Edge Adaptive Image Steganography Based on LSB Matching Revisited

Weiqi Luo, *Member, IEEE*, Fangjun Huang, *Member, IEEE*, and Jiwu Huang, *Senior Member, IEEE*

Abstract—The least-significant-bit (LSB)-based approach is a popular type of steganographic algorithms in the spatial domain. However, we find that in most existing approaches, the choice of embedding positions within a cover image mainly depends on a pseudorandom number generator without considering the relationship between the image content itself and the size of the secret message. Thus the smooth/flat regions in the cover images will inevitably be contaminated after data hiding even at a low embedding rate, and this will lead to poor visual quality and low security based on our analysis and extensive experiments, especially for those images with many smooth regions. In this paper, we expand the LSB matching revisited image steganography and propose an edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. For lower embedding rates, only sharper edge regions are used while keeping the other smoother regions as they are. When the embedding rate increases, more edge regions can be released adaptively for data hiding by adjusting just a few parameters. The experimental results evaluated on 6000 natural images with three specific and four universal steganalytic algorithms show that the new scheme can enhance the security significantly compared with typical LSB-based approaches as well as their edge adaptive ones, such as pixel-value-differencing-based approaches, while preserving higher visual quality of stego images at the same time.

Index Terms—Content-based steganography, least-significant-bit (LSB)-based steganography, pixel-value differencing (PVD), security, steganalysis.

I. INTRODUCTION

STEGANOGRAPHY is a technique for information hiding. It aims to embed secret data into a digital cover media, such as digital audio, image, video, etc., without being suspicious. On the other side, steganalysis aims to expose the presence of hidden secret messages in those stego media. If there exists a steganalytic algorithm which can guess whether a given media is a cover or not with a higher probability than random guessing, the steganographic system is considered broken. In practice,

two properties, undetectability and embedding capacity, should be carefully considered when designing a steganographic algorithm. Usually, the larger payload embedded in a cover, the more detectable artifacts would be introduced into the stego. In many applications, the most important requirement for steganography is undetectability, which means that the stegos should be visually and statistically similar to the covers while keeping the embedding rate as high as possible. In this paper, we consider digital images as covers and investigate an adaptive and secure data hiding scheme in the spatial least-significant-bit (LSB) domain.

LSB replacement is a well-known steganographic method. In this embedding scheme, only the LSB plane of the cover image is overwritten with the secret bit stream according to a pseudorandom number generator (PRNG). As a result, some structural asymmetry (never decreasing even pixels and increasing odd pixels when hiding the data) is introduced, and thus it is very easy to detect the existence of hidden message even at a low embedding rate using some reported steganalytic algorithms, such as the Chi-squared attack [2], regular/singular groups (RS) analysis [3], sample pair analysis [4], and the general framework for structural steganalysis [5], [6].

LSB matching (LSBM) employs a minor modification to LSB replacement. If the secret bit does not match the LSB of the cover image, then $+1$ or -1 is randomly added to the corresponding pixel value. Statistically, the probability of increasing or decreasing for each modified pixel value is the same and so the obvious asymmetry artifacts introduced by LSB replacement can be easily avoided. Therefore, the common approaches used to detect LSB replacement are totally ineffective at detecting the LSBM. Up to now, several steganalytic algorithms (e.g., [7]–[10]) have been proposed to analyze the LSBM scheme. In [7], Harmsen and Pearlman showed that LSBM works as a low-pass filter on the histogram of the image, which means that the histogram of the stego image contains fewer high-frequency components compared with the histogram of its cover. Based on this property, the authors introduced a detector using the center of mass (COM) of the histogram characteristic function (HCF). In [8], Ker pointed out that the original HCF COM method in [7] does not work well on grayscale images and introduced two ways of applying the HCF COM method, namely utilizing the down-sampled image and the adjacency histogram instead of the traditional histogram, which are effective for grayscale images that have been JPEG compressed with a low quality factor, say, 58. In a recent work [10], Li *et al.* proposed to calculate calibration-based detectors, such as Calibrated HCF COM, on the difference image. The experimental results showed that the new detector outperforms Ker's approaches in [8] and achieved acceptable accuracy at an embedding rate of 50%. In [9], Huang

et al. investigated the statistical features of those small overlapping blocks in the subimage which consists of the first two bit planes of the image and proposed another kind of steganalytic feature based on the alteration rate of the number of neighborhood pixel values. The experimental results demonstrated that the method was more effective on uncompressed grayscale images. Besides those specific detectors, some universal steganalytic algorithms such as [11], [12], and [13] can also be used for exposing the stego images using LSBM and/or other steganographic methods with a relatively high detection accuracy.

Unlike LSB replacement and LSBM, which deal with the pixel values independently, LSB matching revisited (LSBMR) [1] uses a pair of pixels as an embedding unit, in which the LSB of the first pixel carries one bit of secret message, and the relationship (odd–even combination) of the two pixel values carries another bit of secret message. In such a way, the modification rate of pixels can decrease from 0.5 to 0.375 bits/pixel (bpp) in the case of a maximum embedding rate, meaning fewer changes to the cover image at the same payload compared to LSB replacement and LSBM. It is also shown that such a new scheme can avoid the LSB replacement style asymmetry, and thus it should make the detection slightly more difficult than the LSBM approach based on our experiments.

The typical LSB-based approaches, including LSB replacement, LSBM, and LSBMR, deal with each given pixel/pixel-pair without considering the difference between the pixel and its neighbors. Until now, several edge adaptive schemes such as [14]–[19] have been investigated. In [14], Hempstalk proposed a hiding scheme by replacing the LSB of a cover according to the difference values between a pixel and its four touching neighbors. Although this method can embed most secret data along sharper edges and can achieve more visually imperceptible stegos (please refer to Fig. 1(g) and Table I), the security performance is poor. Since the method just modifies the LSB of image pixels when hiding data, it can be easily detected by existing steganalytic algorithms, such as the RS analysis (please refer to Section IV-C1). In [15], Singh *et al.* proposed an embedding method which first employs a Laplacian detector on every 3×3 nonoverlapping block within the cover to detect edges, and then performs data hiding on center pixels whose blocks are located at the sharper edges according to a threshold θ. As mentioned in [15], the maximum embedding capacity of such a method is relatively low ($1/9 \approx 11.1\%$). Furthermore, the threshold θ is predetermined and thus it cannot change adaptively according to the image contents and the message to be embedded. The pixel-value differencing (PVD)-based scheme (e.g., [17]–[19]) is another kind of edge adaptive scheme, in which the number of embedded bits is determined by the difference between a pixel and its neighbor. The larger the difference, the larger the number of secret bits that can be embedded. Usually, PVD-based approaches can provide a larger embedding capacity (on average, larger than 1 bpp). Based on our extensive experiments, however, we find that the existing PVD-based approaches cannot make full use of edge information for data hiding, and they are also poor at resisting some statistical analyses.

One of the common characteristics of most the steganographic methods mentioned above is that the pixel/pixel-pair

selection is mainly determined by a PRNG while neglecting the relationship between the image content and the size of the secret message. By doing this, these methods can spread the secret data over the whole stego image randomly even at low embedding rate. However, based on our analysis and extensive experiments, we find that such embedding schemes do not perform well in terms of the security or visual quality of the stego images. Assuming that a cover image is made up of many nonoverlapping small subimages (regions) based on a predetermined rule, then different regions usually have different capacities for hiding the message. Similar to the problem of cover image selection [20], we should preferentially use those subimages with good hiding characteristics while leaving the others unchanged. Therefore, deciding how to select the regions is the key issue of our proposed scheme. Generally, the regions located at the sharper edges present more complicated statistical features and are highly dependent on the image contents. Moreover, it is more difficult to observe changes at the sharper edges than those in smooth regions.

In this paper, we propose an edge adaptive scheme and apply it to the LSBMR-based method. The experimental results evaluated on thousands of natural images using different kinds of steganalytic algorithms show the superiority of the new method.

The rest of the paper is arranged as follows. Section II analyzes the limitations of the relevant steganographic schemes and proposes some strategies. Section III shows the details of data embedding and data extraction in our scheme. Section IV presents experimental results and discussions. Finally, concluding remarks and future work are given in Section V.

II. ANALYSIS OF LIMITATIONS OF RELEVANT APPROACHES AND STRATEGIES

In this section, we first give a brief overview of the typical LSB-based approaches including LSB replacement, LSBM, and LSBMR, and some adaptive schemes including the original PVD scheme [17], the improved version of PVD (IPVD) [18], adaptive edges with LSB (AE-LSB) [19], and hiding behind corners (HBC) [14], and then show some image examples to expose the limitations of these existing schemes. Finally we propose some strategies to overcome these limitations.

