Contents lists available at ScienceDirect

Pattern Recognition

journal homepage: www.elsevier.com/locate/pr

Multilevel reversible data hiding based on histogram modification of difference images

Chia-Chen Lin[a,*], Wei-Liang Tai[b], Chin-Chen Chang[b,c]

[a]Department of Computer Science and Information Management, Providence University, Taichung 43301, Taiwan, ROC
[b]Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi 621, Taiwan, ROC
[c]Department of Information Engineering and Computer Science, Feng Chia University, Taichung 407, Taiwan, ROC

ARTICLE INFO

Article history:
Received 18 December 2007
Received in revised form 26 March 2008
Accepted 6 May 2008

Keywords:
Data hiding
Multilevel hiding strategy
Reversibility
Histogram

ABSTRACT

Reversible data hiding has drawn considerable attention in recent years. Reversibility allows original media to be completely recovered from marked media without distortion after embedded message has been extracted. In this paper we propose a multilevel reversible data hiding scheme based on the difference image histogram modification that uses the peak point to hide messages. Through a joint imperceptibility and hiding capacity evaluation, we show that our proposed scheme uses a multilevel hiding strategy to achieve large hiding capacity and keep distortion low. Performance comparisons with other existing reversible hiding schemes are provided to demonstrate the validity of our proposed scheme.

1. Introduction

Data hiding [1–4] refers to the process of embedding information into a cover object. Its applications can be classified into two categories according to the relationship between the cover image and the embedded message [5–7]. The first application is steganography, in which the embedded message has no relationship with the cover image. The cover image is just a decoy and is of no value to the recipient, and therefore the receiver has no interest in the original cover image. As a result, there is no demand to restore the original cover image after extraction of any embedded message.

The second application is digital watermarking. In this application, the embedded message is closely related to the cover image. The embedded message can supply additional information for the cover image, such as an authentication code, author's signature, and so on. Inevitably, hiding some data will change the cover image even though the distortion caused by hiding is imperceptible to the human visual system. However, for some sensitive images, such as military images, medical images or artwork preservation, even the slightest alteration in pixel values is intolerable. To make sure a sensitive image can be completely recovered after embedded messages are completely extracted, reversible data hiding, or so-called lossless data embedding, has been proposed. In this paper, a reversible data hiding scheme for the second application is proposed.

From the application point of view, reversible data hiding can be used as a fragile invertible authentication method that embeds an authentication code into a digital image in a lossless manner. Only an authenticated party could extract the embedded information and restore the marked image to its pristine state. The image is deemed authentic only if the embedded authentication code matches the extracted information. By embedding the message that has a close relationship to the host image, reversible data hiding provides a self-authentication scheme without requiring extra support. Related applications include embedding private information of patients into the corresponding medical images and providing lossless authentication watermarking for satellite images [8].

A general framework representing reversible data hiding is illustrated in Fig. 1. The sender embeds the message M to a host image H in a manner that the receiver could extract the embedded message and also recover the host image. The difference between marked image S and host image H is the distortion caused by the hiding process. Note that although the recovery phase guarantees the complete recovery of the original host image, it is still desired that the distortion caused by data hiding should be as small as possible.

Although the literature on reversible data hiding is scant, some interesting research has been presented recently. In 2001, Fridrich et al. [9] presented an invertible watermarking scheme to authenticate digital images in the JPEG domain. They used an order-2 function, which is an inverse function, to modify the quantization table to enable lossless embedding of one bit per DCT coefficient. For uncompressed image formats, Fridrich et al. [10] proposed the so-called RS scheme that is a lossless data hiding scheme with high payload by embedding bits into the status of groups of

[*] Corresponding author. Tel.: +886 4 26328001x18108; fax: +886 4 26324045.
E-mail addresses: mhlin3@pu.edu.tw (C.-C. Lin), taiwl@cs.ccu.edu.tw (W.-L. Tai), ccc@cs.ccu.edu.tw (C.-C. Chang).

0031-3203/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.patcog.2008.05.015

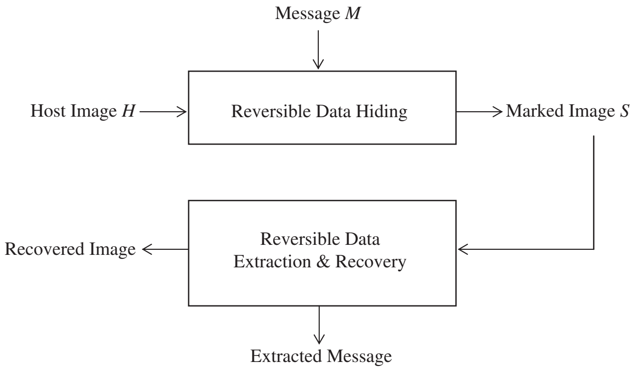

Fig. 1. General framework of reversible data hiding.

pixels. In 2003, De Vleeschouwer et al. [11] proposed a lossless watermarking algorithm that relies on circular interpretation of bijective transformations. In this approach, the histograms of quantized pixel values are mapped to a circle. The relative orientation of the histograms of two groups of pixels hides only one bit of an embedded message. Therefore, this scheme can achieve only limited hiding capacity. Later, Tian [12] proposed an interesting scheme for reversible data hiding called difference expansion (DE), whose kernel idea is to add, rather than replace, embedded messages in the resulting high-pass band of the Haar wavelet decomposition. Later, Alattar [13] proposed a reversible watermarking scheme for color images by using the DE of a generalized integer transform. Kamstra et al. [14] improved the DE scheme by using sorting to increase the efficiency of lossless compression. Thodi et al. [15] used a histogram shifting technique to embed the location map for solving the location map problem generated by DE, and also proposed a prediction-error expansion approach that better exploited the correlation inherent in the neighborhood of a pixel than the DE scheme. Celik et al. [16] proposed a lossless generalized-LSB data embedding scheme that is a generalization of the LSB-embedding method, called G-LSB. They transformed the embedded message using a variant of arithmetic encoding, then hidden the interval number in a cover image.

In 2006, Ni et al. [17] used the zero point and peak point of an image histogram to hide message and achieved reversibility. Their idea is very simple and causes only slight distortion with low complexity; however, their experimental results demonstrate that its largest hiding capacity is only about 5 kb when the test image is "Lena" (512×512×8 bits). Chang et al. [18,19] presented a reversible data hiding technique for lossy compression domain side match vector quantization (SMVQ). Finding redundant space in SMVQ-based compressed images is very difficult because SMVQ is a lossy low-bit-rate compression algorithm. To achieve reversibility, therefore, Chang et al. sorted the codebook and used adjacent indices to approximate codewords for conveying embedded messages. Hu et al. [20] proposed a reversible visible watermarking scheme for a new application scenario where the visible watermark servers as a tag or ownership identifier. In 2007, Lee et al. [21] proposed a high capacity reversible image watermarking scheme based on integer-to-integer wavelet transforms.

It does not matter whether scholars hide embedded messages in the spatial, frequency or compression domains. A common approach in reversible data hiding is to define a free space in an image first, also called the hiding area, then hide the embedded message in that area. To hide a larger payload in an image and maintain the highest possible image quality of a marked image at the same time, inspired by Ni et al.'s scheme [17] we explore the peak point of the histogram in pixel differences in an image, then slightly modify the pixel values to hide the embedded message. As we show later in this paper, our proposed scheme uses a multilevel hiding strategy to provide large hiding capacity while keeping distortion low.

