Robust Watermarking Scheme Based on Radius Weight Mean and Feature-Embedding Technique

Ching-Yu Yang

In this paper, the radius weight mean (RWM) and the feature-embedding technique are used to present a novel watermarking scheme for color images. Simulations validate that the stego-images generated by the proposed scheme are robust against most common image-processing operations, such as compression, color quantization, bit truncation, noise addition, cropping, blurring, mosaicking, zigzagging, inversion, (edge) sharpening, and so on. The proposed method possesses outstanding performance in resisting high compression ratio attacks: JPEG2000 and JPEG. Further, to provide extra hiding storage, a steganographic method using the RWM with the least significant bit substitution technique is suggested. Experiment results indicate that the resulting perceived quality is desirable, whereas the peak signal-to-noise ratio is high. The payload generated using the proposed method is also superior to that generated by existing approaches.

Keywords: Robust watermarking algorithm, color image steganography, radius weighted mean, feature-embedding technique.

I. Introduction

Because of the practical use and interesting functionality of steganography and digital watermarking, numerous researchers have focused on data hiding [1], [2]. A major distinction between steganography and digital watermarking is that steganography is capable of providing a large payload with a perceived high quality [3], [4]. However, extracting the hidden message would fail, even with a slight alteration to the stego-images. A remarkable feature of digital watermarking is its tolerance of common image-processing operations [5], [6]. To demonstrate hiding performance, most authors use gray-level images as the test sample. However, the human eye is more sensitive to the change in color images than in grayscale images; therefore, a small color distortion (or false color contour) could appear on resulting images, which might attract the attention of third parties (or hackers). Hence, the security of the hidden message might be compromised.

To develop an effective data-hiding method for color images, several authors have presented their algorithms in the literature [7]-[11]. Yang [7] proposed a simple color image steganographic method based on three types of module substitution: Mod-u, Mod-v, and Mod-w. According to the base value of the blocks, various secret bits were effectively embedded into an RGB trichromatic system by module substitutions. The simulation results showed that the embedding rate provided by the method was high, whereas the resulting perceived quality was desirable. Fu and Shen [8] suggested a novel color image watermarking scheme based on linear discriminant analysis. Two watermarks, namely, the true watermark and the reference watermark, were embedded simultaneously into RGB color images. The simulations indicated the proposed scheme to be tolerant of several attacks.

Manuscript received July 15, 2012; revised Oct. 17, 2012; accepted Nov. 19, 2012.

Ching-Yu Yang (phone: +886 6926 4115 3502, chingyu@npu.edu.tw) is with the Department of Computer Science and Information Engineering, National Penghu University of Science and Technology, Penghu, Taiwan.

http://dx.doi.org/10.4218/etrij.13.0112.0480

Findik and others [9] used the notion of the artificial immune recognition system to develop an effective watermarking technique. The watermark and a predetermined *k*-bit binary stream were embedded into the B-component of an RGB system. The extracted watermarks survived such attacks as noise addition, blurring, and sharpening.

To further promote robustness performance, the researchers in [10], [11] proposed color image watermarking algorithms in transform domains, such as discrete cosine transform (DCT) and integer wavelet transform (IWT). Phadikar and Maity [10] used a quality access control scheme of color images and proposed a data-hiding method in the DCT domain. The secret messages were embedded in the C_b component of the YC_bC_r color space by using the spread spectrum technique. The simulations implied that the scheme provided a feasible quality access control for compressed color images. Based on state coding, Su and others [11] presented color image watermarking in the IWT domain. An RGB color host image was converted to the YC_bC_r system. The three components were then transformed by the level 1 IWT. Subsequently, data bits were embedded into the low-frequency coefficients of the IWT domain. A watermark could be hidden in the low-low, low-high, and high-low subbands of the three transformed components. The experiment results indicated that the stego-images were capable of resisting manipulations, and the resulting peak signal-to-noise ratio (PSNR) was desirable.

This paper proposes a robust watermarking scheme for color images based on the radius weight mean (RWM) and the feature-embedding technique. A steganographic method using the RWM with the least significant bit (LSB) substitution technique is subsequently presented to provide extra hiding storage. The remainder of this paper is organized as follows. The RWM is briefly reviewed in section II. The procedures for bit embedding and bit extraction of the proposed robust watermarking scheme are given in subsection III.1. The details of the encoding part and decoding part of the proposed steganographic method are described in subsection III.2. Overhead analysis is specified in subsection III.3. Simulation results are demonstrated in section IV. Finally, the conclusion is summarized in section V.

II. Review of RWM

In the new method, HH HHthe 3D RWM is employed in the proposed method to hide data bits in a color image $S = \{(r_i, g_i, b_i) \mid i = 1, 2, ..., MN\}$, where MN is the size of the image. The RWM is a special type of point (also known as a shape-specific point), originally introduced to register shapes [12], [13] and has thereafter been used to generate economic block truncation coding for real-time compression [14]. The RWM was subsequently used for color image quantization to generate a feasible palette [15]. 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.

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

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

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

where

$$\omega_i = \sum_{i=1}^{MN} \sqrt{\left[(r_i - \bar{r})^2 + (g_i - \bar{g})^2 + (b_i - \bar{b})^2\right]}, \tag{4}$$

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

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

and

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

III. Proposed Method

The main goal of Phase I of the proposed method is to design a robust watermarking approach for color images. Because several blocks may contain no data bits after the end of Phase I, a steganographic approach is presented to hide extra secret bits (or private data) in these blocks. Both approaches are related to the RWM. Notice that the proposed method can be divided into two procedures and independently performed in the RGB color systems. The details of (the two-phase version of) the proposed method are specified in the following subsections.

1. Robust Watermarking Approach

To provide a robust watermarking approach, each host block is embedded with at most two bits based on the RWM decision policy and feature-embedding technique. The feature-embedding technique consists of two procedures: the X-sampling technique and the directional-sampling technique. Specifically, two data bits can be embedded into a host block by using the X-sampling technique followed by the directional-sampling technique if neither technique violates the RWM decision

policy during bit embedding. A host block may contain only one data bit if either the X-sampling or the directional-sampling violates the RWM decision policy. However, if both techniques violate the RWM decision policy, then the block contains no data bits. The skipped blocks are later used in Phase II of the proposed steganographic approach. The details of the encoding part for the proposed watermarking approach are described below.