In the LSB replacement and LSBM approaches, the embedding process is very similar. Given a secret bit stream to be embedded, a traveling order in the cover image is first generated by a PRNG, and then each pixel along the traveling order is dealt with separately. For LSB replacement, the secret bit simply overwrites the LSB of the pixel, i.e., the first bit plane, while the higher bit planes ($2 \sim 8$) are preserved. For the LSBM scheme, if the secret bit is not equal to the LSB of the given pixel, then ± 1 is added randomly to the pixel while keeping the altered pixel in the range of $[0, 255]$. In such a way, the LSB of pixels along the traveling order will match the secret bit stream after data hiding both for LSB replacement and LSBM. Therefore, the extracting process is exactly the same for the two approaches. It first generates the same traveling order according to a shared key, and then the hidden message can be extracted correctly by checking the parity bit of pixel values.
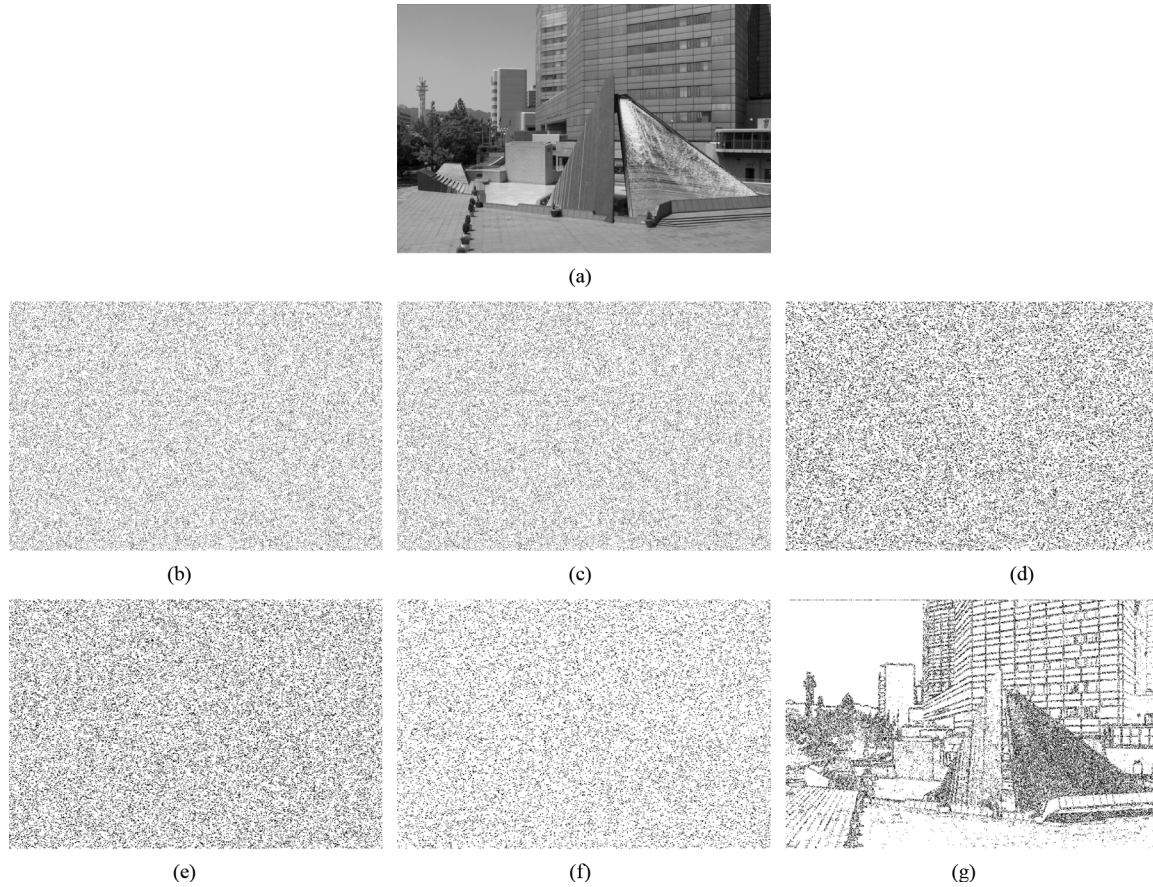
Fig. 1.   (a) Cover image. (b)–(g) Differences between cover and stego images using the six steganographic approaches with the same embedding rate of 30%. The black pixels denote that those pixel values in the corresponding positions have been modified after data hiding. (a) Cover image. (b) LSBM. (c) LSBMR. (d) PVD. (e) IPVD. (f) AE-LSB. (g) HBC.

TABLE I
AVERAGE PSNR, wPSNR, AND THE MODIFICATION RATE OVER 6000 STEGO
IMAGES WITH DIFFERENT STEGANOGRAPHIC ALGORITHMS AND EMBEDDING
RATES. THE NUMBERS IN BRACKETS DENOTE THE BEST VALUES IN THE
CORRESPONDING CASES

Embedding Rate	Steganographic Algorithms		Average PSNR	Average wPSNR	Avg. rate of Modification
10%	LSB-Based	LSBM	61.1	63.1	0.0500
		LSBMR	(62.2)	64.1	0.0375
	Edge-Based	PVD	51.5	56.3	0.0488
		IPVD	53.8	58.8	0.0490
		AE-LSB	52.0	56.1	(0.0277)
		HBC	61.1	(68.9)	0.0500
	Our Proposed		61.9	(68.9)	0.0386
30%	LSB-Based	LSBM	56.4	58.4	0.1500
		LSBMR	(57.4)	59.4	0.1125
	Edge-Based	PVD	46.8	51.5	0.1465
		IPVD	49.0	54.0	0.1471
		AE-LSB	47.2	51.3	(0.0831)
		HBC	56.4	(61.0)	0.1500
	Our Proposed		56.8	60.8	0.1187
50%	LSB-Based	LSBM	54.2	56.1	0.2500
		LSBMR	(55.2)	57.1	0.1875
	Edge-Based	PVD	44.5	49.3	0.2441
		IPVD	46.8	51.8	0.2452
		AE-LSB	45.0	49.1	(0.1384)
		HBC	54.2	(57.4)	0.2500
	Our Proposed		54.1	56.8	0.2022

LSBMR applies a pixel pair (x_i, x_{i+1}) in the cover image as an embedding unit. After message embedding, the unit is modified as (x'_i, x'_{i+1}) in the stego image which satisfies

$$\text{LSB}(x'_i) = m_i, \quad \text{LSB}\left(\left\lfloor \frac{x'_i}{2} \right\rfloor + x'_{i+1}\right) = m_{i+1}$$

where the function $\text{LSB}(x)$ denotes the LSB of the pixel value x. m_i and m_{i+1} are the two secret bits to be embedded.

By using the relationship (odd–even combination) of adjacent pixels, the modification rate of pixels in LSBMR would decrease compared with LSB replacement and LSBM at the same embedding rate. What is more, it does not introduce the LSB replacement style asymmetry. Similarly, in data extraction, it first generates a traveling order by a PRNG with a shared key. And then for each embedding unit along the order, two bits can be extracted. The first secret bit is the LSB of the first pixel value, and the second bit can be obtained by calculating the relationship between the two pixels as shown above.

Our human vision is sensitive to slight changes in the smooth regions, while it can tolerate more severe changes in the edge regions. Several PVD-based methods such as [17]–[19] have been proposed to enhance the embedding capacity without introducing obvious visual artifacts into the stego images. The basic idea of PVD-based approaches is to first divide the cover image into many nonoverlapping units with two consecutive pixels and then deal with the embedding unit along a pseudo-random order which is also determined by a PRNG. The larger
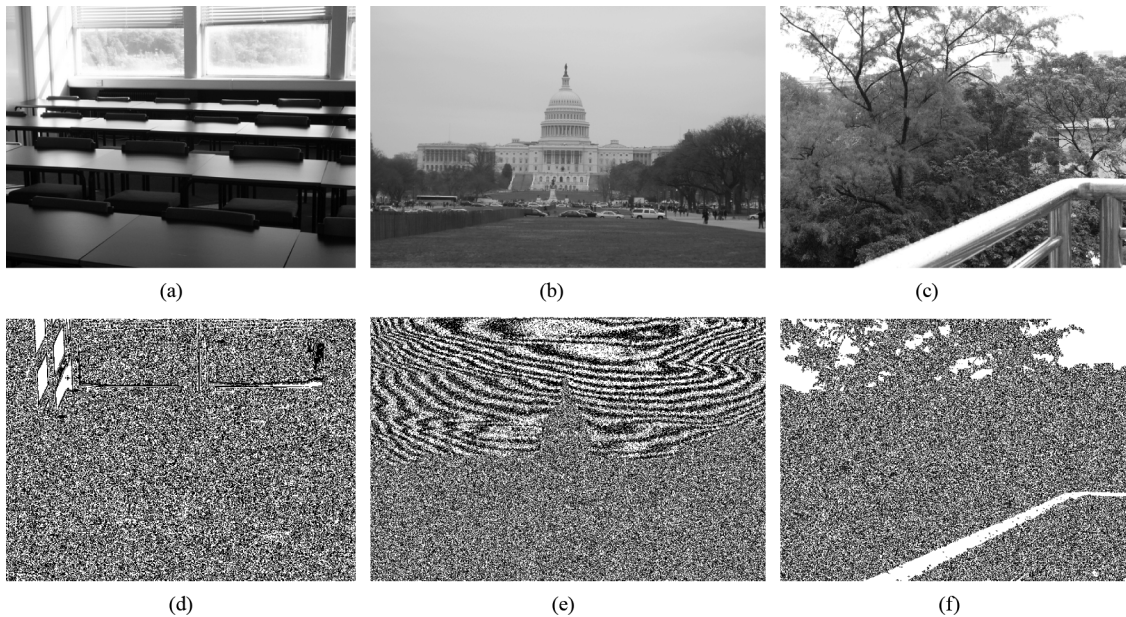
Fig. 2. LSB of three cover images. It can be observed that the LSB is not completely random. Some of the LSB planes would even present texture information just like those in the higher bit planes (a) Example 1. (b) Example 2. (c) Example 3. (d) LSB of Example 1. (e) LSB of Example 2. (f) LSB of Example 3.

the difference between the two pixels, the larger the number of secret bits that can be embedded into the unit. To a certain extent, existing PVD-based approaches are edge adaptive since more secret data is embedded in those busy regions. However, similar to the LSBM and LSBMR approaches, pixel pair selection is mainly dependent on a PRNG, which means that the modified pixels will still be spread around the whole stego image as illustrated in Fig. 1(b)–(f). It is observed that many smooth regions will be altered inevitably after data hiding even when the difference between two consecutive pixels is zero (meaning the subimages are located over flat regions), while many available sharp edge regions have not been fully exploited.

Most existing steganographic approaches usually assume that the LSB of natural covers is insignificant and random enough, and thus those pixels/pixel pairs for data hiding can be selected freely using a PRNG. However, such an assumption is not always true, especially for images with many smooth regions. Fig. 2 shows the LSB planes of some image examples. It can be clearly observed that the LSB can reflect the texture information of the cover image to some extent. Based on extensive experiments, we find that uncompressed natural images usually contain some flat regions (it may be as small as 5×5 and it is hard to notice), and the LSB in those regions have the same values (1 or 0). Therefore, if we embed the secret message into these regions, the LSB of stego images would become more and more random, which may lead to visual and statistical differences between cover (contains flat regions/texture information) and stego images (appearing as a noise-like distribution) in the LSB plane as illustrated in Fig. 3.