The rest of this paper is organized as follows. The proposed multilevel reversible data hiding scheme, which includes evaluations of the lower bound of the peak signal-to-noise ratio (*PSNR*) and computational complexity, is presented in Section 2. Section 3 experimentally investigates the relationship between the hiding capacity and any resulting distortion, and discusses performance comparisons against other existing reversible data hiding schemes. Finally, concluding remarks appear in Section 4.

2. Proposed scheme

In this paper, we apply the peak point of a histogram in a difference image to generate an inverse transformation in the spatial domain to create free space. We also try to enhance the hiding capacity of the proposed scheme as much as possible to extend its potential applications. To give a better explanation in the following sections, we define several terms to be used in our proposed scheme here. The histogram for a given grayscale image, "Lena" (512×512 pixels in size), is shown in Fig. 2. The peak point corresponds to the grayscale value, which corresponds to the maximum number of pixels in the histogram of the given image. For example, in Fig. 2, the total number of pixels corresponding to the grayscale value "154" is 2787 and is depicted as $h(154) = 2787$, which is the largest pixel number compared with other grayscale values; therefore, the peak point in Fig. 2 is set at 154. However, the maximum number of pixels in the digital image is not large enough to hide embedded message. Take "Lena" in Fig. 2, for example. Because its $h(154) = 2787$, which means the largest hiding capacity of "Lena" is 2787 bits, by shifting all the pixels whose grayscale value is "154" in "Lena" to hide the embedded message. In other words, because the peak point of an image's histogram cannot provide large hiding capacity; the concept must be extended before it can be used to hide a large embedded message.

When we observed the characteristic of an image carefully, we discovered that in terms of an image, there is a large probability that adjacent pixels in an image have similar pixel values. From this observation, we concluded that the difference between two adjacent pixels in an image can be a value in its difference image, as shown in Fig. 3(a). As expected, in a difference image the grayscale value with the maximum number of pixel values tends to be around 0, as shown in Fig. 3(b). Hence, we use the characteristics of the difference histogram derived from a difference image that has been generated from an original image to generate a higher peak point value in

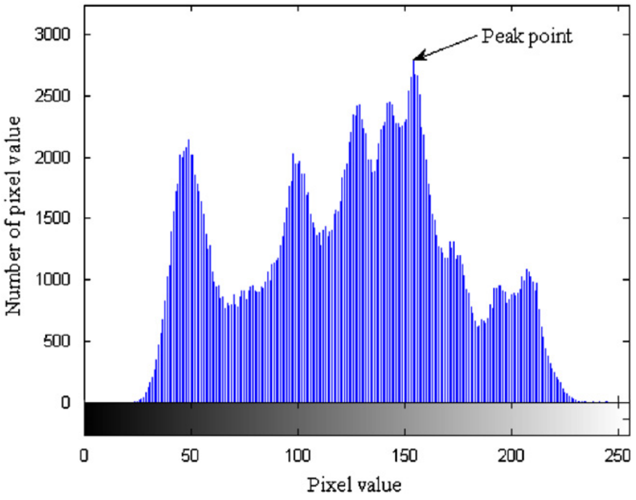

Fig. 2. Histogram of "Lena" image with a peak point of 154.

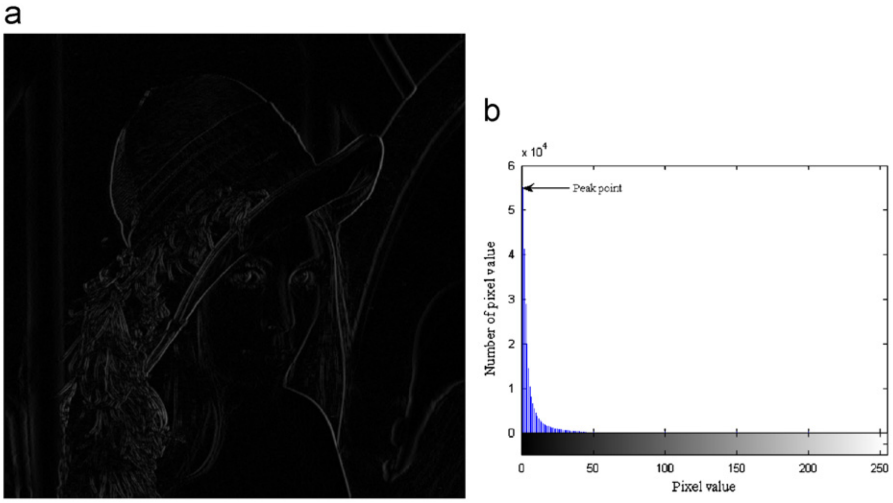

Fig. 3. Image characteristics of “Lena”: (a) difference image of “Lena” and (b) histogram of (a).

our proposed scheme. The objective in finding a peak point from a difference image is to increase hiding capacity to the greatest degree possible.

A detailed description for creating the histogram phase appears later in this paper. The general model of our proposed scheme is described in Section 2.1. Section 2.2 evaluates the computational complexity of data hiding process. Section 2.3 presents a solution to the overflow and underflow problem caused during the hiding phase. The lower bound of the distortion caused by our proposed hiding is estimated in Section 2.4. In essence, the proposed multilevel hiding strategy can be easily integrated into our hiding phase, which is presented in Section 2.1.

2.1. General model of our proposed scheme

Fig. 4 is a flowchart of our proposed reversible data hiding scheme. For the sender part, the embedded message M is a binary sequence. Then, the proposed transformation T, which is based on the properties of a histogram in a difference image, is used to create the free space for hiding the embedded message M. During the hiding phase, the embedded message M is hidden in the difference image by using the proposed histogram modification process. Later, the marked image is obtained through the inverse transformation T^{-1}. For the receiver part, the receiver can use the same transformation T to extract the embedded message and reverse the marked image to its original. Our proposed scheme can be divided into three phases: creating the histogram phase, the hiding phase, and the extracting and reversing phase. The three phases in our proposed scheme are described in detail in the following paragraphs.

2.1.1. Creating the histogram phase

To create a large free space for data hiding, a difference image of an image must be generated before the hiding phase. For a grayscale image $H(i, j)$ $P{\times}Q$ pixels in size, a difference image $D(i, j)$, $P{\times}(Q{-}1)$ pixels in size can be generated from the original image H by using following formula:

$$D(i,j) = |H(i,j) - H(i,j+1)|, \quad 0 \leqslant i \leqslant P-1, \quad 0 \leqslant j \leqslant Q-2, \tag{1}$$

Here $|\cdot|$ is the absolute value operation. Fig. 3 clearly shows the property of a difference image. Unlike the original image in Fig. 2, the maximum pixel values in a difference image tend to be around pixel value 0. In Fig. 3(b), the peak point is “1” and its corresponding number of pixels in the histogram of the difference image is more than 55,000. Hence, the peak point in the histogram of a difference image is used to create the free space for hiding embedded messages. Therefore, by using the property of the difference image histogram, we can hide a larger number of messages in comparison with the original image.