A. RWM Decision Policy

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 color image. In addition, let $\Omega_1 = \{p_{lj} \mid\mid p_{lj}O \mid\mid \le h \mid\mid OR \mid\mid, p_{lj} \in P_j\}$ and $\Omega_2 = \{p_{mj} \mid\mid p_{mj}O \mid\mid > h \mid\mid OR \mid\mid p_{mj} \in P_j\}$ be the two subsets of P_j with $P_j = \Omega_1 \cup \Omega_2$, where h is a control parameter. The Euclidean distance of (the color pixels in) P_j and O is represented by $\| P_jO \|$, and the Euclidean distance of O and R is represented by $\|OR\|$. To hide one data bit in a host block based on the RWM, the following decision policy is used. If an input bit is 1 and $|\Omega_2| \ge |\Omega_1|$, then do nothing, which means that the block "carries" data bit 1; otherwise, repeatedly increase p_{lj} by the λ value each time until either $|\Omega_2| > |\Omega_1|$ or times η is encountered. Both η and λ are integers. However, if an input bit is 0 and $|\Omega_2| \le |\Omega_1|$, then do nothing, which means that the block "carries" bit 0; otherwise, repeatedly reduce the pixels p_{mj} by the λ value each time until either $|\Omega_2| \le |\Omega_1|$ or η times is encountered. If a block fails to satisfy either $|\Omega_2| > |\Omega_1|$ or $|\Omega_2| \le |\Omega_1|$ after increment or decrement adjustment, then it is marked as a non-hidden block. To embed two bits into a host block, the proposed method employs the RWM decision policy with the X-sampling and directional-sampling techniques to achieve the goal.

B. Bit Embedding

Let $C_j = \{(r_{kj}, g_{kj}, b_{kj})\}_{k=0}^{n^2-1}$ be the j-th block of size $n \times n$ taken from a host color image, as shown in Fig. 1 (when n=4), and let $C_j = \hat{C} \cup \tilde{C}$ with $\hat{C} = \{(r_{ij}, g_{ij}, b_{ij}) \mid i = 0,3,5,6,9,10,12,15\}$ and $\tilde{C} = \{(r_{tj}, g_{tj}, b_{tj}) \mid t = 1,2,4,7,8,11,13,14\}$. In addition, let $\hat{\Omega}_1 = \{\hat{c}_{lj} \mid\mid \hat{c}_{lj}O \mid\mid \le h \mid\mid OR \mid\mid, \hat{c}_{lj} \in \hat{C}\}$ and $\hat{\Omega}_2 = \{\hat{c}_{mj} \mid\mid \hat{c}_{mj}O \mid\mid > h \mid\mid OR \mid\mid, \hat{c}_{mj} \in \hat{C}\}$ be the two subsets of $\hat{C}$ with $\hat{C} = \hat{\Omega}_1 \cup \hat{\Omega}_2$, and let $\tilde{\Omega}_1 = \{\mid\mid \tilde{c}_{lj}O \mid\mid \le h \mid\mid OR \mid\mid, \tilde{c}_{lj} \in \tilde{C}\}$ and $\tilde{\Omega}_2 = \{\tilde{c}_{mj} \mid \tilde{c}_{mj} \mid\mid\mid \tilde{c}_{mj}O \mid\mid > h \mid\mid OR \mid\mid, \tilde{c}_{mj} \in \tilde{C}\}$ be the two subsets of $\tilde{C}$ with $\tilde{C} = \tilde{\Omega}_1 \cup \tilde{\Omega}_2$. Bit embedding for the proposed method is specified in the following algorithm.

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

Fig. 1. 4×4 block taken from RGB color image.

Algorithm 1. Hiding data bits in RGB color image.

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

Output. A stego-image, the RWM R, the centroid O, and a block map M.

Method.

Step 0. Compute the centroid O and the RWM R of S, and the Euclidean distance $\| OR \|$ of O and R, respectively.

Step 1. Input a block C_j, 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 substeps.

Step 2.1. If δ'=1 and $|\hat{\Omega}_2| \ge |\hat{\Omega}_1|$, then do nothing, which means that data bit 1 can be carried by X-sampling without altering the pixel value, and proceed to Step 3.

Step 2.2. If δ'=1 and $|\hat{\Omega}_2| \le |\hat{\Omega}_1|$, then increase $\hat{c}_{lj}$ in $\hat{\Omega}_1$ repeatedly by λ value each time until either $|\hat{\Omega}_2| > |\hat{\Omega}_1|$ or times η is encountered, and proceed to Step 3.

Step 2.3. If δ'=0 and $|\hat{\Omega}_2| \le |\hat{\Omega}_1|$, then do nothing, which means that data bit 0 can be carried by X-sampling without altering the pixel value, and proceed to Step 3.

Step 2.4. If δ'=0 and $|\hat{\Omega}_2| > |\hat{\Omega}_1|$ then reduce $\hat{c}_{mj}$ in $\hat{\Omega}_2$ repeatedly by the λ value each time until either $|\hat{\Omega}_2| \le |\hat{\Omega}_1|$, or η times is encountered.

Step 3. Obtain the next data bit δ'' from W, and perform the following substeps.

Step 3.1. If δ''=1 and $|\tilde{\Omega}_2| \ge |\tilde{\Omega}_1|$, then do nothing, which means that data bit 1 can be carried by directional-sampling without altering the pixel value, and proceed to Step 4.

Step 3.2. If δ''=1 and $|\tilde{\Omega}_2| \le |\tilde{\Omega}_1|$, then increase $\tilde{c}_{lj}$ in $\tilde{\Omega}_1$ repeatedly by the λ value each time until either $|\tilde{\Omega}_2| > |\tilde{\Omega}_1|$ or times η is encountered, and proceed to Step 4.

Step 3.3. If δ''=0 and $|\tilde{\Omega}_2| \le |\tilde{\Omega}_1|$, then do nothing, which means that data bit 0 can be carried by directional-sampling without altering the pixel value, and proceed to Step 4.