Compared with smooth regions, the LSB of pixels located in edge regions usually present more random characteristics, and they are statistically similar to the distribution of the secret message bits (assuming a 1/0 uniform distribution). Therefore, it is expected that fewer detectable artifacts and visual artifacts

would be left in the edge regions after data hiding. Furthermore, the edge information (such as the location and the statistical moments) is highly dependent on image content, which may make detection even more difficult. This is why our proposed scheme will first embed the secret bits into edge regions as far as possible while keeping other smooth regions as they are. As shown in Fig. 1(g), we found that the HBC method [14] has this property. However, the HBC method just modifies the LSBs while keeping the most significant bits unchanged; thus it can be regarded as an edge adaptive case of LSB replacement, and the LSB replacement style asymmetry will also occur in their stegos. We will show some experimental evidence to expose the limitation of the HBC method in Section IV-C1.

Please note that we do not evaluate the security of JPEG images in this paper. The reason is that all the nonoverlapping 8×8 blocks within JPEG images are arranged regularly due to lossy JPEG compression. If spatial-domain steganographic methods were performed on JPEG decompressed images, it would inevitably lead to JPEG incompatibilities [21], namely the additional secret message would destroy the unique fingerprints introduced by the previous JPEG compression with a given quantization table. We can even potentially detect a hidden message as short as one bit from the JPEG stegos.

III. PROPOSED SCHEME

The flow diagram of our proposed scheme is illustrated in Fig. 4. In the data embedding stage, the scheme first initializes some parameters, which are used for subsequent data preprocessing and region selection, and then estimates the capacity of those selected regions. If the regions are large enough for hiding the given secret message M, then data hiding is performed on the selected regions. Finally, it does some postprocessing to obtain the stego image. Otherwise the scheme needs to revise the
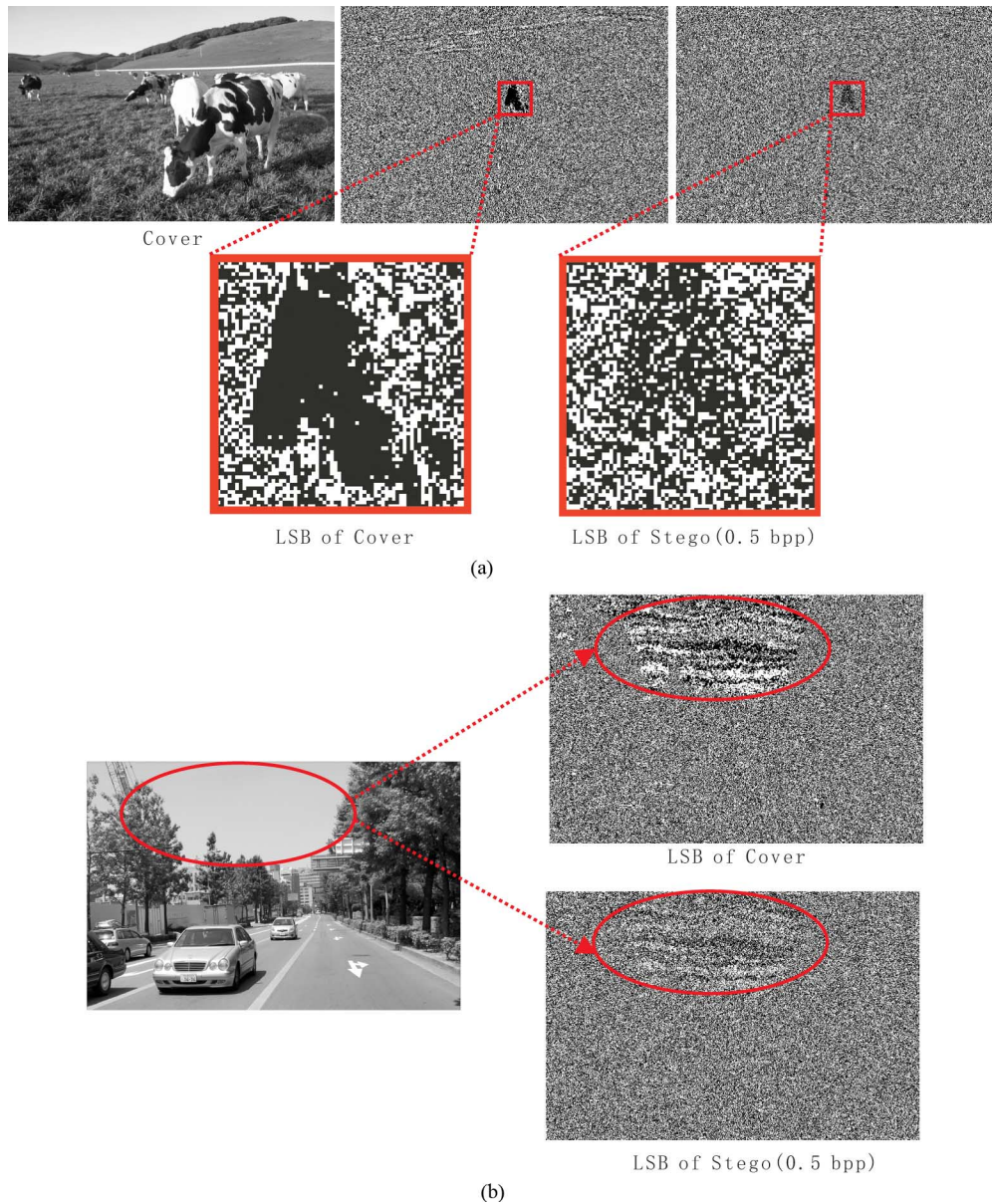
(a)

(b)

Fig. 3. LSB before and after random contamination by LSBM (a) Randomization in the small flat region (b) Randomization in the large texture region.

parameters, and then repeats region selection and capacity estimation until M can be embedded completely.

Please note that the parameters may be different for different image content and secret message M. We need them as side information to guarantee the validity of data extraction. In practice, such side information (7 bits in our work) can be embedded into a predetermined region of the image.

In data extraction, the scheme first extracts the side information from the stego image. Based on the side information, it then does some preprocessing and identifies the regions that have been used for data hiding. Finally, it obtains the secret message M according to the corresponding extraction algorithm.

In this paper, we apply such a region adaptive scheme to the spatial LSB domain. We use the absolute difference between two adjacent pixels as the criterion for region selection, and use LSBMR as the data hiding algorithm. The details of the data embedding and data extraction algorithms are as follows.
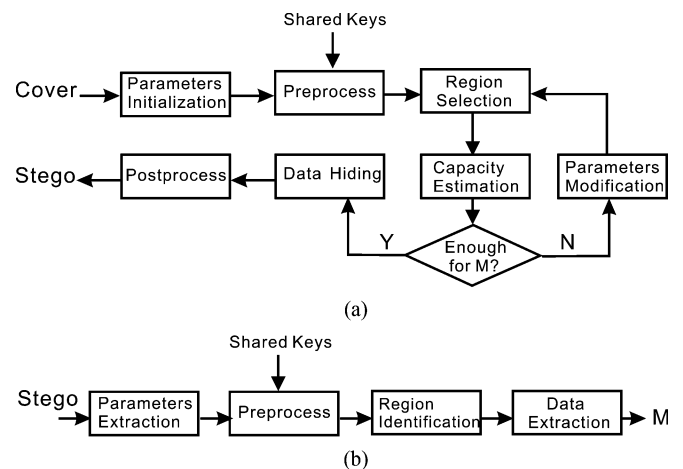

Fig. 4. Proposed scheme. (a) Data embedding. (b) Data extraction.

A. Data Embedding

- **Step 1**: The cover image of size of $m \times n$ is first divided into nonoverlapping blocks of $Bz \times Bz$ pixels. For each small block, we rotate it by a random degree in the range of $\{0, 90, 180, 270\}$, as determined by a secret key key_1. The resulting image is rearranged as a row vector V by raster scanning. And then the vector is divided into nonoverlapping embedding units with every two consecutive pixels (x_i, x_{i+1}), where $i = 1, 3, \ldots, mn - 1$, assuming n is an even number.

  Two benefits can be obtained by the random rotation. First, it can prevent the detector from getting the correct embedding units without the rotation key key_1, and thus security is improved. Furthermore, both horizontal and vertical edges (pixel pairs) within the cover image can be used for data hiding.

- **Step 2**: According to the scheme of LSBMR, 2 secret bits can be embedded into each embedding unit. Therefore, for a given secret message M, the threshold T for region selection can be determined as follows. Let $EU(t)$ be the set of pixel pairs whose absolute differences are greater than or equal to a parameter t

$$EU(t) = \{(x_i, x_{i+1}) \mid |x_i - x_{i+1}| \geq t, \forall (x_i, x_{i+1}) \in V\}.$$

Then we calculate the threshold T by

$$T = \arg\max_t \{2 \times |EU(t)| \geq |M|\}$$

where $t \in \{0, 1, \ldots, 31\}$, $|M|$ is the size of the secret message M, and $|EU(t)|$ denotes the total number of elements in the set of $EU(t)$.

Please note that when $T = 0$, the proposed method becomes the conventional LSBMR scheme, which means that our method can achieve the same payload capacity as LSBMR (except for 7 bits).

- **Step 3**: Performing data hiding on the set of

$$EU(T) = \{(x_i, x_{i+1}) \mid |x_i - x_{i+1}| \geq T, \forall (x_i, x_{i+1}) \in V\}.$$

We deal with the above embedding units in a pseudorandom order determined by a secret key key_2. For each unit (x_i, x_{i+1}), we perform the data hiding according to the following four cases.