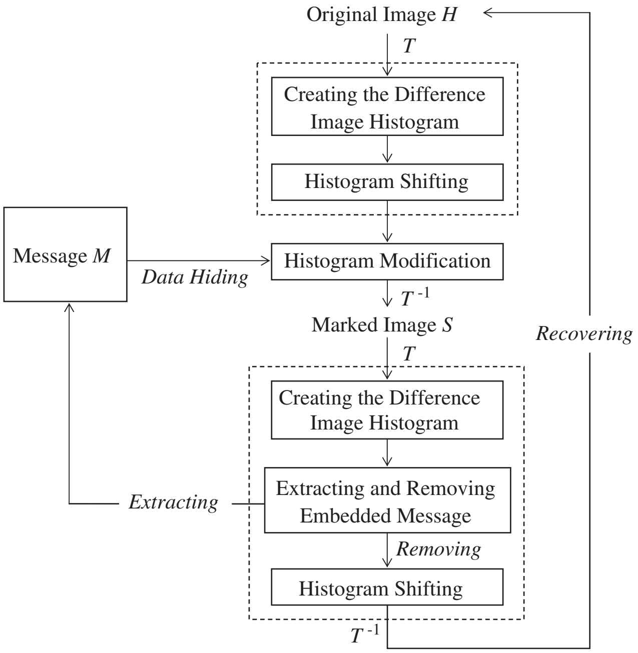

Fig. 4. Flowchart of proposed reversible data hiding.

2.1.2. Hiding phase

The proposed hiding phase can be divided into five steps as follows.

Step 1: Divide the original cover image into blocks $A{\times}B$ in size. Generate a difference image $D_b(I,j)$ of size $A{\times}(B{-}1)$ for each block by using following formula:

$$D_b(i,j) = |H_b(i,j) - H_b(i,j+1)|, \quad 0 \leqslant i \leqslant A-1, \quad 0 \leqslant j \leqslant B-2, \quad 0 \leqslant b \leqslant \frac{M \times N}{A \times B} - 1. \tag{2}$$

a H_b

162	156	163	160
161	159	158	159
160	161	159	155
158	158	156	157

b D_b

6	7	3
2	1	1
1	2	4
0	2	1

c D_b'

7	8	4
3	1	1
1	3	5
0	3	1

d D_b''

7	8	4
3	1	2
2	3	5
0	3	1

e S_b

163	156	164	160
162	159	158	160
160	162	159	154
158	158	155	156

Fig. 5. Example of the hiding phase: (a) 4×4 block of the original image "Lena"; (b) difference image D_b; (c) modified difference image D_b', (d) hidden difference image D_b''; and (e) marked image S_b.

Step 2: Generate the histogram of the difference image D_b and record the peak point P_b for each block.

Step 3: If the pixel value $D_b(i,j)$ of block b is larger than the peak point P_b of block b, change the pixel value $D_b(i,j)$ of block b to $D_b(i,j)+1$. Otherwise, the pixel value $D_b(i,j)$ remains unchanged. The modification principle is defined as

$$D_b'(i,j)=\begin{cases} D_b(i,j)+1 & \text{if } D_b(i,j)>P_b,\\ D_b(i,j) & \text{otherwise,}\end{cases}$$

$$\text{for } 0\leqslant i\leqslant A-1,\quad 0\leqslant j\leqslant B-2,\ \text{ and }\ 0\leqslant b\leqslant \frac{M\times N}{A\times B}-1, \tag{3}$$

where P_b is the peak point of block b.

Step 4: For the modified difference image D_b', the pixels having grayscale values the same as peak point P_b can be modified as follows to hide embedded message bit m:

$$D_b''(i,j)=\begin{cases} D_b'(i,j)+m & \text{if } D_b'(i,j)=P_b,\\ D_b'(i,j) & \text{otherwise,}\end{cases}$$

$$\text{for } 0\leqslant i\leqslant A-1,\quad 0\leqslant j\leqslant B-2,\quad \text{and}\quad 0\leqslant b\leqslant \frac{M\times N}{A\times B}-1, \tag{4}$$

where P_b is the peak point of block b, and $m\in\{0,1\}$.

Step 5: Use the original image and its hidden difference image to construct the marked image by performing the following inverse transformation T^{-1}. For the first two pixels in each row, the inverse operation is expressed as

$$S_b(i,0)=\begin{cases} H_b(i,0) & \text{if } H_b(i,0)>H_b(i,1),\\ H_b(i,1)+D_b''(i,0) & \text{otherwise,}\end{cases}$$

$$S_b(i,1)=\begin{cases} H_b(i,0)+D_b''(i,0) & \text{if } H_b(i,0)\leqslant H_b(i,1),\\ H_b(i,1) & \text{otherwise,}\end{cases}$$

$$\text{for } 0\leqslant i\leqslant A-1,\quad 0\leqslant b\leqslant \frac{M\times N}{A\times B}-1. \tag{5}$$

a S_b

163	156	164	160
162	159	158	160
160	162	159	154
158	158	155	156

b SD_b

7	8	4
3	1	2
2	3	5
0	3	1

c RD_b

6	7	3
2	1	1
1	2	4
0	2	1

d RH_b

162	156	163	160
161	159	158	159
160	161	159	155
158	158	156	157

Fig. 6. Example of extracting and reversing phase: (a) 4×4 block of the received marked image; (b) extracting embedded message in difference image SD_b; (c) reconstructed difference image ED_b; and (d) recovered original image.

For any residual pixels, the inverse operation is defined as

$$S_b(i,j)=\begin{cases} S_b(i,j-1)+D_b''(i,j-1) & \text{if } H_b(i,j-1)\leqslant H_b(i,j),\\ S_b(i,j-1)-D_b''(i,j-1) & \text{otherwise,}\end{cases}$$

$$\text{for } 0\leqslant i\leqslant A-1,\quad 2\leqslant j\leqslant B-2,\quad 0\leqslant b\leqslant \frac{M\times N}{A\times B}-1. \tag{6}$$

To enhance the security of the embedded message or to allow only the authorized party to remove the embedded message, most lossless data embedding techniques [5–7] transmit a secret key to the receiver side. The secret key serves as the seed of a pseudo random

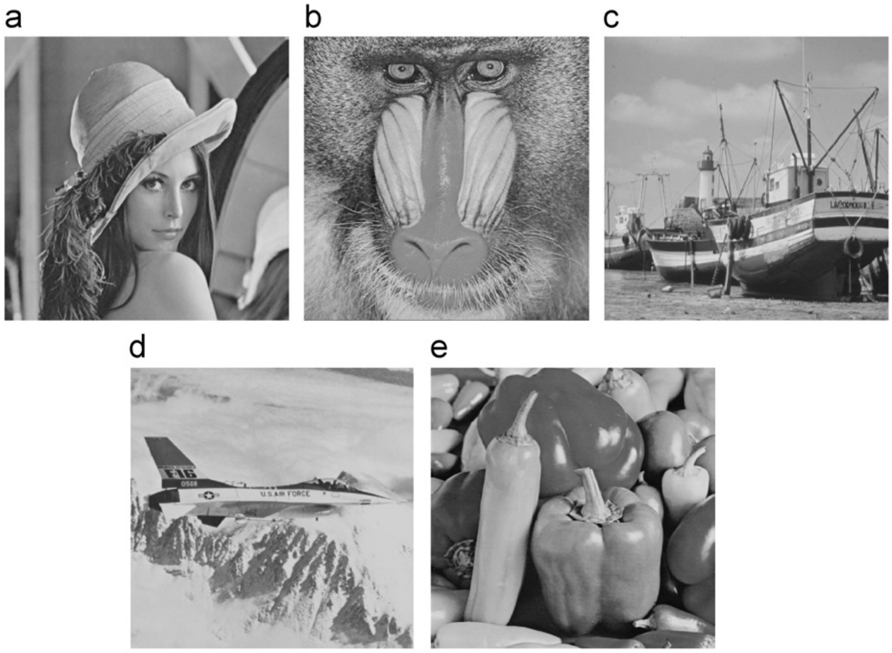

Fig. 7. Original five test images used for performance evaluation: (a) Lena; (b) Baboon; (c) boat; (d) jet; and (e) pepper.

number generator (PRNG) to generate a random non-intersecting walk and, for increased security, message bits are hidden according to the random walk. Although the proposed scheme hides embedded message bits sequentially rather than randomly, the peak point P_b still behaves in the same manner as the secret key. Hence, our scheme takes the same strategy as Ni et al.'s scheme [17], in which all peak points are concatenated as a secret key and are transmitted to the receiver side for extraction of the embedded message and restoration of the original image.