Step 3.4. If δ''=0 and $|\tilde{\Omega}_2| > |\tilde{\Omega}_1|$, then reduce $\tilde{c}_{mj}$ in $\tilde{\Omega}_2$ repeatedly by the λ value each time until either

$|\tilde{\Omega}_2| \le |\tilde{\Omega}_1|$ or η times is encountered.

Step 4. Set 0 to the mark in the corresponding position of the block map *M* if only X-sampling is used; set Mark 1 to that of *M* if only directional-sampling is used; set Mark 2 to that of *M* if both sampling techniques are used; and set Mark 3 to that of *M* if neither X-sampling nor directional-sampling is used, and return to Step 1.

Step 5. Stop.

Notice that Steps 2.2 and 3.2 attempt to (with a limit of times η) enlarge the set $\hat{\Omega}_2$ (or $\tilde{\Omega}_2$) to achieve the goal of $|\hat{\Omega}_2| > |\hat{\Omega}_1|$ (or $|\tilde{\Omega}_2| > |\tilde{\Omega}_1|$). Conversely, Steps 2.4 and 3.4 attempt to reduce the set $\hat{\Omega}_2$ (or $\tilde{\Omega}_2$) to achieve $|\hat{\Omega}_2| \le |\hat{\Omega}_1|$ (or $|\tilde{\Omega}_2| \le |\tilde{\Omega}_1|$). To avoid overflow during the enlargement procedure, the increment is bypassed to the pixels $\hat{c}_{lj}$ (or $\tilde{c}_{lj}$), with a value greater than (255–η). Similarly, to avoid underflow during the reducing procedure, the decrement is bypassed to the pixels $\hat{c}_{mj}$ (or $\tilde{c}_{mj}$), with a value less than or equal to η.

C. Bit Extraction

The decoding part of the proposed method is much simpler than the encoder. Without loss of generality, let $D_j = \{(r_{kj}, g_{kj}, b_{kj})\}_{k=0}^{n^2-1}$ be the *j*-th hidden block of size *n*×*n* taken from a stego-image, and let $D_j = \hat{D} \cup \tilde{D}$ with $\hat{D} = \{(r_{ij}, g_{ij}, b_{ij}) | \, i = 0,3,5,6,9,10,12,15\}$ and $\tilde{D} = \{(r_{tj}, g_{tj}, b_{tj}) | \, t = 1,2,4,7,8,11,13,14\}$. In addition, let $\hat{\Theta}_1 = \{ \hat{d}_{lj} \,|\, \|\hat{d}_{lj} O\| \le h \,\|OR\|, \hat{d}_{lj} \in \hat{D}\}$ and $\hat{\Theta}_2 = \{ \hat{d}_{mj} \,|\, \|\hat{d}_{mj} O\| > h \,\|OR\|, \hat{d}_{mj} \in \hat{D}\}$ be the two subsets of $\hat{D}$ with $\hat{D} = \hat{\Theta}_1 \cup \hat{\Theta}_2$; and let $\tilde{\Theta}_1 = \{ \tilde{d}_{lj} \,|\, \|\tilde{d}_{lj} O\| \le h \,\|OR\|, \tilde{d}_{lj} \in \tilde{D}\}$ and $\tilde{\Theta}_2 = \{ \tilde{d}_{mj} \,|\, \|\tilde{d}_{mj} O\| > h \,\|OR\|, \tilde{d}_{mj} \in \tilde{D}\}$ be the two subsets of $\tilde{D}$ with $\tilde{D} = \tilde{\Theta}_1 \cup \tilde{\Theta}_2$. The bit extraction of the proposed method is described in the following algorithm.

Algorithm 2. Extracting bits from stego-image.

Input. A stego-image $\hat{S} = \{(r_i, g_i, b_i) \,|\, i = 1,2,...,MN\}$, the RWM *R* and the centroid *O*, a control parameter *h*, two integers η and λ, and a block map *M*.

Output. A watermark *W*.

Method.

Step 0. Compute the Euclidean distance $\|OR\|$ of *O* and *R*.

Step 1. Input a block D_j derived from $\hat{S}$. If the end of the input is encountered, then proceed to Step 6.

Step 2. If the corresponding mark M_{d_j} of D_j in the block map *M* is equal to 0 and $|\hat{\Theta}_2| > |\hat{\Theta}_1|$, then data bit 1 is extracted; otherwise, data bit 0 is extracted, and return to Step 1.

Step 3. If $M_{d_j} = 1$ and $|\tilde{\Theta}_2| > |\tilde{\Theta}_1|$, then data bit 1 is extracted; otherwise, data bit 0 is extracted, and return to Step 1.

Step 4. If $M_{d_j} = 2$, then perform the following substeps.

Step 4.1. If $|\hat{\Theta}_2| > |\hat{\Theta}_1|$, then data bit 1 is extracted; otherwise, data bit 0 is extracted.

Step 4.2. If $|\tilde{\Theta}_2| > |\tilde{\Theta}_1|$, then data bit 1 is extracted; otherwise, data bit 0 is extracted, and return to Step 1.

Step 5. Repeat from Step 1.

Step 6. Assemble the extracted bits to form the watermark *W*.

Step 7. Stop.

2. Steganographic Approach

As described previously, Phase II of the proposed method embeds data bits into the non-hidden blocks, which is skipped by the proposed watermarking approach.

A. Data Embedment

The notion of data embedment and data extraction for the proposed steganographic method jointly employs the RWM decision policy with the LSB substitution technique. The RWM decision policy is similar to the one discussed in subsection II.2. Specifically, data bits can be embedded into a candidate pixel $P_k = (r_{kj}, g_{kj}, b_{kj})$ of the *j*-th block by using the LSB substitution technique if the Euclidean distance $\|P_k O\|$ of P_k and *O* satisfies both conditions $\|P_k O\| > (\phi_1 \times \|OR\|)$ and $\|P_k O\| < (\phi_2 \times \|OR\|)$, where $\varphi_1 < \varphi_2$ are two control parameters. However, if a candidate pixel violates the RWM decision policy during bit embedding, the candidate pixels are skipped. A skipped pixel contains no data bits. Let $C_j = \{(r_{kj}, g_{kj}, b_{kj})\}_{k=0}^{n^2-1}$ be the *j*-th non-hidden block, bypassed by the Phase I procedure. The major steps of data embedment are summarized as follows.