Case #1: $\text{LSB}(x_i) = m_i$ & $f(x_i, x_{i+1}) = m_{i+1}$

$$(x'_i, x'_{i+1}) = (x_i, x_{i+1});$$

Case #2: $\text{LSB}(x_i) = m_i$ & $f(x_i, x_{i+1}) \neq m_{i+1}$

$$(x'_i, x'_{i+1}) = (x_i, x_{i+1} + r);$$

Case #3: $\text{LSB}(x_i) \neq m_i$ & $f(x_i - 1, x_{i+1}) = m_{i+1}$

$$(x'_i, x'_{i+1}) = (x_i - 1, x_{i+1});$$

Case #4: $\text{LSB}(x_i) \neq m_i$ & $f(x_i - 1, x_{i+1}) \neq m_{i+1}$

$$(x'_i, x'_{i+1}) = (x_i + 1, x_{i+1})$$

where m_i and m_{i+1} denote two secret bits to be embedded. The function f is defined as $f(a, b) = \text{LSB}(\lfloor a/2 \rfloor + b)$. r is a random value in $\{-1, +1\}$ and (x'_i, x'_{i+1}) denotes the pixel pair after data hiding.

After the above modifications, x'_i and x'_{i+1} may be out of $[0, 255]$, or the new difference $|x'_{i+1} - x'_i|$ may be less than the threshold T. In such cases,[1] we need to readjust them as (x''_i, x''_{i+1}) by $(x''_i, x''_{i+1}) = \arg\min_{(e_1, e_2)} \{|e_1 - x_i| + |e_2 - x_{i+1}| \mid e_1 = x'_i + 4k_1, e_2 = x'_{i+1} + 2k_2, |e_1 - e_2| \geq T, 0 \leq e_1, e_2 \leq 255, 0 \leq T \leq 31, k_1, k_2 \in Z\}$. (∗)
Finally, we have

$$\text{LSB}(x''_i) = m_i, f(x''_i, x''_{i+1}) = m_{i+1}$$

where $0 \leq x''_i, x''_{i+1} \leq 255, |x''_i - x''_{i+1}| \geq T$. Please refer to the Appendix for the proof of the existence of solutions.

- **Step 4**: After data hiding, the resulting image is divided into nonoverlapping $Bz \times Bz$ blocks. The blocks are then rotated by a random number of degrees based on key_1. The process is very similar to **Step 1** except that the random degrees are opposite. Then we embed the two parameters (T, Bz) into a preset region which has not been used for data hiding.

Please note that there are two parameters in our approach. The first one is the block size Bz for block dividing in data preprocessing; another is the threshold T for embedding region selection. In this paper, Bz is randomly selected from the set of $\{1, 4, 8, 12\}$, T belongs to $\{0, 1, \ldots, 31\}$ and can be determined by the image contents and the secret message M (please refer to **Step 2**). In all, only 7 ($7 = \log_2(4) + \log_2(32)$) bits of side information are needed for each image.

Here, an example is shown. Assume that we are dealing with an embedding unit $(x_i, x_{i+1}) = (62, 81)$, $m_i = 1, m_{i+1} = 0$, $T = 19$. It is easy to verify that $|x_{i+1} - x_i| = 19 \geq T$ and

$$\text{LSB}(62) = 0 \neq m_i, \text{LSB}\left(\left\lfloor \frac{(62 - 1)}{2} \right\rfloor + 81\right)$$
$$= 1 \neq m_{i+1}.$$

Therefore, we invoke Case #4 and obtain

$$(x'_i, x'_{i+1}) = (x_i + 1, x_{i+1}) = (63, 81).$$

Then the new difference becomes $d' = |81 - 63| = 18 < T$. We need to readjust them according to the formula (∗) and finally get $k_1 = 0, k_2 = 1$

$$x''_i = x'_i + 4k_1 = 63 + 4 \times 0 = 63$$
$$x''_{i+1} = x'_{i+1} + 2k_2 = 81 + 2 \times 1 = 83.$$

In such a case, we have $d'' = |83 - 63| = 20 \geq T$ and

$$\text{LSB}(63) = m_i, \text{LSB}\left(\left\lfloor \left(\frac{63}{2}\right) \right\rfloor + 83\right) = m_{i+1}.$$

---

[1]It is noted that such cases occur with a low probability according to our experiments. Please compare the average modification rates between LSBMR and our proposed method in Table I.
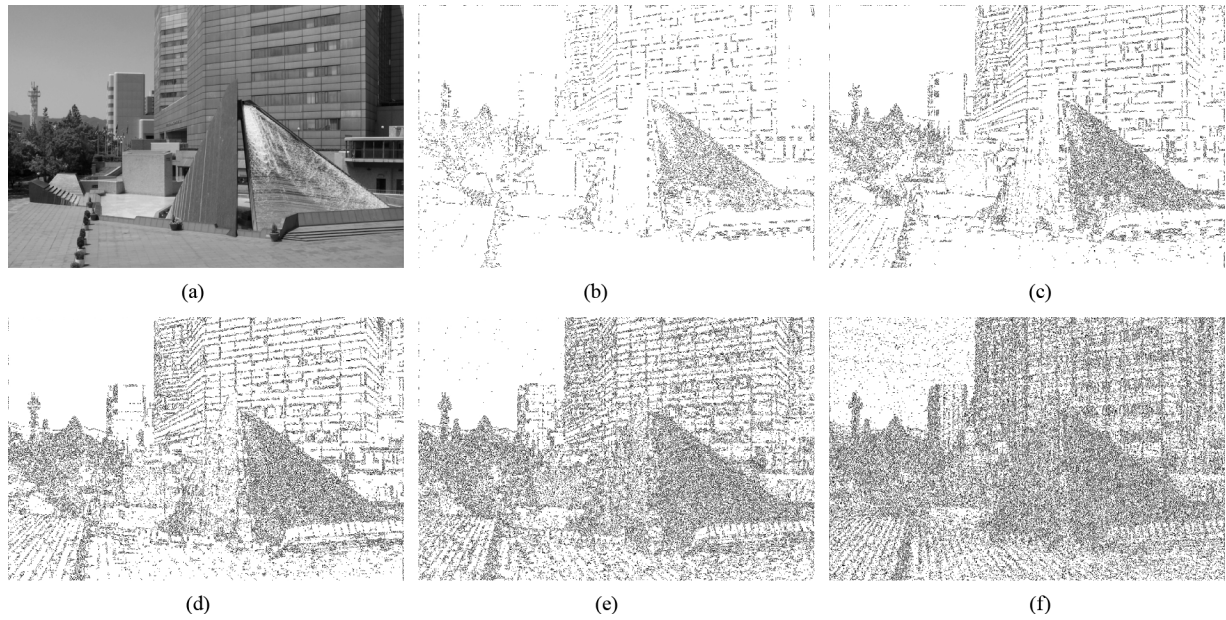
Fig. 5. (a) Cover image. (b)–(f) Positions of those modified pixels (black pixels) after data hiding using our proposed method with embedding rates of 10%, 20%, 30%, 40%, and 50%, respectively. It is observed that at lower embedding rates, e.g., 10%–40%, only sharper edges (such as the edge regions in the buildings etc.) within the cover image are used, while keeping those smooth regions (such as the smooth sky in the top left corner) as they are. When the embedding rate increases, more regions can be released adaptively by decreasing the threshold T. For instance, in the case of 50%, many embedding units in the sky are also used for data hiding. (a) Cover image. (b) 10%, $T = 21$. (c) 20%, $T = 9$. (d) 30%, $T = 5$. (e) 40%, $T = 3$. (f) 50%, $T = 2$.

B. Data Extraction

To extract data, we first extract the side information, i.e., the block size Bz and the threshold T from the stego image. We then do exactly the same things as **Step 1** in data embedding. The stego image is divided into $Bz \times Bz$ blocks and the blocks are then rotated by random degrees based on the secret key key_1. The resulting image is rearranged as a row vector V'. Finally, we get the embedding units by dividing V' into nonoverlapping blocks with two consecutive pixels.

We travel the embedding units whose absolute differences are greater than or equal to the threshold T according to a pseudorandom order based on the secret key key_2, until all the hidden bits are extracted completely. For each qualified embedding unit, say, (x'_i, x'_{i+1}), where $|x'_{i+1} - x'_i| \geq T$, we extract the two secret bits m_i, m_{i+1} as follows:

$$m_i = \text{LSB}(x''_i), m_{i+1} = \text{LSB}\left(\left\lfloor \frac{x'_i}{2} \right\rfloor + x'_{i+1}\right).$$

For instance, we are dealing with the unit $(x'_i, x'_{i+1}) = (63, 83)$ with $T = 19$. We eventually get the secret bits by

$$m_i = \text{LSB}(63) = 1, \quad m_{i+1} = \text{LSB}\left(\left\lfloor \frac{63}{2} \right\rfloor + 83\right) = 0.$$

IV. Experimental Results and Analysis

In this section, we will present some experimental results to demonstrate the effectiveness of our proposed method compared with existing relevant methods as mentioned in Section II. Three image datasets have been used for algorithm evaluation, UCID [22] including 1338 uncompressed color images with a size of 384×512 or 512×384, NJIT dataset including 3680 uncompressed color images with a size of either 512×768 or 768×512, which were taken with different kinds of camera, and our dataset SYSU including 982 TIFF color images with a size of 640×480. In all, there are 6000 original uncompressed color images including (but not limited to) landscapes, people, plants, animals, and buildings. All the images have been converted into grayscale images in the following experiments.

A. Embedding Capacity and Image Quality Analysis

One of the important properties of our steganographic method is that it can first choose the sharper edge regions for data hiding according to the size of the secret message by adjusting a threshold T. As illustrated in Fig. 5, the larger the number of secret bits to be embedded, the smaller the threshold T becomes, which means that more embedding units with lower gradients in the cover image can be released (please refer to the definition of $EU(T)$ in **Step 3** in data embedding). When T is 0, all the embedding units within the cover become available. In such a case, our method can achieve the maximum embedding capacity of 100% (100% means 1 bpp on average for all the methods in this paper), and therefore, the embedding capacity of our proposed method is almost the same as the LSBM and LSBMR methods except for 7 additional bits.