Fig. 5 shows an example of our hiding phase. In Fig. 5(a), we assume that the divided block size is 4×4 and the embedded message bits are "0110". By using Eq. (2), we can generate a difference image, as shown in Fig. 5(b), in which the maximum pixel number of pixel value "1" is 4; hence, the peak point P_b is set as 1. According to our modification principle in Eq. (3), only the pixel values of $D_b(1,1)$, $D_b(1,2)$, $D_b(2,0)$, $D_b(3,0)$ and $D_b(3,2)$ remain unchanged and the rest of the pixel values are added by 1, as shown in Fig. 5(c). In Fig. 5(b), the peak point P_b is "1" and its corresponding number of pixels is "4". That is, four message bits can be hidden in this block. Because the embedded message bits are "0110", the pixel values of $D'_b(1,1)$, $D'_b(1,2)$, $D'_b(2,0)$, and $D'_b(3,2)$ are changed to "1", "2", "2", and "1", respectively, to comply with our proposed hiding rules in Eq. (4). By using Eq. (5), we can easily combine the hidden difference image D''_b and the original image to generate the marked image S_b shown in Fig. 5(e). For example, the pixel values for $H(0,0)$ and $H(0,1)$ are 162 and 156, respectively. Because 162 is larger than 156, $S(0,0)$ is set as 173(=156+7), which is the sum of $H(0,1)$ and $D''_b(0,0)$, according to the first rule in Eq. (5). According to the second rule in Eq. (5), $S(0,1)$ is set the same as $H(0,1)$.

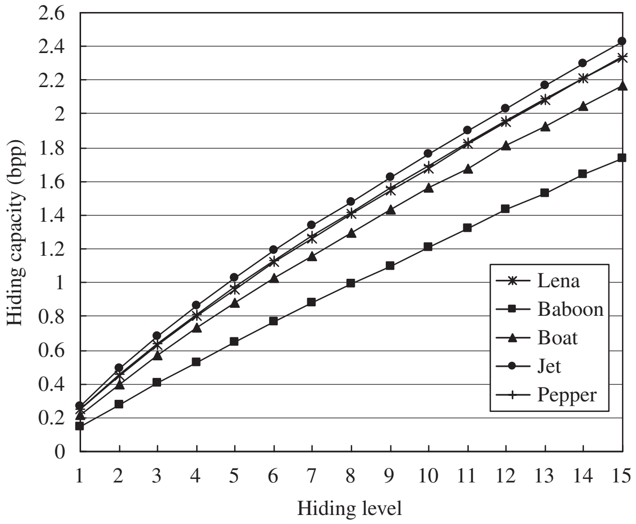

Fig. 8. Hiding capacity (bpp) versus hiding level for five test images.

2.1.3. *Extracting and reversing phase*

In this process, we extract the embedded message and reverse the marked image to its original. The basic steps for the extracting and reversing process are as follows.

Step 1: Divide the received marked image into blocks $A\times B$ in size. Generate the difference image $SD_b(i,j)$ of block b from the received marked image by using the following formula:

$$SD_b(i,j)=|S_b(i,j)-S_b(i,j+1)|,$$

$$\text{for } 0\leqslant i\leqslant A-1,\quad 0\leqslant j\leqslant B-2,\quad 0\leqslant b\leqslant \frac{M\times N}{A\times B}-1. \tag{7}$$

Step 2: Perform the embedded message extracting on the difference image $SD_b(i,j)$ of block b by using the following rule:

$$m=\begin{cases}0 & \text{if } SD_b(i,j)=P_b,\\ 1 & \text{if } SD_b(i,j)=P_b+1,\end{cases}$$

$$\text{for } 0\leqslant i\leqslant A-1,\quad 0\leqslant j\leqslant B-2,\ \text{ and }\ 0\leqslant b\leqslant \frac{M\times N}{A\times B}-1, \tag{8}$$

where P_b is the received peak point of block b. We first scan the entire difference image of block b. For block b, if the pixel with

Table 1
Hiding capacities (bits) versus hiding level and average *PSNR* for five test images

Level	1	2	3	4	5	6	9	12	15	18
PSNR	48.67	43.02	39.64	37.21	35.28	33.70	30.19	27.58	25.39	23.53
Lena	65349	115963	158815	196653	230762	262215	346568	416882	475466	527788
Baboon	38465	70730	99234	125048	148709	170739	230079	283333	333853	383369
Boat	56713	101896	140580	175008	206317	235523	314196	379624	435510	486827
Jet	69941	123660	168769	208295	243796	276369	362847	436168	497052	550497
Pepper	64632	110929	153512	191083	225148	256916	342175	412341	470342	522531

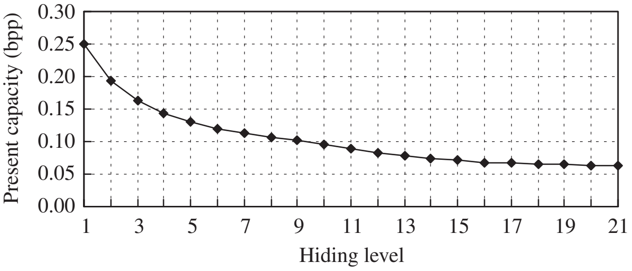

Fig. 9. Hiding capacity of "Lena" image at various hiding levels.

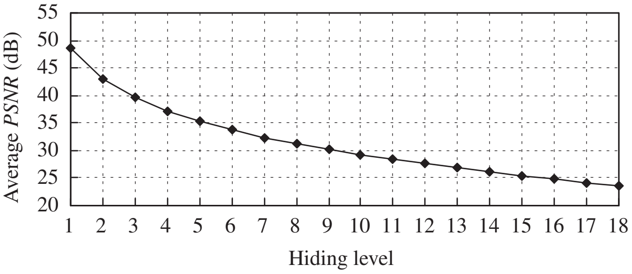

Fig. 10. Average *PSNR* for the five test images at various hiding levels.

P_b is encountered, bit 0 is retrieved. If the pixel with (P_b+1) is encountered, bit 1 is retrieved.