Step 1. Input block C_j. If the end of input is encountered, then proceed to Step 6.

Step 2. Obtain pixel c_{kj} from C_j; if all of the pixels in C_j have been processed, then return to Step 1; otherwise, compute the Euclidean distance $\|c_{kj} O\|$.

Step 3. If both conditions of $\|c_{kj} O\| > (\phi_1 \times \|OR\|)$ and $\|c_{kj} O\| < (\phi_2 \times \|OR\|)$ are satisfied, then embed *u* bits into r_{kj} and g_{kj}, respectively, and *v* bits into b_{kj}, using the LSB substitution technique, and form the stego-pixel $\hat{c}_{kj}$; otherwise, return to Step 2.

Step 4. If both conditions of $\|\hat{c}_{kj} O\| > (\phi_1 \times \|OR\|)$ and $\|\hat{c}_{kj} O\| < (\phi_2 \times \|OR\|)$ are satisfied, then return to Step 2.

Step 5. Restore (2*u*+v) bits from the stego-pixel $\hat{c}_{kj}$, and repeat from Step 2.

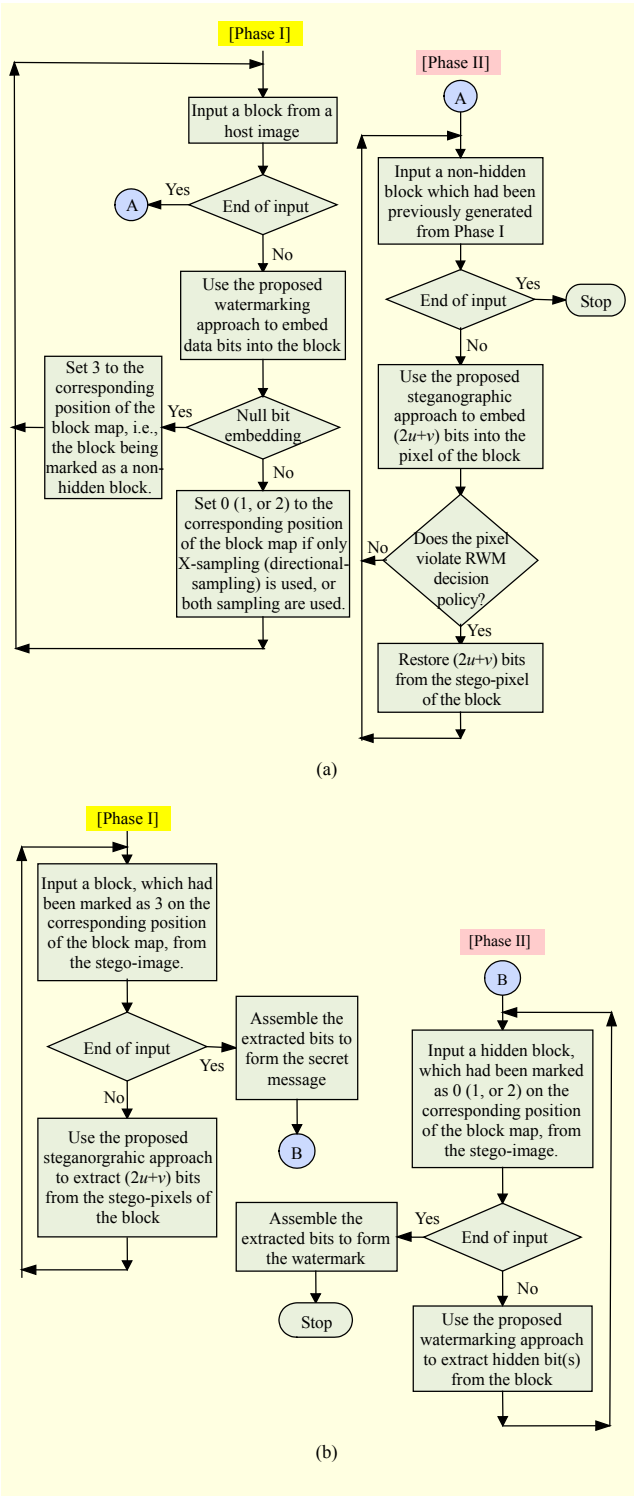


Fig. 2. Flowchart of proposed method: (a) encoding part and (b) decoding part.

Step 6. Stop.

The number of candidate pixels that can be used to hide secret bits is determined by the "interval" computed from φ_1 and φ_2. A larger interval scale indicates a higher hiding capacity. The values of both parameters vary for each image. Step 5 restores secret bits back to the state at Step 3 as $\|\hat{c}_{kj}O\|$ violates the RWM decision policy, which means that the candidate pixels failed to hide bits.

B. Data Extraction

Let $D_j = \{(\hat{r}_{kj}, \hat{g}_{kj}, \hat{b}_{kj})\}_{k=0}^{n^2-1}$ be the j-th hidden block of size $n \times n$ that is introduced from the encoding part of the proposed steganographic scheme. The decoding part of the proposed steganographic method is summarized in the following steps.

Step 0. Read in the RWM R and the centroid O, and compute the Euclidean distance $\|OR\|$ of O and R.

Step 1. Read in the block D_j; if all blocks have been processed, then proceed to Step 3.

Step 2. For each stego-pixel $\hat{d}_{kj}$ in D_j, compute the Euclidean distance $\|\hat{d}_{kj}O\|$. If all pixels in D_j have been examined, then return to Step 1.

Step 3. If both conditions of $\|\hat{d}_{kj}O\| > (\phi_1 \times \|OR\|)$ and $\|\hat{d}_{kj}O\| < (\phi_2 \times \|OR\|)$ are satisfied, then extract $2u$ bits from $\hat{r}_{kj}$ and $\hat{g}_{kj}$, and v bits from $\hat{b}_{kj}$, respectively, by using the LSB technique, and return to Step 2; otherwise, proceed directly to Step 2.