From Fig. 5, it can also be observed that most secret bits are hidden within the edge regions when the embedding rate is low, e.g., less than 30% in the example, while keeping those smooth regions such as the sky in the top left corner as they are. Therefore, the subjective quality of our stegos would be improved based on the human visual system (HVS) characteristics.

Table I shows the average PSNR, weight-PSNR (wPSNR is a better image quality metric adopted in Checkmark Version 1.2
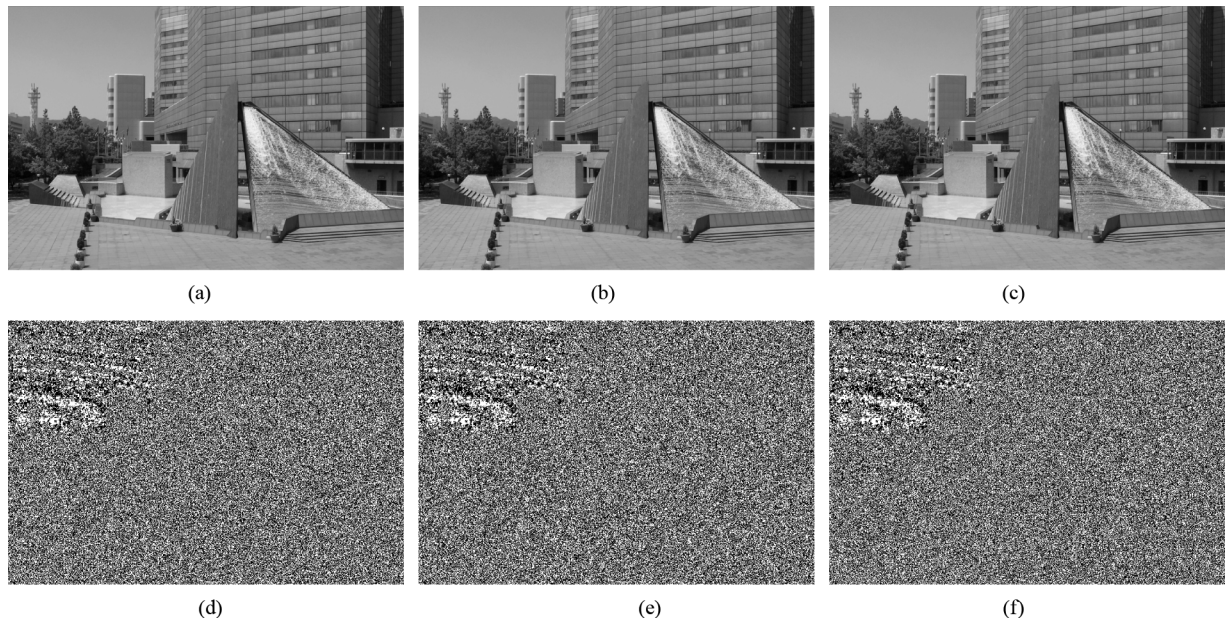
Fig. 6. LSB planes of the cover image and its stego images using our proposed method. It is observed that there are no obvious visual traces leaving along the embedded content edges [please refer to Fig. 5(d) and (f)] after data hiding. Furthermore, most texture information in smooth regions (upper-left corner) can be well preserved. (a) Cover image. (b) Stego with 30%. (c) Stego with 50%. (d) LSB of cover. (e) LSB of stego with 30%. (f) LSB of stego with 50%.

[23]. It takes into account HVS characteristics and improves the classical PSNR by

$$\mathrm{wPSNR} = 10 \log_{10} \frac{\max(x)^2}{\|\mathrm{NVF}(x' - x)\|^2}$$

where x is the cover image and x' is the stego image. NVF denotes the noise visibility function [24]) and the average modification rate over 6000 images with different embedding rates for the seven steganographic methods.

For the average PSNR, it is observed that the LSBMR method performs best since it employs the ± 1 embedding scheme and its modification rate is lower than the others except for the AE-LSB method. Please note that the value of PSNR is independent of the location of the modified pixels. Thus the average PSNR of our proposed method will be slightly lower than that of LSBMR since some embedding units need to be readjusted to guarantee the correct data extraction (please refer to the Appendix for more details) in the proposed method.

For the average wPSNR, the performances of the HBC and our proposed methods are very similar and usually outperform the others. The reason is that the modified pixels using both methods always locate at the sharper edges within covers while preserving the smoother regions after data hiding [please refer to Figs. 1(g) and 5(b)–(f)]. According to the NVF in [24], the weighting for the changes in sharper regions is smaller than those in smoother regions, which means the values of wPSNR should become higher than those of stegos with the random embedding scheme.

For the average modification rate, the AE-LSB method is always the lowest. The reason is that according to the embedding procedure of AE-LSB, the average payload capacity for each single pixel is the largest among the schemes, which means that fewer pixels need to be modified at the same embedding capacity. Please note that the average modification rates of LSBM

and HBC are the same and equal to one half of the embedding rate or 4/3 of the modification rate of LSBMR.

On the whole, the object qualities including PSNR and wPSNR of our stegos are nearly the best among the seven steganographic methods (please compare the underlined values and those values in brackets).

B. Visual Attack

Although our method embeds the secret message bits by changing those pixels along the edge regions, it would not leave any obvious visual artifacts in the LSB planes of the stegos based on our extensive experiments. Fig. 6 shows the LSB of the cover and its stegos using our proposed method with an embedding rate of 30% and 50%, respectively. It is observed that there is no visual trace like those shown in Fig. 5(d) and (f); also, most smooth regions such as the sky in the upper-left corner are well preserved. While for the LSBM, LSBMR, and some PVD-based methods with the random embedding scheme, the smooth regions would be inevitably disturbed and thus become more random. Fig. 7 shows the LSB planes of the cover and its stegos using the seven steganographic methods with the same embedding rate of 50%, respectively. It is observed that the LSB planes of stegos using the LSBM, LSBMR, PVD, and IPVD methods (especially for the LSBM due to its higher modification rate) look more random compared with others. On zooming in, these artifacts are more clearly observed, as illustrated in Fig. 3. Please note that the smooth regions can also be preserved for HBC, and less smooth regions will be contaminated for AE-LSB due to its lower modification rate as shown in Table I.

C. Statistical Attack

1) RS Analysis: RS steganalysis [3] is one of the famous methods for detecting stegos with LSB replacement and for es-
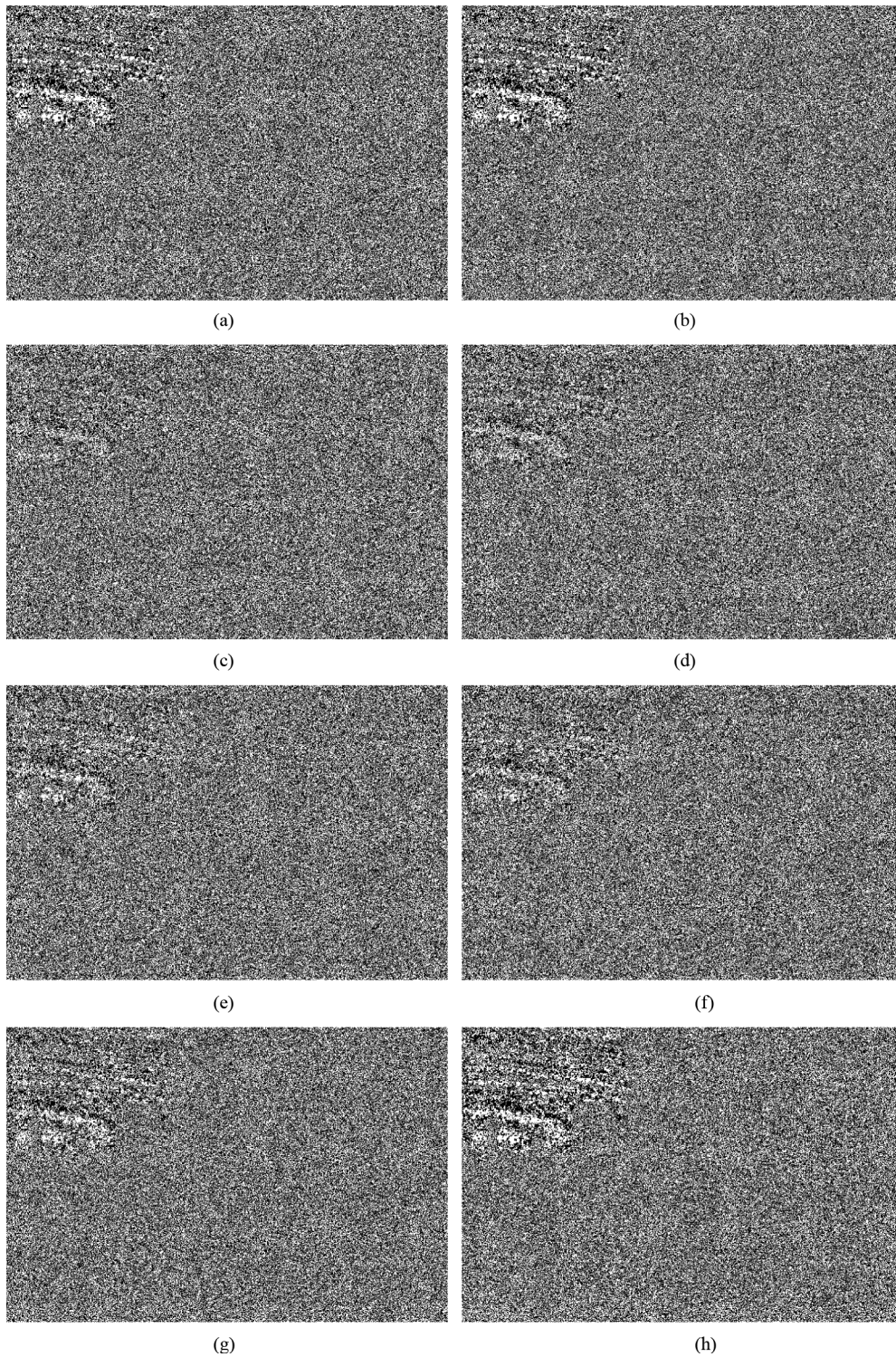
Fig. 7. LSB planes of cover [Fig. 6(a)] and stego images with the seven steganographic methods at the same embedding rate of 50%. (a) LSB of cover. (b) LSB of our stego. (c) LSB of LSBM stego. (d) LSB of LSBMR stego. (e) LSB of PVD stego. (f) LSB of IPVD stego. (g) LSB of stego with AE-LSB. (h) LSB of stego with HBC.

timating the size of the hidden message. In this test, we employ this steganalysis to evaluate the security of our proposed method and HBC method.