Step 3: Remove the embedded message from the difference image $SD_b(i,j)$ for block b by using the following formula:

$$SD'_b(i,j)=\begin{cases}SD_b(i,j)-1 & \text{if } SD_b(i,j)=P_b+1,\\ SD_b(i,j) & \text{otherwise,}\end{cases}$$

$$\text{for } 0\leqslant i\leqslant A-1,\quad 0\leqslant j\leqslant B-2,\ \text{and } 0\leqslant b\leqslant \frac{M\times N}{A\times B}-1. \qquad (9)$$

Step 4: Shift some pixel values in the difference image $SD'_b(i,j)$ to obtain its reconstructed original difference image $RD_b(i,j)$ according to

$$RD_b(i,j)=\begin{cases}SD'_b(i,j)-1 & \text{if } SD_b(i,j)>P_b+1,\\ SD'_b(i,j) & \text{otherwise,}\end{cases}$$

$$\text{for } 0\leqslant i\leqslant A-1,\quad 0\leqslant j\leqslant B-2,\ \text{and } 0\leqslant b\leqslant \frac{M\times N}{A\times B}-1. \qquad (10)$$

Step 5: Finally, obtain the recovered original image $RH_b(i,j)$ by performing the inverse transformation T^{-1}. Similar to Step 5 in the hiding phase, for the first two pixels of each row the inverse operation is expressed as

$$RH_b(i,0)=\begin{cases}S_b(i,0) & \text{if } S_b(i,0)\leqslant S_b(i,1),\\ S_b(i,1)+RD_b(i,0) & \text{otherwise,}\end{cases}$$

$$RH_b(i,1)=\begin{cases}S_b(i,0)+RD_b(i,0) & \text{if } S_b(i,0)\leqslant S_b(i,1),\\ S_b(i,1) & \text{otherwise,}\end{cases}$$

$$\text{for } 0\leqslant i\leqslant A-1,\quad 0\leqslant b\leqslant \frac{M\times N}{A\times B}-1. \qquad (11)$$

For the remaining pixels, the corresponding inverse operation is shown as

$$RH_b(i,j)=\begin{cases}RH_b(i,j-1)+RD_b(i,j-1) & \text{if } S_b(i,j-1)\\ & \quad\leqslant S_b(i,j),\\ RH_b(i,j-1)-RD_b(i,j-1) & \text{otherwise,}\end{cases}$$

$$\text{for } 0\leqslant i\leqslant A-1,\quad 2\leqslant j\leqslant B-2,\quad 0\leqslant b\leqslant \frac{M\times N}{A\times B}-1. \qquad (12)$$

The marked image in Fig. 5(e) is used to demonstrate our extracting and reversing process. In essence, we can use the received peak point P_b to extract the embedded message bits "0110", as shown in Fig. 6(b). Then, as Fig. 6(c) shows, we generate the reconstructed difference image by removing the embedded message bits. After the lossless inverse transformation, the recovered original image is obtained as shown in Fig. 6(d).

2.2. Computational complexity

All the processing of our proposed scheme is in the spatial domain. The computational complexity of the proposed scheme is low since it does not need to do any frequency domain transforms such as DCT, DWT, and so on. The operation requires generating the difference image histogram for a cover image, determining peak point based on the histogram, hiding messages, and doing the inverse transformation in the spatial domain. Thus, the execution time of the proposed scheme is quite short. Assume that the block size is $A\times B$, and there are k blocks in a cover image. For each block, our proposed scheme only needs to scan the whole block five times in the hiding phase. Hence, the computational complexity is $O(5AB)$. As a result, the total computational complexity is $O(5ABk)$ because the whole image case is just a multiple repetition of single block case. With a computer Intel Core Duo 1.86 GHz CPU and software Borland C + + Builder 6, the total embedding time needed for the "Lena" image (512 × 512 × 8) is just 80 ms.

2.3. Preventing possible "over/underflow"

Note that it is possible for a marked image generated by using the proposed scheme to have some pixels with overflowed or underflowed grayscale values, meaning that the grayscale values of some pixels in the marked image may exceed the upper bound (255 for an eight-bit grayscale image) or the lower bound (0 for an eight-bit grayscale image). This is possibly caused by the addition or subtraction operations perform on pixel values that are close to 255 or 0. To

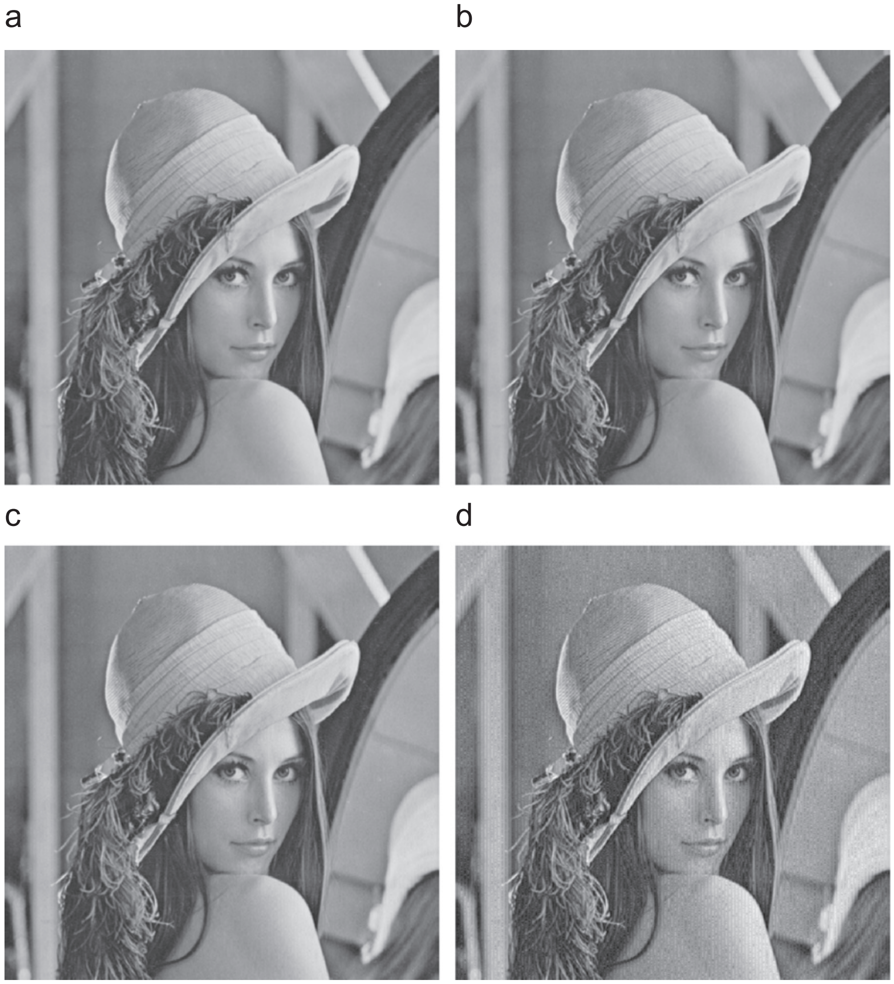

Fig. 11. Original and marked grayscale Lena images: (a) original image "Lena"; (b) 50.64 dB with 0.25 bpp; (c) 35.21 dB with 1.12 bpp; and (d) 28.06 dB with 2.08 bpp.