Step 4. Assemble the extracted bits to form the secret message.

Step 5. Stop.

A flowchart of the encoding part and decoding part for the proposed method is summarized in Fig. 2.

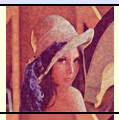
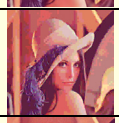
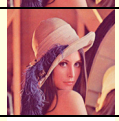
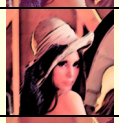
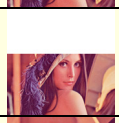
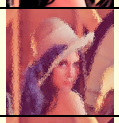
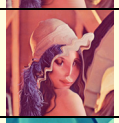
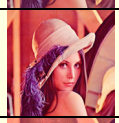
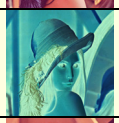
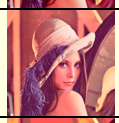
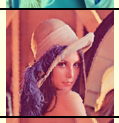
3. Overhead Analysis

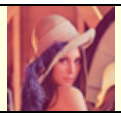
The overhead for the proposed watermarking approach is the RWM R, the centroid O, a control parameter h, two integers η and λ, and the block map B, whereas that for the proposed steganographic approach includes two control parameters φ_1 and φ_2 and two integers u and v. The total overhead of the proposed two approaches is $OH_R + OH_O + OH_B + OH_\tau$, where OH_R, OH_O, OH_B, OH_B, and OH_τ represent the overhead bits required by R, O, B, and the remaining parameters (or integers), respectively. Because OH_B is much larger than $OH_R + OH_O + OH_\tau$, the total overhead bits OH_{Total} of the proposed method can be rewritten as

$$OH_{\text{Total}} = OH_R + OH_O + OH_B + OH_\tau$$
$$\approx OH_B = \left\lfloor \frac{M}{n} \right\rfloor \times \left\lfloor \frac{N}{n} \right\rfloor \times 2 \le (2MN / n^2). \quad (8)$$

The overhead bits of the watermarking approach can be embedded into the non-hidden blocks by the proposed

Table 1. Examples of surviving watermarks after manipulations of stego-image (Lena).

Attack	Manipulated stego-image	Survived watermark	Attack	Manipulated stego-image	Survived watermark
Attack-free BCR = 100%			Sponge distortion BCR = 80.54%		
JPEG2000 (CR=96) BCR = 90.52%			Truncation† BCR = 91.36%		
JPEG (CR=64) BCR = 83.65%			Diffusing BCR = 79.30%		
Uniform noise (9%) BCR = 87.95%			Sprayed BCR =70.27 %		
Gaussian noise (5%) BCR = 88.10%			Ink-painting BCR = 77.93%		
Cropping (42%) BCR = 88.20%			Glassing-distorted BCR = 82.28%		
Edge sharpening BCR = 99.95%			Winding BCR = 79.56%		
Sharpening BCR = 99.65%			Zigzagging BCR = 89.43%		
Equalized BCR = 85.04%			Inversion BCR = 85.93%		
Grain distortion BCR = 82.91%			Rippling BCR = 96.25%		
Posterized (4-level) BCR = 85.28%			Mosaicking BCR = 88.69%		
Brightness (100%) BCR = 75.56%			Contrast (70%) BCR = 66.81%		
Brightness (–100%) BCR = 62.67%			Contrast (–70%) BCR = 80.30%		
Gaussian-blurring BCR =90.37 %			Motion-blurring BCR = 87.60%		
Twisting BCR = 80.64%			Companding BCR = 73.04%		

Ghosting BCR = 84.15%					

† Last five bits of stego-pixel truncated.

steganographic approach. Note that a non-hidden block is the block skipped by Phase I of the proposed method. However, to maintain robustness of the proposed watermarking approach, it is suggested that the overhead information is directly sent to the receiver by out-of-band transmission.

IV. Experiment Results

1. Simulations of Robust Watermarking Approach

To demonstrate robustness performance of the proposed method, examples of surviving watermarks (sized 45×45 with 8 bits/pixel, two colors) are shown in Table 1. The watermark is extracted from the stego-image, which has been intentionally distorted (or manipulated). The stego-image, as shown in Fig. 3, is generated using the proposed method by embedding a watermark (and a grayscale image of size 512×512) into a color image Lena sized 512×512. Each RGB pixel of the image is represented by 24 bits, with 8 bits per component. The block size is 4×4, and the control parameters h, η, and λ are set at 5.2, 6, and 1, respectively. The PSNR of the stego-image is 39.55 dB. However, the PSNR of value 48.69 dB is achieved only if the watermarking approach is used solely. Namely, Phase II of the proposed method is bypassed during bit embedding. The PSNR is defined by

$$\mathrm{PSNR} = 10 \times \log_{10} \frac{255^2}{\mathrm{MSE}} \tag{9}$$

with

$$\mathrm{MSE} = \frac{1}{3MN} \sum_{i=1}^{MN} \left[(r_i - \hat{r}_i)^2 + (g_i - \hat{g}_i)^2 + (b_i - \hat{b}_i)^2 \right]. \tag{10}$$

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 stego-image.

In addition, the bit correct ratio (BCR) is defined by

$$\mathrm{BCR} = \left(\sum_{i=0}^{ab-1} \overline{w_i \oplus \tilde{w}_i} \Big/ a \times b \right) \times 100\%, \tag{11}$$

where w_i and $\tilde{w}_i$ represent the values of the original watermark and the extracted watermark, respectively, and the size of a watermark is $a \times b$. The BCR for an extracted watermark is 100% if a marked image is not attacked. Table 1 shows that most extracted watermarks are easily recognized. Although the BCR for some of them is below 75%, for example, the watermarks extracted from brightness manipulations (–100%), sprayed, contrast (±70%), and companding are identifiable. Figure 4 illustrates the BCR values of the extracted watermarks under attack: JPEG2000 and JPEG with various compression ratios (CRs). The BCR is approximately 85% when the stego-image is attacked by JPEG compression with a CR of 60.94. Further, the proposed method has excellent performance in resisting compression attacks.