Since the HBC can be regarded as a special case (edge adaptive) of LSB replacement, the structural asymmetry artifacts introduced by LSB replacement can be reflected in the corresponding RS diagram. As shown in Fig. 8(a), the difference be-

tween $R_M(S_M)$ and $R_{-M}(S_{-M})$ will become larger with increasing the embedding rates. While our proposed method is actually an LSBM-based scheme, these LSB replacement style artifacts will be easily avoided and thus the RS steganalysis is ineffective at detecting our stegos. As shown in Fig. 8(b), the difference between $R_M(S_M)$ and $R_{-M}(S_{-M})$ remains close even with an embedding rate of 100%.

TABLE II
AVERAGE ACCURACY (%) OF RS FEATURES SET ON FLD WITH DIFFERENT EMBEDDING RATES. VALUES WITH AN ASTERISK (*) DENOTE THE MINIMUM
ACCURACY OF THE TWO STEGANOGRAPHIC ALGORITHMS

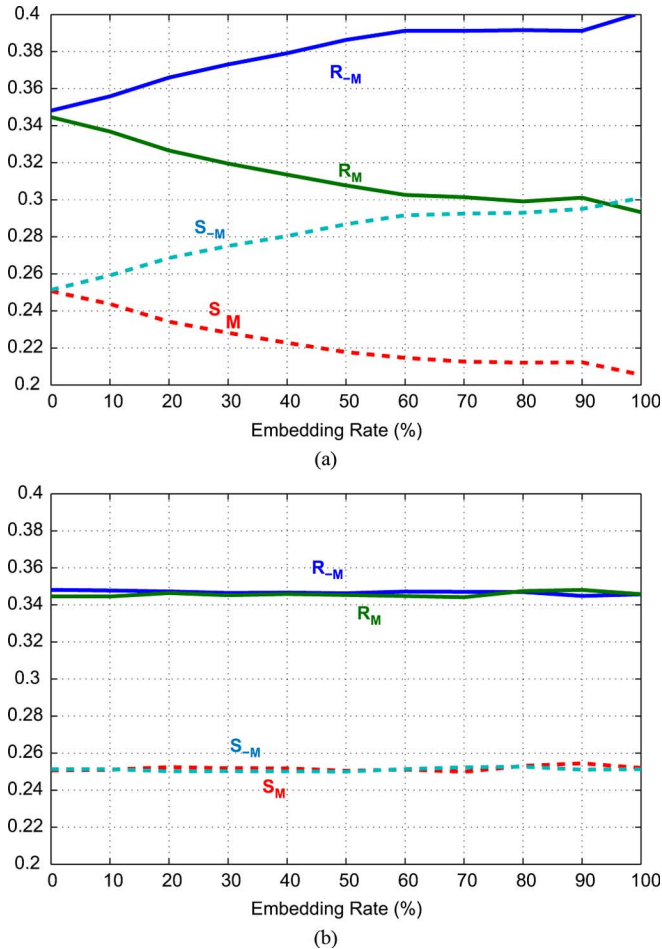| Embedding Rate Methods	10%	20%	30%	40%	50%
HBC	88.07	92.96	94.99	97.05	98.52
Proposed	**50.21 ***	**50.60 ***	**50.45 ***	**50.66 ***	**51.12 ***

Fig. 8. RS diagram of gray Pepper image with size of 512×512. The x-axis denotes the embedding rate and the y-axis denotes the relative percentages of regular and singular groups with marks M and $-M$, where $M = [0\ 1\ 1\ 0]$. (a) RS diagram for HBC. (b) RS diagram for our proposed.

To further test the security of our method with HBC method, we use the 4-D RS features, namely R_M, S_M, R_{-M}, S_{-M}, to differentiate natural cover images from their stego counterparts. At each embedding rate, the original samples (including covers and their stegos counterparts) are first randomly partitioned into ten nonoverlapping subsamples. And then a single subsample is retained as the testing data, and the remaining nine subsamples are used as training data. In the experiments, a Fisher linear discriminant (FLD) classifier is employed. Table II shows the average detection results for different embedding rates which are averaged over 10 times for splitting the testing data and training data alternately. It is clearly observed that the RS steganalysis is very effective at detecting the stego images using the HBC method even at a low embedding rate, e.g., 10%, while it fails to detect our stegos (close to the random 50% guessing for all embedding rates).

2) Two Specific Feature Sets: According to the embedding procedures in Section III-A, our proposed scheme can be classified as an edge adaptive scheme based on LSBM. Therefore, the two following specific feature sets for LSBM have been employed to evaluate the security of our method and of two other LSB-based steganographic methods, i.e., LSBM and LSBMR.

a) **Li-1D** [10]. Calculate the calibration-based detectors (e.g., calibrated HCF COM) as the difference between adjacent pixels within an image. The experimental results in [10] shows that the method outperforms the previous calibrated HCF COM methods in [8].

b) **Huang-1D** [9]. Calculate the alteration rate of the number of neighborhood gray levels. Unlike the HCF COM-based methods [8], [10], it detects the statistical changes of those overlapping flat blocks with 3×3 pixels in the first two bit planes after re-embedding operations.

The receiver operating characteristic (ROC) curves are shown in Fig. 9. It can be clearly observed that both specific steganalytic algorithms would fail (still getting closer to the random guessing) in detecting our proposed method even when the embedding rate is as high as 75%, while they obtain satisfactory results for detecting stegos using LSBM and LSMR methods.

Please note that for a given false positive rate (FPR), the true positive rate (TPR) of LSBMR is slightly lower than LSBM. One of the reasons may be that both methods employ the ± 1 embedding scheme. However, as shown in Table I, the modification rate of LSBMR is slightly lower than LSBM at the same embedding rate. And similar detection results can also be observed from the following tests.

3) Four Universal Feature Sets: In this subsection, we employ the following four universal feature sets to further evaluate the security of our proposed steganographic scheme and the other six relevant ones, including two typical LSB based and four edge-based schemes.

a) **Shi-78D** [11]. The statistical moments of characteristic functions (CFs) of the prediction error image, the test image, and their wavelet subbands are employed to reflect the differentiation property of the associated histogram between cover and stego images. (78 Dimension).

b) **Farid-72D** [25]. The higher-order statistical moments taken from a multiscale decomposition, which includes basic coefficient statistics as well as error statistics based on an optimal linear predictor, are employed to capture certain natural properties of cover images. (72 Dimension).

c) **Moulin-156D** [26]. Features are extracted from both empirical probability density functions (pdfs) moments and the normalized absolute CF. In our experiments, we follow the extraction scheme proposed in paper [26] but without feature selection processing. The highest
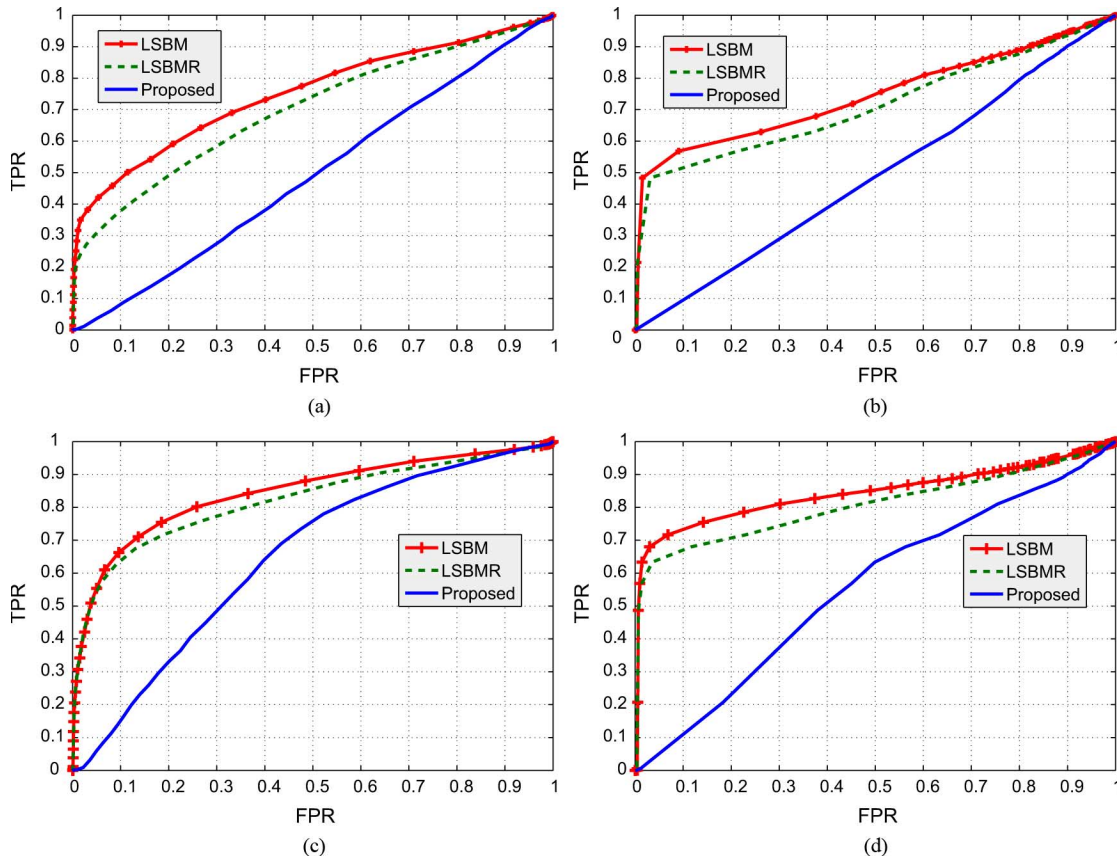
Fig. 9. ROC curves for three LSBM-based steganographic methods with two specific steganalytic algorithms. The x-coordinate and y-coordinate denote the FPR (false positive rate) and TPR (true positive rate), respectively. (a) 50% using Li-1D [10]. (b) 50% using Huang-1D [9]. (c) 75% using Li-1D [10]. (d) 75% using Huang-1D [9].

statistical order is set as $N = 6$, so we get 156 dimension features.

d) **Li-110D** [12]. Steganalytic features are extracted from the normalized histogram of the local linear transform coefficients [27] of the image. The experimental results in [12] show that these features can capture certain changes of the local textures before and after data embedding, and thus can detect the presence of a hidden message, especially for some adaptive steganographic algorithms, such as MBNS [28], MPB [29], and JPEG2000 BPCS [30], effectively even with low embedding rates, for instance 10% (110 Dimension).