overcome this over/underflow problem, the modulo operation proposed by Goljan et al. [5] and Honsinger et al. [22] was adopted to avoid truncation as overflow or underflow occurs in the proposed scheme. For the marked image, we define each pixel $S_b(i,j)$ as

$$S_b(i,j) = S_b(i,j) \bmod 256. \tag{13}$$

In the receiver side, whether the received pixel, for example, $S_b(i,j)$=255, was derived from 255 or −1 must be distinguished. Considering the characteristics of an image, no tremendous variations exist for adjacent pixels. Therefore, in case of a significant difference between $S_b(i,j–1)$ and $S_b(i,j)$, $S_b(i,j)$ was conducted by a modulo operation. Two evaluations are presented here to restore the original value of $S_b(i,j)$ after the modulo operation is performed. If $S_b(i,j–1)$ is larger than TH_1, $S_b(i,j)$ is restored as

$$S_b(i,j) = \begin{cases} S_b(i,j) + 256 & \text{if } S_b|(i,j-1) - S_b(i,j)| \\ & \quad \geqslant TH_2, \\ S_b(i,j) & \text{otherwise,} \end{cases} \tag{14}$$

where TH_1 and TH_2 are threshold values. If $S_b(i,j–1)$ is smaller than TH_1, $S_b(i,j)$ is restored as

$$S_b(i,j) = \begin{cases} S_b(i,j) - 256 & \text{if } |S_b(i,j-1) - S_b(i,j)| \\ & \quad \geqslant TH_2, \\ S_b(i,j) & \text{otherwise.} \end{cases} \tag{15}$$

2.4. Lower bound of PSNR

The *PSNR* of an image is a general measure for evaluating image quality. In this section, we also adopt *PSNR* to measure the image quality of a marked image generated by our proposed scheme and investigate the lower bound of the image quality of the marked image.

Assume that data hiding is at the first level and the block size is set to 4×4. In the worst case, all embedded message bits are 1; thus, all pixel values of the difference image must be added by 1. For each row of each block from left to right, the distortion, which is the pixel difference between the marked image and the original image, forms an arithmetic sequence "0", "1", "2", and "3", respectively. Therefore, the distortion in each block can be depicted as $4 \times \sum_{k=0}^{3} k$, where k is the pixel difference between the marked image and the original image. In this case, the mean squared error (MSE) is $(4 \times \sum_{k=0}^{3} k^2)/16 = 3.5$. Therefore, the lower bound of *PSNR* for the marked image can be calculated as

$$PSNR\,(\mathrm{dB}) = 10 \log_{10}\left(\frac{255^2}{MSE}\right) \approx 42.69. \tag{16}$$

In short, the lower bound of *PSNR* theoretically proved here is about 42.69 dB in our first-level hiding, which is also supported by our numerous experiments.

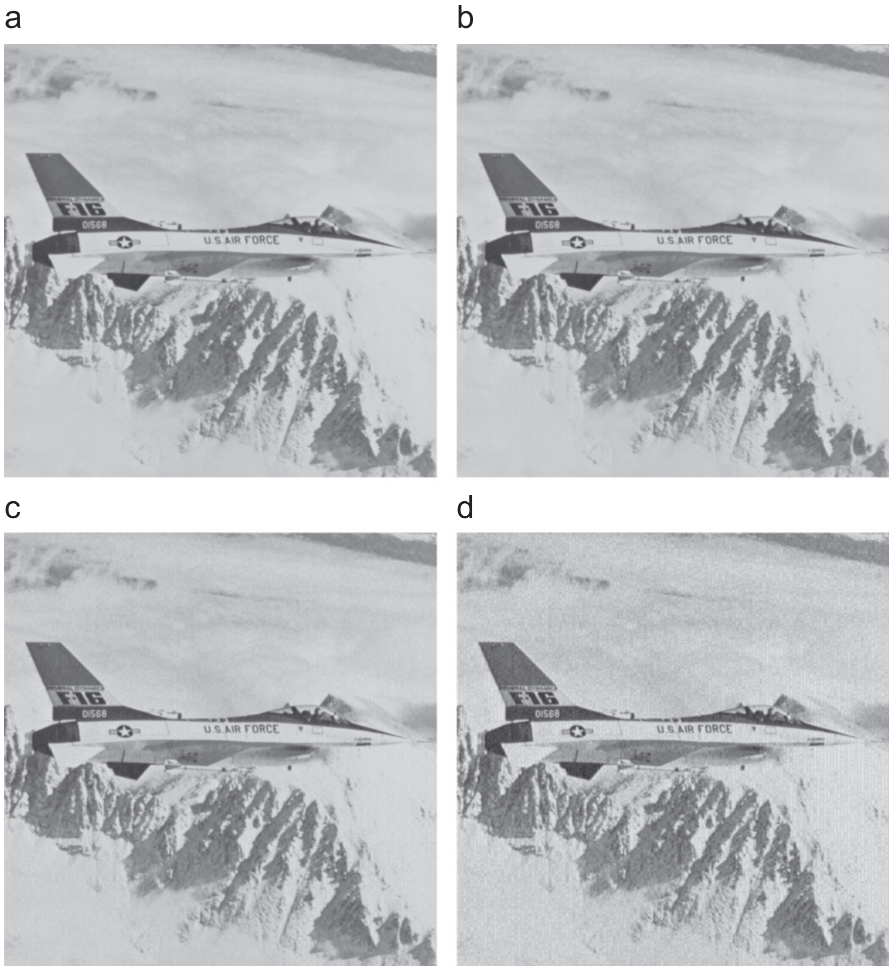

Fig. 12. Original and marked grayscale jet images: (a) original image "jet"; (b) 51.14 dB with 0.27 bpp; (c) 37.35 dB with 1.03 bpp; and (d) 29.28 dB with 2.03 bpp.

3. Experimental results

Section 2 offers proof of the reversibility of our proposed scheme. In this section, we conducted several experiments to demonstrate our performance in hiding capacity and image quality of a marked image. For these experiments, the five grayscale images in Fig. 7, "Lena", "Pepper", "Baboon", "Boat", and "Jet", all 512 × 512 in size, served as test images. In essence, the hiding capacity of our proposed scheme is equal to the sum of the number of pixels associated with the peak points of the blocks in the difference image. Based on the distinctive nature of an image, the grayscale values close to 0 in its difference image may be the maximum number of pixels. Moreover, the number of pixels that correspond to the peak point in a difference image is always larger than the number in its original image. Based on this property of the difference image histogram, we can hide a large amount of embedded messages in a marked image in comparison with its original image.

Because our hiding algorithm is based on a multilevel concept, the algorithm can be performed repeatedly to convey a large amount of embedded messages. At the beginning of this section, we demonstrate the performance of our proposed multilevel hiding algorithm in hiding capacity and image quality at various hiding levels. Fig. 8 shows hiding capacities (in bits per pixel) versus various hiding levels for test images. A subset of these results is tabulated in Table 1, which includes the average *PSNR* induced by hiding at each level. From Fig. 8 and Table 1, we can see that the hiding capacity of the proposed scheme depends strongly on the characteristics of the original cover image. Images with large smooth regions such as "Jet" provide higher hiding capacities than those with irregular textures such as "Baboon". The principal reason for this larger capacity is that most adjacent pixels have similar pixel values in a smooth region; therefore, they can contribute a higher number of pixels associated with the peak point compared with those in a complex region. In other words, once an image has many smooth regions, the number of pixels that correspond to the peak point in its image is larger than that of an image with fewer smooth regions; thus, the hiding capacity of the former will be larger than that of the latter.