(a) (b)

Fig. 3. Resultant image of Lena generated by proposed method: (a) original image and (b) stego-image.

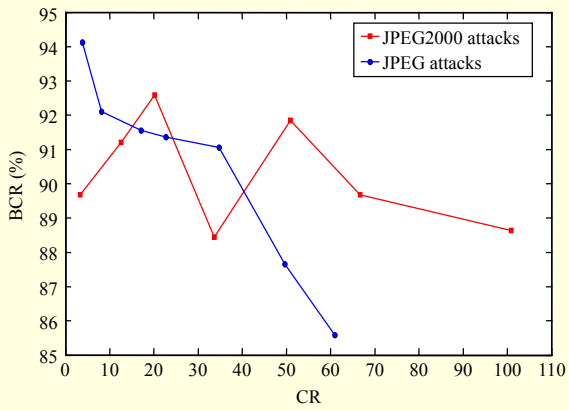
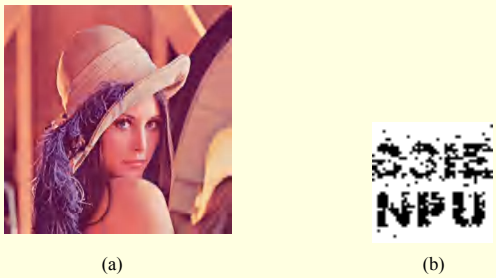


Fig. 4. BCR performance of proposed method under JPEG2000 and JPEG attacks.

Figure 5 shows a surviving watermark extracted from the stego-image compressed by JPEG2000 with a CR of 194.26. Under such a high CR attack, the extracted watermark is still recognized. This robustness is hardly achieved by reported works, each of which embeds the watermark into a host image in the spatial domain. The BCR for watermarks extracted from



(a) (b)

Fig. 5. Robustness of proposed method under JPEG2000 attack: (a) stego-image after manipulated by JPEG2000 with CR=194.26 and (b) extracted watermark (with BCR=89.23%).

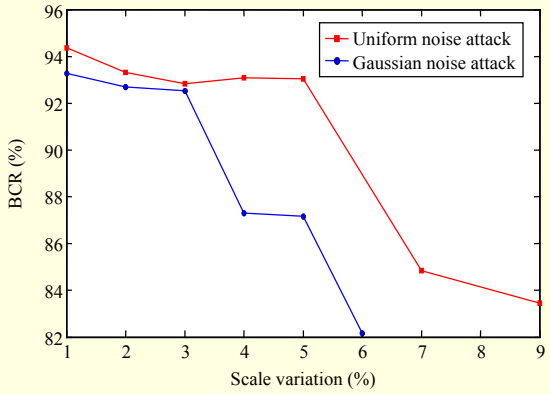


Fig. 6. BCR performance of proposed method under uniform and Gaussian noise addition attacks.

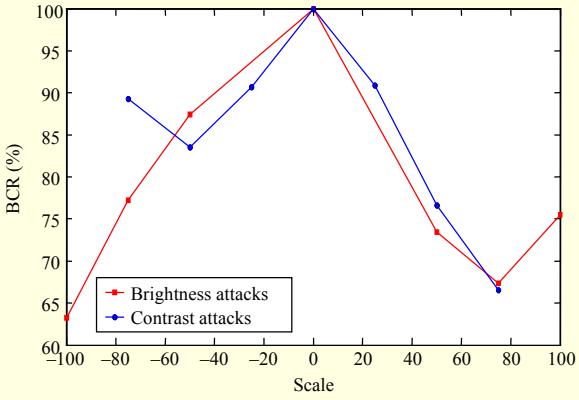


Fig. 7. BCR performance of proposed method under brightness and contrast attacks.

stego-images manipulated by uniform and Gaussian noise addition are displayed in Fig. 6, which shows that the BCR watermark performance obtained from uniform noise attacks is superior to that obtained from Gaussian noise attacks. The stego-images generated using the proposed method are more robust against uniform noise attacks than from Gaussian noise attacks. Figure 7 shows that the stego-images generated by the proposed method have better performances in resisting brightness attacks than contrast attacks with a scale between –60 and +80. In addition, the ones generated by the proposed method tolerate brightness and contrast attacks with a scale ranging from –100 to +80 and 75 to 100, respectively. A majority-vote policy is used during bit extraction.

Table 2. Payload/PSNR comparison between various methods.

Method	Payload (bits)	PSNR (dB)
Fu and Shen [8]	32×25=800	41.34
Findik and others [9]	32×32=1,024	41.83
Proposed method	45×45×8=16,200	48.68

Table 3. BCR performance comparison between various methods.

Attack	BCR		
	Fu and Shen [8]	Findik and others [9]	Proposed method
Blurring	99.75%	53.61%	90.37%
Mosaicking	92.13%	N/A†	88.69%
Luminance (+50%) & contrast (+50%)	98.88%	N/A†	75.04%
Noise (5%)	N/A†	97.94%	93.04%
JPEG (QF=80)	89.75%	N/A†	91.06%
Sharpening	N/A†	100%	99.65%
Distortion (2^0)	86.88%	N/A†	N/A†
Cropping (25% cutoff)	95%	N/A†	97.58%
Other attacks (bit truncation, color quantization, winding, zigzagging and poster edge distortion, inversion, twirling, rippling, diffusing, sprayed, winding, ghosting, companding, etc.)	N/A†	N/A†	(see Table 1)

†N/A: not available.

From the preceding demonstration, the conclusion is that stego-images generated by the proposed watermarking scheme are able to resist various attacks, such as JPEG2000, JPEG, noise addition, cropping, (edge) sharpening, blurring, bit truncation, brightness, contrast, (color) quantization, winding, zigzagging and poster edge distortion, inversion, twirling, mosaicking, and rippling.

For evaluation, two watermarking schemes [8], [9] for color images based on the spatial domain are compared with the proposed method. Their payload and PSNR performance are listed in Table 2, which shows that the payload for the proposed method is larger than the payloads for the other two schemes, whereas the resulting PSNR is the best among them. Table 3 also shows the robustness performance of these methods.