In the experiments, we first create the stego images using the seven steganographic methods with different embedding rates ranging from 10% to 50% with a step of 10%. And then extract those image features as mentioned above both for the cover and stego images. The FLD classifier is also used for the classification. Table III shows the detection accuracy which is averaged over the results of a ten-fold cross-validation just as it did in Section IV-C1. From Table III, it can be observed that our proposed method outperforms the other six relevant methods nearly for all the situations, especially for the stegos with lower embedding rates, e.g., less than 30%.

For example, when the embedding rate is 20%, our maximum accuracy is 59.29%, that is around 20% improvement on the typical LSB-based methods including LSBM and LSBMR. When the embedding rate increases, say 50%, our results will

get closer to the performance of the LSBMR method. The reason is that the sharper edge regions within cover images are not numerous enough for hiding a secret message of such a large size; the method has to decrease the threshold T to release more smooth/flat regions. For instance, the embedding units whose absolute differences are larger than or equal to 2 of the image as shown in Fig. 5(f) have been used for data hiding, which would lead to poor security based on our extensive experiments. Please note that unlike the digital watermarking or fingerprinting hiding techniques, the steganographer has the freedom to select the cover image and/or steganography to carry the message [20]. In practice, we can select those cover images with good hiding characteristics, namely the covers with more edge regions using our proposed scheme. Therefore, for a given secret message, the threshold T can be used as a blind criterion for cover image selection. Usually the larger the threshold T, the larger the number of sharp edges within the selected cover, and thus the higher the security achieved.

Based on experiments, we also observe that the performances of the first three edge-based schemes, i.e., PVD, IPVD, and AE-LSB, are poorer than the LSB-based approaches. For the HBC method, its performance is similar to our method although it can be easily detected by the RS analysis (please refer to Table II), which indicates that it is more difficult to detect those pixel changes that along the edges regions using the four universal feature sets.

TABLE III

AVERAGE ACCURACY (%) OF EACH FEATURE SET ON FLD WITH DIFFERENT EMBEDDING RATES. VALUES WITH AN ASTERISK (*) DENOTE THE MINIMUM
ACCURACY AMONG THE SEVEN STEGANOGRAPHIC ALGORITHMS

Embedding Rate	Steganographic Algorithms		Shi 78-D	Farid 72-D	Moulin 156-D	Li 110-D	Max. Accuracy
10%	LSB-Based	LSBM	69.39	55.04	57.61	74.11	74.11
		LSBMR	68.01	56.83	57.51	72.90	72.90
	Edge-Based	PVD	83.96	77.68	86.21	84.93	86.21
		IPVD	75.58	68.86	75.97	80.42	80.42
		AE-LSB	80.90	68.17	77.91	82.18	82.18
		HBC	54.31	50.68	**51.23 ***	54.61	54.61
	Our Proposed		**52.56 ***	**50.56 ***	51.39	**52.94 ***	**52.94 ***
20%	LSB-Based	LSBM	77.05	59.29	65.22	79.21	79.21
		LSBMR	75.30	60.68	63.61	78.01	78.01
	Edge-Based	PVD	91.15	85.68	90.95	88.15	91.15
		IPVD	84.54	75.27	83.74	84.85	84.85
		AE-LSB	88.19	74.25	86.46	87.86	88.19
		HBC	62.15	52.25	53.74	59.24	62.15
	Our Proposed		**59.29 ***	**51.84 ***	**53.26 ***	**56.59 ***	**59.29 ***
30%	LSB-Based	LSBM	80.92	63.14	69.91	82.05	82.05
		LSBMR	79.78	63.50	67.72	81.01	81.01
	Edge-Based	PVD	94.31	89.58	92.85	89.86	94.31
		IPVD	88.29	78.41	86.89	86.96	88.29
		AE-LSB	90.62	77.12	89.75	89.36	90.62
		HBC	70.80	55.44	57.72	65.92	70.80
	Our Proposed		**67.48 ***	**54.59 ***	**57.49 ***	**63.16 ***	**67.48 ***
40%	LSB-Based	LSBM	83.90	66.05	73.40	83.86	83.90
		LSBMR	83.09	65.90	71.40	83.30	83.30
	Edge-Based	PVD	95.84	91.87	94.15	90.78	95.84
		IPVD	90.47	80.41	88.61	88.61	90.47
		AE-LSB	91.88	79.10	91.36	89.97	91.88
		HBC	78.48	60.10	**62.45 ***	73.58	78.48
	Our Proposed		**76.62 ***	**58.96 ***	63.80	**71.01 ***	**76.62 ***
50%	LSB-Based	LSBM	86.08	68.20	77.23	85.13	86.08
		LSBMR	85.13	67.70	75.29	84.46	85.13
	Edge-Based	PVD	96.80	93.13	94.99	91.79	96.80
		IPVD	91.97	82.16	89.42	89.59	91.97
		AE-LSB	92.98	80.50	92.29	90.49	92.98
		HBC	84.00	64.26	**68.95 ***	79.92	84.00
	Our Proposed		**83.24 ***	**63.99 ***	69.63	**77.05 ***	**83.24 ***

V. CONCLUDING REMARKS

In this paper, an edge adaptive image steganographic scheme in the spatial LSB domain is studied. As pointed out in Section II, there usually exists some smooth regions in natural images, which would cause the LSB of cover images not to be completely random or even to contain some texture information just like those in higher bit planes. If embedding a message in these regions, the LSB of stego images becomes more random, and according to our analysis and extensive experiments, it is easier to detect. In most previous steganographic schemes, however, the pixel/pixel-pair selection is mainly determined by a PRNG without considering the relationship between the characteristics of content regions and the size of the secret message to be embedded, which means that those smooth/flat regions will be also contaminated by such a random selection scheme even if there are many available edge regions with good hiding characteristics. To preserve the statistical and visual features in cover images, we have proposed a novel scheme which can first embed the secret message into the sharper edge regions adaptively according to a threshold determined by the size of the secret message and the gradients of the content edges. The experimental results evaluated on thousands of natural images using different kinds of steganalytic algorithms show that both visual quality and security of our stego images are improved significantly compared to typical LSB-based approaches and their edge adaptive versions.

Furthermore, it is expected that our adaptive idea can be extended to other steganographic methods such as audio/video steganography in the spatial or frequency domains when the embedding rate is less than the maximal amount.

APPENDIX

In the Appendix, we prove that for every embedding unit (x_i, x_{i+1}) in the cover image, where $d = |x_i - x_{i+1}| \geq T$, $T \in \{0, 1, 2, \ldots, 31\}$, our proposed algorithm can modify it as a new pair (x_i'', x_{i+1}'') with the least distortion according to formula (*), under conditions that $\mathrm{LSB}(x_i'') = m_i$, $f(x_i'', x_{i+1}'') = m_{i+1}$, and $0 \leq x_i'', x_{i+1}'' \leq 255$, $|x_i'' - x_{i+1}''| \geq T$. This is very important in order to guarantee that we can distinguish the same selected regions before and after data embedding with the same threshold T.

Proof: First, we show some important properties of the binary function $f(a, b) = \mathrm{LSB}(\lfloor a/2 \rfloor + b)$ as follows:

$$f(a, b) \neq f(a, b \pm 1),\ f(a-1, b) \neq f(a+1, b),\ \forall a, b \in Z. \quad (1)$$

Then we have

$$f(a,b) = f(a, b + 2k_2)$$
$$f(a,b) = f(a + 4k_1, b), \forall b, k_1, k_2 \in Z. \tag{2}$$

We formulate the four cases as described in Section III-A **Step 3** as follows:

$$x'_i = x_i + r_1, x'_{i+1} = x_{i+1} + r_2$$

where $r_1, r_2 \in \{0, -1, +1\}, |r_1| + |r_2| \leq 1$.

Based on the embedding process and the formula (1), it is easy to verify that the modified pixel pair (x'_i, x'_{i+1}) satisfies

$$\text{LSB}(x'_i) = m_i, f(x'_i, x'_{i+1}) = m_{i+1}. \tag{3}$$

If (x'_i, x'_{i+1}) is out of range $[0, 255]$, or the new difference $d' = |x'_i - x'_{i+1}| < T$, then we need to readjust them as follows. To preserve the property (3), we limit

$$x''_i = x'_i + 4k_1, x''_{i+1} = x'_{i+1} + 2k_2, \forall k_1, k_2 \in Z.$$

Based on formula (2), we have: $\text{LSB}(x''_i) = m_i, f(x''_i, x''_{i+1}) = m_{i+1}$.

In the following, we are going to show that there always exists $k_1, k_2 \in Z$, s.t.

$$0 \leq x''_i, x''_{i+1} \leq 255, |x''_i - x''_{i+1}| \geq T.$$

Without loss of generality, assume that $0 \leq x_i < x_{i+1} \leq 255$. Then we need to readjust (x'_i, x'_{i+1}) in the following two cases.