In both Fig. 8 and Table 1, "hiding level" represents the number of rounds our proposed hiding algorithm undergoes. For example, "level-18 hiding" means our proposed hiding algorithm was performed for 18 rounds. As can be seen in Fig. 8, our proposed multilevel reversible data hiding scheme can hide more than 2 bits per pixel without respect to allowable distortion after performing 18 rounds of the proposed multilevel hiding algorithm. Furthermore, Table 1 shows that the hiding capacity of "Jet" can easily allow up to 550,000 bits after performing 18 rounds. Even when image quality is also considered, the hiding capacity of "Jet" still can rise to about 350,000 bits after nine rounds of hiding while maintaining the image quality of its marked image at 30.2 dB.

Fig. 9 plots the hiding capacity provided by each hiding level from round 1 to round 18 for the "Lena" test image. As can be seen in Fig. 9, at level 1 our proposed hiding algorithm can hide 0.25 bpp.

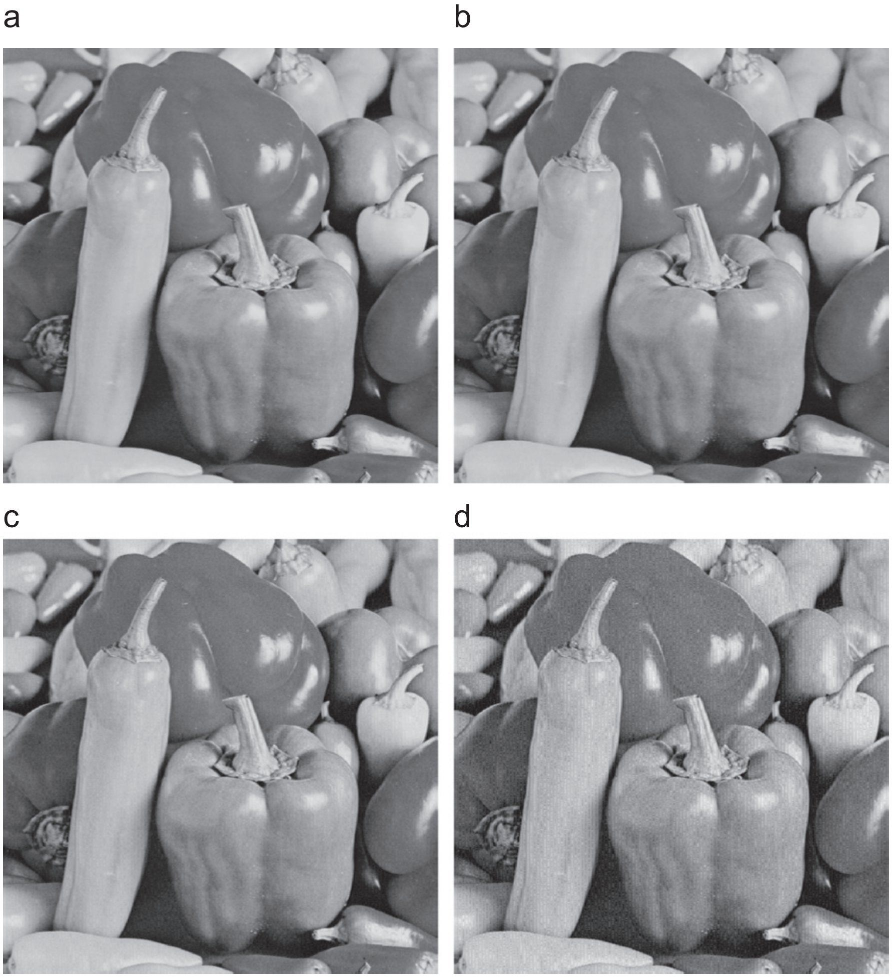

Fig. 13. Original and marked grayscale pepper images: (a) original image "pepper"; (b) 50.71 dB with 0.25 bpp; (c) 36.97 dB with 0.98 bpp; and (d) 29.28 dB with 2.03 bpp.

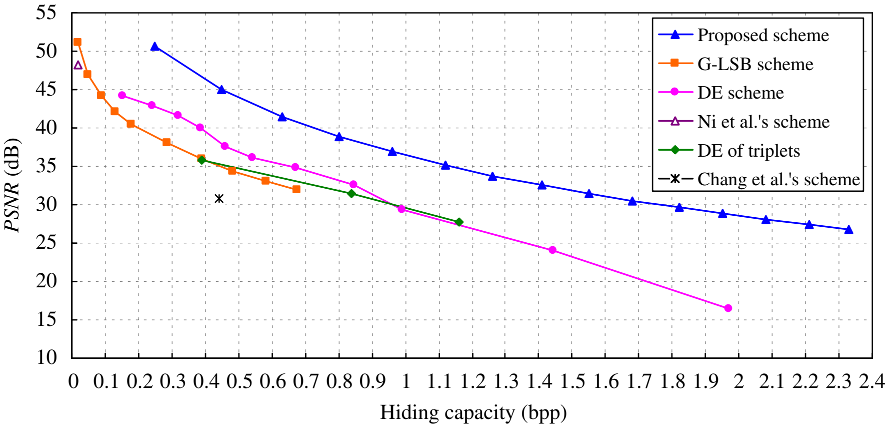

Fig. 14. Comparison of hiding capacity in bpp versus image quality in *PSNR* with existing reversible schemes: G-LSB scheme [16], DE [12], Ni et al.'s scheme [17], DE of triplets [13], and Chang et al.'s scheme [19]. The test image is grayscale "Lena" image.

However, hiding capacity decreases roughly linearly with the number of hiding levels performed. When our proposed hiding algorithm is performed for 21 rounds, it hides more than 0.05 bpp because the hiding capacity depends strongly on the number of pixels associated with the peak point in the difference image. Hence, the hiding capacity limitation at each level decreases gradually as the number of pixels at the peak point becomes fewer and fewer after repeated multilevel data hiding rounds.

Fig. 10 illustrates the average *PSNR* for the five test images at various hiding levels. For level 1, the average *PSNR* value is higher than 48 dB, which satisfies the lower bound of the *PSNR* given in Eq. (16). Even when the original image has undergone five rounds of hiding an embedded message, the average *PSNR* value is still higher than 35 dB. In Fig. 10, we can see that the *PSNR* decreases with the increase in number of hiding levels. The major reason is that hiding a large volume of embedded messages leads to greater distortion in the marked images. That is, a higher payload size yields lower *PSNR* values. This phenomenon presents a tradeoff between imperceptibility and hiding capacity.

Figs. 11, 12 and 13 show the original image and the visual impacts of marked images at different hiding capacities for grayscale images, “Lean”, “Jet”, and “Pepper”, respectively. Even when the hiding capacity exceeds 1 bpp, the visual distortion is still quite small and the *PSNR* is still higher than 35 dB, as shown in Figs. 11(c), 12(c), and 13(c). Unfortunately, the way that solves the over/underflow problem highlights few pixels in marked images when the hiding capacity is around 2 bpp, as shown in Figs. 11(d), 12(d), and 13(d). However, this phenomenon is not perceptually obvious, even when the corresponding *PSNR*s are less than 30 dB. As shown in the figures, the visual quality of the marked image is quite good at moderate hiding capacity, and it is still acceptable especially for smooth image “Jet” even at very high hiding capacity around 2 bpp.

