik, et al. [8]	Niu, et al. [9]	Su, et al. [11] ⁺	Yang [12] [*]	Our method
Lena	1,024/41.83	1,024/40.57	98,034/55.85	14,413/56.97	14,803/58.23
Baboon	1,024/42.75	1,024/41.67	98,034/55.85	13,172/55.25	12,849/58.02
Peppers	–	–	98,034/55.84	14,701/55.63	14,116/56.14
House	–	–	–	15,002/56.50	12,083/57.05
Jet	–	–	98,034/55.88	10,747/58.40	10,504/58.58
Tiffany	–	–	–	16,786/55.14	14,041/57.81
<i>Average</i>	1,024/42.29	1,024/41.12	98,034/55.86	13,952/56.54	12,669/57.95

⁺Using a 24-bit 8-color logo with size of 64×64 as the test watermark.

^{*}With the robust watermarking approach of Yang's technique.

Fig. 4 indicates the superiority of our method. From the above demonstration (Tables 1 and 3, and Fig. 4), we can say that the proposed robust watermarking scheme is tolerant of a variety of attacks. Above all, our method has good performance in resisting JPEG2000 compression with a high CR attack, and large-scale noise-addition attacks.

TABLE 3. BCR performance comparison between Yang's technique [12] and our method under various attacks.

Attacks	BCR	
	Yang [12]	Our method
Blurring	90.37%	91.77%
Contrast (+100%)	N/A [†]	90.65%
Cropping (50%)	N/A [†]	62.39%
Diffusing	79.30%	92.68%
Gaussian-noise (12%)	N/A [†]	74.56%
JPEG (CR=61) (50%)	85.59%	84.65%
JPEG2000 (CR=517)	N/A [†]	84.57%
Rippling	96.25%	89.91%
Sharpening	99.65%	93.80%
Sprayed	70.27%	88.13%
Uniform-noise (21%)	N/A [†]	70.88%
Winding	79.56%	90.51%
Zigzaging	89.43%	87.51%
Other attacks (accented-edge, angle-stroke, cross-hatch, crystalize, facet, liquefy, ocean-ripple, oil-paint, paint-daubs, plastic-wrap, poster-edge, rough-pastels, sumi-e, texturizer, etc.)	N/A [†]	(see Table 1)

[†]N/A: Not Available.

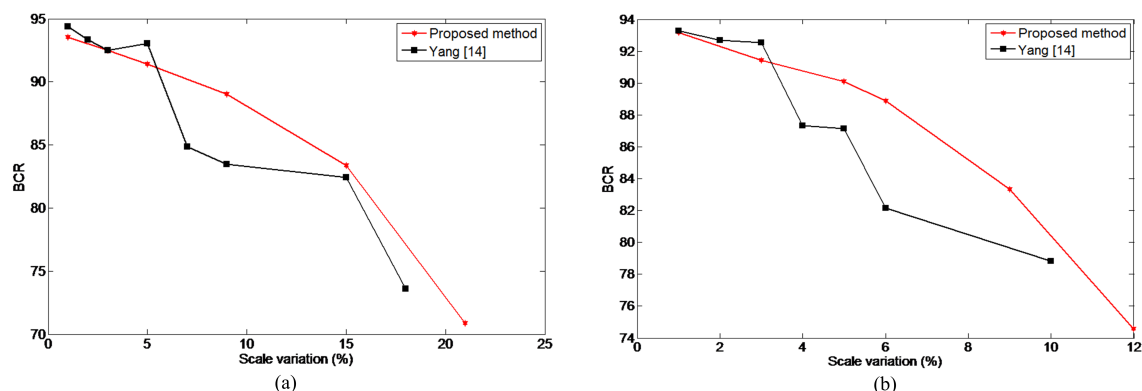


FIGURE 4. BCR comparison between Yang's technique [12] and the proposed method under noise-addition attacks: (a) Uniform-noise attack and (b) Gaussian-noise attack.

5. Conclusion. We presented an effective watermarking scheme for still color images based on the RWM and centroid. Simulations confirmed that the marked images generated by the proposed watermarking scheme were capable of resisting versatile manipulations, such as angle-stroke, color reduction, compression, cropping, noise addition, ocean-ripple, oil-paint, pixel-truncation, poster-edge, texturizer, winding, and zigzaging. Moreover, the proposed scheme exhibited an excellent performance in resisting high-CR JPEG2000 attacks. Further, the proposed scheme was tolerant to large-scale of Uniform-/Gaussian-noise attacks. These capabilities were rare in existing techniques. In addition, the PSNR generated by the robust watermarking scheme was superior to those generated by existing techniques while the payload was feasible. Some major applications of the proposed watermarking scheme can be found in copyright management and image authentication.

REFERENCES

- [1] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich and T. Kalker, *Digital Watermarking and Steganography*, Morgan Kaufmann, MA, 2008.
- [2] F. Y. Shih, *Digital Watermarking and Steganography: Fundamentals and Techniques*, FL: CRC Press, 2008.
- [3] A. Cheddad, J. Condell, K. Curran and P. M. Kevitt, Digital image steganography: survey and analysis of current methods, *Signal Processing*, vol. 90, no. 3, pp. 727-752, 2010.
- [4] L. Li and B. Luo, A color image steganography method by multiple embedding strategy based on sobel operator, *International Conference on Multimedia Information Network and Security*, vol. 2, pp. 118-121, 2009.
- [5] C. C. Chang, Y. H. Chen and C. C. Lin, A data embedding scheme for color images based on genetic algorithm and absolute moment block truncation coding, *Soft Computing*, vol. 13, no. 4, pp.321-331, 2009.
- [6] Y. G. Fu and R. M. Shen, Color image watermarking scheme based on linear discriminant analysis, *Computer Standards & Interface*, vol. 30, no.3, pp. 115-120, 2008.
- [7] O. Findik, I. Babaoglu and E. Ulker, A color image watermarking scheme based on hybrid classification method: particle swarm optimization and k-nearest neighbor algorithm, *Optics Communications*, vol. 283, no.24, pp. 4916-4922, 2010.
- [8] O. Findik, I. Babaoglu and E. Ulker, A color image watermarking scheme based on artificial immune recognition system, *Expert Systems with Applications*, vol. 38, no.3, pp. 1942-1946, 2011.

- [9] P. P. Niu, X. Y. Wang, Y. P. Yang, and M. Y. Lu, A novel color image watermarking scheme in nonsampled contourlet-domain, *Expert Systems with Applications*, vol. 38, no. 3, pp. 2081-2098, 2011.
- [10] C. Y. Yang, Use of radius weighted mean to hide data in colour images, *The 5th IET Int. Conf. on U-Media Comp.*, pp. 248-252, 2012.
- [11] Q. Su, Y. Niu, X. Liu, and Y. Zhu, A blind dual color images watermarking scheme based on IWT and state coding, *Optics Communications*, vol. 285, no. 7, pp. 1717-1724, 2012.
- [12] C. Y. Yang, Robut watermarking scheme based on radius weight mean and feature-embedding technique, *ETRI Journal*, vol. 35, no.3, pp. 512-522, 2013.
- [13] P. G. Howard, F. Kossentini, B. Martins, S. Forchhammer and W. J. Rucklidge, The emerging JBIG2 standard, *IEEE Trans. on Circuits and Systems for Video Technology* , vol. 8, no. 7, pp. 838-848, 2002.
- [14] <http://www.adobe.com/>, 2013.
- [15] <http://www.faststone.org/>, 2013.