Case #1. x'_i or x'_{i+1} is out of range $[0, 255]$, then only one of the following two subcases would happen.

- **Case #1.1.** $x_i = 0, r_1 = -1, r_2 = 0$.

  $$(x'_i = x_i - 1 = 0 - 1 = -1, x''_{i+1} = x_{i+1}).$$

  Then $d' = |x'_{i+1} - x'_i| = x_{i+1} - (x_i - 1) = d + 1 \geq T + 1$.
  —If $d \leq 34$, then $x'_{i+1} = 0 + d \leq 34$, we let $x''_i = x'_i + 4 = -1 + 4 = 3, x''_{i+1} = x'_{i+1} + 4 \leq 38(k_1 = 1, k_2 = 2)$, then $d'' = d' = d + 1 \geq T$.
  —If $d > 34$, then $x'_{i+1} = 0 + d > 34$, we let $x''_i = x'_i + 4 = -1 + 4 = 3, x''_{i+1} = x'_{i+1}(k_1 = 1, k_2 = 0)$, then $d'' = |x''_{i+1} - x''_i| = x_{i+1} - (x_i - 1 + 4) = d - 3 > 31 = max(T) \geq T$.
- **Case #1.2.** $x_{i+1} = 255, r_1 = 0, r_2 = +1$.

  $$(x'_i = x_i, x'_{i+1} = x_{i+1} + 1 = 255 + 1 = 256).$$

  The analysis is similar to **Case #1.1.**

Case #2. $d = T, d' = |x'_{i+1} - x'_i| = d - 1 = T - 1 < T$. In such a case, both x'_i and x'_{i+1} must be in the region of $[0, 255]$. We let

$$R_l = [0, x'_i), R_r = (x'_{i+1}, 255].$$

Since $|R_l| + d + |R_r| = 256$, then $d = 256 - |R_l| - |R_r| = T \leq max(T) = 31$, then we have $|R_l| + |R_r| \geq 256 - 31 = 225$. Therefore, there must exist a region R_l or R_r which satisfies $|R_l| \geq 4$ or $|R_r| \geq 2$. Otherwise, we have $|R_l| + |R_r| < 4 + 2 = 6$, get contradiction.

- If $|R_r| \geq 2$, then we let $x''_i = x'_i, x''_{i+1} = x'_{i+1} + 2 \leq 255(k_1 = 0, k_2 = 1)$, then $d'' = d' + 2 = T - 1 + 2 = T + 1 \geq T$.
- If $|R_l| \geq 4$ & $|R_r| < 2$, then we let $x''_i = x'_i - 4 \geq 0, x''_{i+1} = x'_{i+1}(k_1 = -1, k_2 = 0)$, then $d'' = d' + 4 = T - 1 + 4 = T + 3 \geq T$. $\qquad \square$

REFERENCES

[1] J. Mielikainen, "LSB matching revisited," *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 285–287, May 2006.
[2] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Proc. 3rd Int. Workshop on Information Hiding*, 1999, vol. 1768, pp. 61–76.
[3] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images," *IEEE Multimedia*, vol. 8, no. 4, pp. 22–28, Oct. 2001.
[4] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," *IEEE Trans. Signal Process.*, vol. 51, no. 7, pp. 1995–2007, Jul. 2003.
[5] A. D. Ker, "A general framework for structural steganalysis of LSB replacement," in *Proc. 7th Int. Workshop on Information Hiding*, 2005, vol. 3427, pp. 296–311.
[6] A. D. Ker, "A fusion of maximum likelihood and structural steganalysis," in *Proc. 9th Int. Workshop on Information Hiding*, 2007, vol. 4567, pp. 204–219.
[7] J. Harmsen and W. Pearlman, "Steganalysis of additive-noise modelable information hiding," *Proc. SPIE Electronic Imaging*, vol. 5020, pp. 131–142, 2003.
[8] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Process. Lett.*, vol. 12, no. 6, pp. 441–444, Jun. 2005.
[9] F. Huang, B. Li, and J. Huang, "Attack LSB matching steganography by counting alteration rate of the number of neighbourhood gray levels," in *Proc. IEEE Int. Conf. Image Processing*, Oct. 16–19, 2007, vol. 1, pp. 401–404.
[10] X. Li, T. Zeng, and B. Yang, "Detecting LSB matching by applying calibration technique for difference image," in *Proc. 10th ACM Workshop on Multimedia and Security*, Oxford, U.K., 2008, pp. 133–138.
[11] Y. Q. Shi *et al.*, "Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network," in *Proc. IEEE Int. Conf. Multimedia and Expo*, Jul. 6–8, 2005, pp. 269–272.
[12] B. Li, J. Huang, and Y. Q. Shi, "Textural features based universal steganalysis," *Proc. SPIE on Security, Forensics, Steganography and Watermarking of Multimedia*, vol. 6819, p. 681912, 2008.
[13] M. Goljan, J. Fridrich, and T. Holotyak, "New blind steganalysis and its implications," *Proc. SPIE on Security, Forensics, Steganography and Watermarking of Multimedia*, vol. 6072, pp. 1–13, 2006.
[14] K. Hempstalk, "Hiding behind corners: Using edges in images for better steganography," in *Proc. Computing Women's Congress*, Hamilton, New Zealand, 2006.

[15] K. M. Singh, L. S. Singh, A. B. Singh, and K. S. Devi, "Hiding secret message in edges of the image," in *Proc. Int. Conf. Information and Communication Technology*, Mar. 2007, pp. 238–241.

[16] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Robust data hiding for images," in *Proc. IEEE on Digital Signal Processing Workshop*, Sep. 1996, pp. 37–40.

[17] D. Wu and W. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognit. Lett.*, vol. 24, pp. 1613–1626, 2003.

[18] X. Zhang and S. Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security," *Pattern Recognit. Lett.*, vol. 25, pp. 331–339, 2004.

[19] C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 488–497, Sep. 2008.

[20] M. Kharrazi, H. T. Sencar, and N. Memon, "Cover selection for steganographic embedding," in *Proc. IEEE Int. Conf. Image Processing*, Oct. 8–11, 2006, pp. 117–120.

[21] J. Fridrich, M. Goljan, and R. Du, "Steganalysis based on JPEG compatibility," in *Proc. Special Session on Theoretical and Practical Issues in Digital Watermarking and Data Hiding, Multimedia Systems and Applications IV*. Denver, Co: , 2001, pp. 275–280.

[22] G. Schaefer and M. Stich, "UCID: An uncompressed color image database," *Proc. SPIE Electronic Imaging, Storage and Retrieval Methods and Applications for Multimedia*, vol. 5307, pp. 472–480, 2003.

[23] S. Pereira, S. Voloshynovskiy, M. Madueno, S. Marchand-Maillet, and T. Pun, "Second generation benchmarking and application oriented evaluation," in *Proc. 4th Int. Workshop on Information Hiding*, 2001, vol. 2137, pp. 340–353.

[24] S. Voloshynovskiy, A. Herrigel, N. Baumgaertner, and T. Pun, "A stochastic approach to content adaptive digital image watermarking," in *Proc. 3th Int. Workshop on Information Hiding*, 1999, vol. 1768, pp. 211–236.

[25] H. Farid, "Detecting hidden messages using higher-order statistical models," in *Proc. IEEE Int. Conf. Image Processing*, Sep. 22–25, 2002, vol. 2, pp. 905–908.

[26] Y. Wang and P. Moulin, "Optimized feature extraction for learning-based image steganalysis," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 1, pp. 31–45, Mar. 2007.

[27] M. Unser, "Local linear transforms for texture measurements," *Signal Processing*, vol. 11, no. 1, pp. 61–79, 1986.

[28] X. Zhang and S. Wang, "Steganography using multiple-base notational system and human vison sensitivity," *IEEE Signal Process. Lett.*, vol. 12, no. 1, pp. 67–70, Jan. 2005.

[29] B. C. Nguyen, S. M. Yoon, and H. K. Lee, "Multi bit plane image steganography," in *Proc. 5th Int. Workshop on Digital Watermarking*, 2006, pp. 61–70.

[30] H. Noda and J. Spaulding, "Bit-plane decomposition steganography combine with JPEG2000 compression," in *Proc. 5th Int. Workshop on Information Hiding*, 2002, vol. 2578, pp. 295–309.
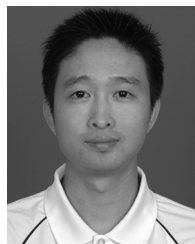
Weiqi Luo (S'07–M'09) received the Ph.D. degree from Sun Yat-Sen University, China, in 2008.

He is currently a postdoctoral researcher in Guangdong Key Laboratory of Information Security Technology, Guangzhou, China. His research interests include digital multimedia forensics, pattern recognition, steganography, and steganalysis.

Fangjun Huang (M'09) received the B.S. degree from Nanjing University of Science and Technology, China, in 1995, the M.S. and Ph.D. degrees from Huazhong University of Science and Technology, China, in 2002 and 2005, respectively.

Now, he is with the faculty at the School of Information Science and Technology, Sun Yat-Sen University, China. From June of 2008, he has been doing his postdoctoral research at the Department of Electrical and Computer Engineering, New Jersey Institute of Technology. His research interests include digital forensics and multimedia security.

Jiwu Huang (M'98–SM'00) received the B.S. degree from Xidian University, China, in 1982, the M.S. degree from Tsinghua University, China, in 1987, and the Ph.D. degree from the Institute of Automation, Chinese Academy of Science, in 1998.

He is currently a Professor with the School of Information Science and Technology, Sun Yat-Sen University, Guangzhou, China. His current research interests include multimedia forensics and security.

Dr. Huang has served as a Technical Program Committee member for many international conferences. He serves as a member of IEEE CAS Society Technical Committee of Multimedia Systems and Applications and the chair of IEEE CAS Society Guangzhou chapter. He is an associated editor of the *EURASIP Journal of Information Security*.