Fig. 14 shows the comparison of hiding capacity in bpp versus image quality in *PSNR* of the proposed scheme with that of five existing reversible schemes: G-LSB scheme [16], DE [12], Ni et al.'s scheme [17], DE of triplets [13], and Chang et al.'s scheme [19] for the grayscale “Lena” image. As shown in the figure, the Ni et al.'s scheme [17] has low hiding capacity compared to the others. In Ni et al.'s scheme [17] and Chang et al.'s scheme [19], the achievable hiding capacity and image quality is fixed for a given test image. In the other schemes, the balance between hiding capacity and image quality is achievable. The top curve in Fig. 14 is the proposed scheme, and shows that its *PSNR* is about 4–5 dB higher than the other schemes with the same volume of embedded messages. That is, the proposed scheme achieves relatively higher hiding capacity with low distortion than the other schemes.

4. Conclusions

By combining the peak point of a difference image concept with a multilevel hiding strategy, our proposed hiding scheme not only hides a large amount of embedded messages but also achieves reversibility. Certainly, it is hard to maintain a balance between hiding capacity and image distortion in marked images. Through a joint imperceptibility and hiding capacity measure, our experimental results confirm that our proposed multilevel reversible data hiding scheme can provide higher hiding capacity while keeping distortion low. Even when our proposed hiding algorithm is performed for nine rounds, the average *PSNR* is still higher than 30 dB and the average hiding capacity still can reach 1.3 bpp. Performance comparisons with existing reversible schemes further demonstrate the effectiveness of the proposed scheme. In the future, we will explore the possibility of providing higher hiding capacity with lower distortion and extend our scheme to transform domains such as DCT and the wavelet domain to improve the transmission quantity of images.

References

[1] M. Wu, B. Lin, Data hiding in image and video: part I—fundamental issues and solutions, IEEE Trans. Image Process. 12 (6) (2003) 685–695.

[2] M. Wu, H. Yu, B. Liu, Data hiding in image and video: part II—designs and applications, IEEE Trans. Image Process. 12 (6) (2003) 696–705.

[3] S.S. Maniccam, N.G. Bourbakis, Lossless compression and information hiding in images, Pattern Recognition 37 (3) (2004) 475–486.

[4] C.-C. Chang, C.-C. Lin, C.-S. Tseng, W.-L. Tai, Reversible hiding in DCT-based compressed images, Inf. Sci. 177 (13) (2007) 2768–2786.

[5] M. Goljan, J. Fridrich, R. Du, Distortion-free data embedding, in: Proceedings of the Four Information Hiding Workshop, Lecture Notes in Computer Science, vol. 2137, Springer, New York, April 25–27, 2001, pp. 27–41.

[6] J. Fridrich, M. Goljan, R. Du, Invertible authentication watermark for JPEG images, in: Proceedings of International Conference on Information Technology: Coding and Computing, Las Vegas, Nevada, April 2001, pp. 223–227.

[7] J. Fridrich, M. Goljan, R. Du, Lossless data embedding for all image formats, in: Proceedings of SPIE Photonic West, Electronic Imaging 2002, Security and Watermarking of Multimedia Contents, vol. 4675, San Jose, California, January 2002, pp. 572–583.

[8] M.U. Celik, G. Sharma, A.M. Tekalp, Lossless watermarking for image authentication: a new framework and an implementation, IEEE Trans. Image Process. 15 (4) (2006) 1042–1049.

[9] J. Fridrich, M. Goljan, R. Du, Invertible authentication, in: Proceedings of the SPIE, Security and Watermarking of Multimedia Contents, San Jose, California, January 2001, pp. 197–208.

[10] J. Fridrich, M. Goljan, R. Du, Lossless data embedding—new paradigm in digital watermarking, EURASIP J. Appl. Signal Process. 2002 (2) (2002) 185–196.

[11] C. De Vleeschouwer, J.F. Delaigle, B. Macq, Circular interpretation of bijective transformations in lossless watermarking for media asset management, IEEE Trans. Multimedia 5 (1) (2003) 97–105.

[12] J. Tian, Reversible data embedding using a difference expansion, IEEE Trans. Circuits Systems Video Technol. 13 (8) (2003) 890–896.

[13] A.M. Alattar, Reversible watermark using the difference expansion of a generalized integer transform, IEEE Trans. Image Process. 13 (8) (2004) 1147–1156.

[14] L. Kamstra, H.J.A.M. Heijmans, Reversible data embedding into images using wavelet techniques and sorting, IEEE Trans. Image Process. 14 (12) (2005) 2082–2090.

[15] D.M. Thodi, J.J. Rodríguez, Expansion embedding techniques for reversible watermarking, IEEE Trans. Image Process. 16 (3) (2007) 721–730.

[16] M.U. Celik, G. Sharma, A.M. Tekalp, E. Saber, Lossless generalized-LSB data embedding, IEEE Trans. Image Process. 14 (2) (2005) 253–266.

[17] Z. Ni, Y.-Q. Shi, N. Ansari, W. Su, Reversible data hiding, IEEE Trans. Circuits Systems Video Technol. 16 (3) (2006) 354–362.

[18] C.-C. Chang, W.-L. Tai, M.-H. Lin, A reversible data hiding scheme with modified side match vector quantization, in: Proceedings of the IEEE 19th International Conference on Advanced Information Networking and Applications, vol. 1, Taipei, Taiwan, March 2005, pp. 947-+-952.

[19] C.-C. Chang, W.-L. Tai, C.-C. Lin, A reversible data hiding scheme based on side match vector quantization, IEEE Trans. Circuits Systems Video Technol. 16 (10) (2006) 1301–1308.

[20] Y. Hu, B. Jeon, Reversible visible watermarking and lossless recovery of original images, IEEE Trans. Circuits Systems Video Technol. 16 (11) (2006) 1423–1429.

[21] S. Lee, C.D. Yoo, T. Kalker, Reversible image watermarking based on integer-to-integer wavelet transform, IEEE Trans. Inf. Forensics Secur. 2 (3) (2007) 321–330.

[22] C. Honsinger, P. Jone, M. Rabbani, J. Stoffel, Lossless recovery of an original image containing embedded data, United States Patent #6278791, August 2001.

About the Author—CHIA-CHEN LIN received her B.S. degree in Information Management in 1992 from the Tamkang University, Taipei, Taiwan. She received both her M.S. degree in Information Management in 1994 and Ph.D. degree in Information Management in 1998 from the National Chiao Tung University, Hsinchu, Taiwan. Dr. Lin is currently an Associate Professor of the Department of Computer Science and Information Management, Providence University, Sha-Lu, Taiwan. Her research interests include image and signal processing, image hiding, mobile agent, and electronic commerce.

About the Author—WEI-LIANG TAI received the B.S. degree in Computer Science from Tamkang University in Tamsui, Taiwan, in 2002 and the M.S. degree in Computer Science and Information Engineering from National Chung Cheng University in Chiayi, Taiwan, in 2004. He is currently pursuing the Ph.D. degree under the supervision of Dr. Chin-Chen Chang. His research focuses on steganography, digital watermarking, reversible data hiding, and image authentication.

About the Author—CHIN-CHEN CHANG received his B.S. degree in Applied Mathematics in 1977 and his M.S. degree in Computer and Decision Sciences in 1979 from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D. in Computer Engineering in 1982 from National Chiao Tung University, Hsinchu, Taiwan. From 1983 to 1989, he was the faculty at the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. Since August 1989, he was a Professor of the Institute of Computer Science and Information Engineering at National Chung Cheng University, Chiayi, Taiwan. Dr. Chang is a Fellow of IEEE and a Fellow of IEE. He is also a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, and the Phi Tau Phi Society of the Republic of China. His research interests include database design, computer cryptography, and data compression.