The BCR generated using the Fu and Shen scheme [8] is larger than the other two approaches under such attacks as blurring, mosaicking, luminance and contrast (enhance +50%), and distortion (with a 2° rotation). However, the hidden watermark extracted using the Fu and Shen scheme [8] is lossy when the stego-images do not suffer an attack. This may be unfeasible for the situation requiring lossless extraction of the watermarks. Although the BCR introduced using Findik and others' [9] scheme has the best value among these approaches on noise addition (5%) and sharpening attacks, the watermarks extracted using the scheme only survive three types of attack. The robustness of the scheme is obviously insufficient. However, for the BCR obtained from the attacks in the proposed method, JPEG compression and cropping are better than that for the other two approaches. The stego-images generated using the proposed method tolerate several types of attack, as indicated in Table 1. The extracted watermarks are also recognizable, although some of them have lower BCR values.

2. Simulations of Steganographic Approach

The main function of the proposed steganographic scheme is to provide extra hiding space for saving a large payload volume (or to provide hiding storage for the overhead, used in Phase I of the proposed method). Several RGB color images sized 512×512 are used as host images. A 512×512 grayscale image Baboon is used as the input data during simulations.

The stego-images generated using the proposed method are shown in Fig. 8. Two control parameters u and ν are set at 3 and 4, respectively. The values of the other two parameters φ_1 and φ_2 have different values in each stego-image. Namely, φ_1 and φ_2 are set at 0 and 24 for the image Lena, at 4 and 29 for the image Peppers, at 5 and 20 for the image House, at 10 and 61 for the image Baboon, at 11 and 35 for the image Scene, and at 0 and 6 for the image Splash. Figure 8 shows no visual (color) distortion in the stego-images, and the perceived quality of the stego-images is desirable. The tradeoff between PSNR and the hiding rate ranging from 0.128 bpp to 8.000 bpp, generated by the high-payload version of the proposed method, is illustrated in Fig. 9. The figure indicates the optimal PSNR to be approximately 54 dB with an embedding rate of 0.098 bpp in image Scene, and the maximum payload of 7.919 bpp with the PSNR value at approximately 36 dB can be found in image Baboon.

A steganographic method color image suggested by Yang [7] is compared with the proposed method. Figure 10 shows the performance of the proposed method to be superior to that of the Yang scheme [7]. The embedding rate of the proposed method can be achieved beyond 2.0 bpp, with the PSNR above

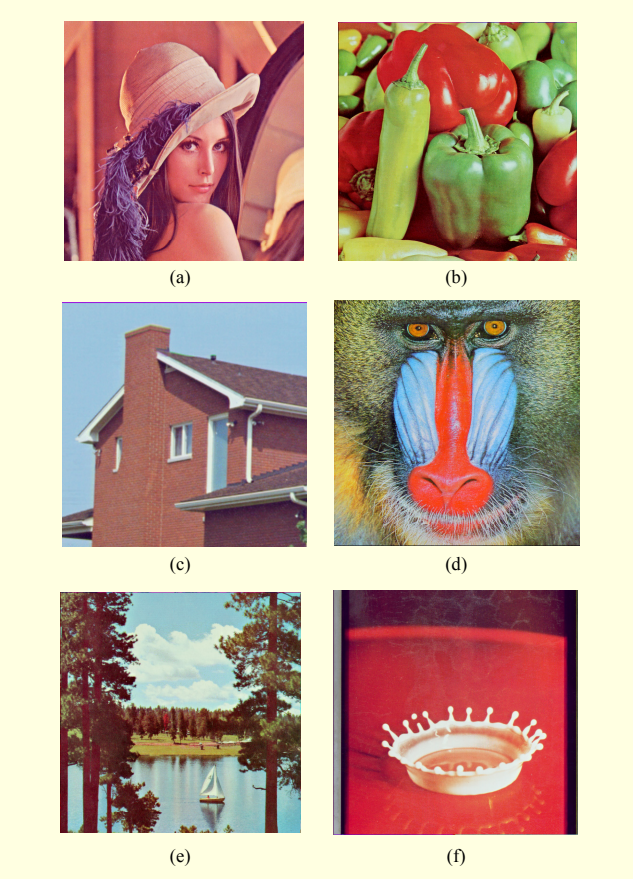


Fig. 8. Stego-images generated by proposed steganographic method (using u=3 and v=4). Their embedding rate (bpp) and PSNR (dB) are (a) Lena (7.180/36.55), (b) Peppers (5.613/37.41), (c) House (4.579/38.29), (d) Baboon (7.872/36.00), (e) Scene (3.538/39.13), and (f) Splash (6.947/36.58).

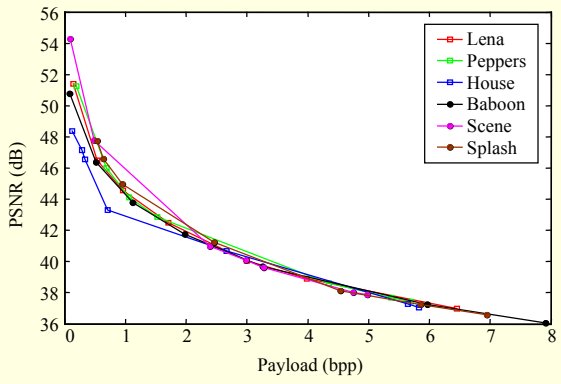


Fig. 9. Tradeoff between PSNR and payload for proposed steganographic method.

42 dB, whereas that of the Yang scheme [7] is limited to approximately 0.5 bpp, with the PSNR at roughly 38 dB.

As described in section III, the proposed steganographic approach can be independently performed in the RGB color

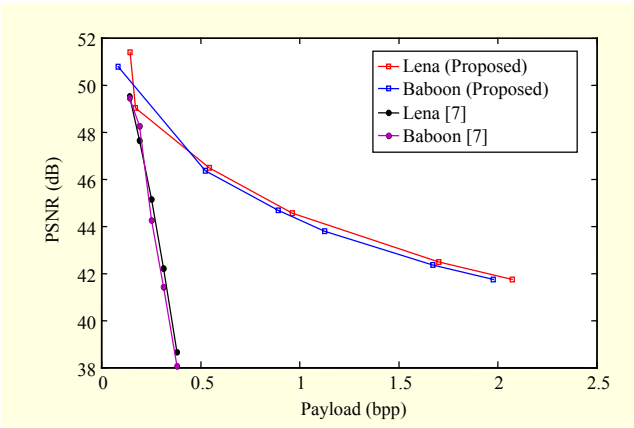


Fig. 10. Performance comparison between Yang's scheme [7] and proposed method in images Lena and Baboon.

systems. That is, for the pixels of each host block, which are derived from an input image, data bits can be embedded into the block if it satisfies the RWM decision policy. Simulations confirm that the average payload of 7.52 bps is achieved with a PSNR around 36.22 dB. On the other hand, the average payload and PSNR computed from Fig. 8 is 5.95 bps and 37.33 dB, respectively. Obviously, the single-phase version of the proposed steganographic approach provides a payload larger than that of the two-phase version of the proposed method with a competitive PSNR performance. The single-phase version of the steganographic approach is suggested if steganography is the pursued goal of users. Since it provides a large payload with a desirable perceived quality, major applications of the steganographic approach can be found in private data saving and a covert channel between two parties.

V. Conclusion

This paper presented a novel watermarking scheme for color images based on the RWM and the feature-embedding technique. The combined use of the RWM decision policy, X-sampling technique, and directional-sampling technique showed that the stego-images generated using the proposed scheme are robust against various manipulations, such as compression, color quantization, bit truncation, noise addition, cropping, blurring, mosaicking, zigzagging, inversion, (edge) sharpening, and so on. The stego-images perform well in resisting attacks from JPEG2000 compression and JPEG compression. The extracted watermarks are recognized, even if the stego-images have been compressed by JPEG2000 with a compression ratio of approximately 195. A steganographic method based on the RWM decision policy with the LSB substitution technique was suggested to provide an extra option for people to hide their private data (or sensitive messages). Experiments confirmed that the perceived quality of the stego-image is desirable, whereas the PSNR is high. The payload generated using the proposed method is also superior to that generated by existing approaches.

Acknowledgment

I would like to thank the editors and anonymous reviewers for providing valuable comments, which helped to improve the content of the paper.

References

[1] I.J. Cox et al., *Digital Watermarking and Steganography*, 2nd ed., Burlington, MA: Morgan Kaufmann Publishers, 2008.

[2] F.Y. Shih, *Digital Watermarking and Steganography: Fundamentals and Techniques*, Boca Raton, FL: CRC Press, 2008.

[3] S. Wang, B. Yang, and X. Niu, "A Secure Steganography Method Based on Genetic Algorithm," *J. Inf. Hiding Multimedia Signal Process.*, vo1. 1, no. 1, 2010, pp. 28-35.

[4] C.Y. Yang and C.H. Lin, "High-Quality and Robust Reversible Data Hiding by Coefficients Shifting Algorithm," *ETRI J.*, vol. 34, no. 3, June 2012, pp. 429-438.

[5] C.Y. Yang et al., "A Simple Digital Watermarking by the Adaptive Bit-Labeling Scheme," *Int. J. Innovative Comput., Info. Control*, vol. 6, no. 3(B), 2010, pp. 1401-1410.

[6] R.M. Noriega et al., "High Payload Audio Watermarking: Toward Channel Characterization of MP3 Compression," *J. Inf. Hiding Multimedia Signal Process.*, vol. 2, no. 2, 2011, pp. 91-107.

[7] C.Y. Yang, "Color Image Steganography Based on Module Substitutions," *Third Int. Conf. Int. Inf. Hiding Multimedia Signal Process.*, Kaohsiung, Taiwan, Nov. 26-28, 2007, pp. 118-121.

[8] Y.G. Fu and R.M. Shen, "Color Image Watermarking Scheme Based on Linear Discriminant Analysis," *Comput Std. Interface*, vol. 30, 2009, pp. 115-120.

[9] O. Findik, I. Babaoglu, and E. Ülker, "A Color Image Watermarking Scheme Based on Artificial Immune Recognition System," *Expert Syst. Appl.*, vol. 38, 2011, pp. 1942-1946.

[10] A. Phadikar and S.P. Maity, "Quality Access Control of Compressed Color Images Using Data Hiding," *Int. J. Electron. Commun*, vol. 64, 2010, pp. 833-843.

[11] Q. Su et al., "A Blind Dual Color Images Watermarking Based on IWT and State Coding," *Optics Commun.*, vol. 285, 2012, pp. 1717-1724.

[12] A. Mitiche and J.K. Aggarwal, "Contour Registration by Shape-Specific Point for Shape Matching," *Comp. Vision, Graph. Image Process.*, vol. 22, 1983, pp. 396-408.

[13] J.C. Lin, S.L Chou, and W.H. Tsai, "Detection of Rotationally Symmetric Shape Orientations by Fold-Invariant Shape-Specific

Points," *Pattern Recog*., vol. 25, 1992, pp. 473-482.
[14] C.Y. Yang and J.C. Lin, "EBTC: An Economical Method for Searching the Threshold of BTC Compression," *Electron. Lett.*, vol. 32, 1996, pp. 1870-1871.
[15] C.Y. Yang and J.C. Lin, "RWM-Cut for Color Image Quantization," *Comput. Graph.*, vol. 20, 1996, pp. 577-588.

Ching-Yu Yang received his BS in electronics engineering in 1983 from the National Taiwan Institute of Technology, Taipei, Taiwan, and his MS in electrical engineering in 1990 from National Cheng Kung University, Tainan City, Taiwan. In 1999, he received his PhD in computer and information science from National Chiao Tung University, Hsinchu, Taiwan. From 1999 to 2005, he was a senior engineer at Chunghwa Telecom Co., Ltd., Taiwan. He joined the Computer Science and Information Engineering Department at National Penghu University of Science and Technology, Penghu, Taiwan, in February 2005 and is currently an associate professor there. His recent research interests include image processing, pattern recognition, data hiding, and network security.