Int. J. Electron. Commun. (AEÜ) 69 (2015) 1745–1754

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

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

Reversible and adaptive image steganographic method

Mingwei Tang [a,*], Jie Hu [b], Wen Song [a], Shengke Zeng [a]

[a] School of Computer and Software Engineering, Xihua University, Chengdu 610039, China
[b] School of Information Science and Technology, Southwest Jiaotong University, Chengdu 611756, China

ARTICLE INFO

Article history:
Received 10 October 2013
Accepted 26 August 2015

Keywords:
Information hiding
Image interpolation
Reversibility
Peak signal-to-noise ratio
Adjacent pixels

ABSTRACT

Reversible image steganographic scheme has become one of main research contents in information hiding field in recent years. Reversibility allows the original images to be completely reconstructed without any distortion after the embedded information has been extracted. Image interpolation is a key image processing method and has been widely applied in imaging processing relevant areas, such as image reconstruction by simulating image adjacent pixels between two-dimensional images. This paper proposed a reversible and adaptive image steganographic algorithm based on a novel interpolation technology, which can improve the performance of information hiding schemes proposed before. The proposed scheme has the benefits of higher embedding capacity with lower computational complexity and better image quality. The experimental results show that the proposed scheme can gain better performance than other state-of-the-art algorithms.

1. Introduction

Information hiding (or data hiding) is the art of secret information communication via public networks [1]. In the past 10 years, information hiding techniques have become an important information security technology. It is widespread in a great deal of application fields [2]. It, for example, is used for protecting secret information not to be perceptible. Secret information sender can apply the information hiding technique to embed secret information which can avoid being detected, stolen, or destroyed by unauthorized persons in the process of transmission. It mainly concerns with embedding of information in a "cover file" so that the very existence of hidden information is concealed. Anyone should not doubt or know the presence of secret messages except for the sender and the authorized users of the stego files. Information hiding is able to avoid suspicion from the visual view, which is lacking in traditional encryption system.

Steganography (or steganographic algorithm) is one of main branches of information hiding which refers to a number of disciplines. Security, capacity, and robustness are three main aspects that affect an information hiding system and its applications. Steganographic methods are concerned primarily with high security and capacity. Robustness is usually one of main research contents in the watermarking technology. Because of their inherent redundant information, digital files (such as digital images, videos, sound files, and other computer files) have widespread application for information hiding and steganography using as "cover files" or carriers to embed secret information.

In the information hiding systems, there are two types of information hiding algorithms. Methods based on spatial domain techniques are a kind of image steganographic techniques. In the spatial domain, information hiding algorithms can embed secret messages into the intensity of pixels value of images directly. The least significant bits (LSB) embedding is the simplest and most popular scheme for digital images. The LSBs of image pixel values have pseudo random and noise-like characteristics. So, embedding information in them cannot be visually detected. Methods based on spatial domain are a widely used technique due to its superior capacity, good image quality and its low computational complexity [3]. Hence, information hiding in the LSBs was one of the most early steganographic methods and its variations are still being considered by the researchers in this field. Methods based on transform domain techniques are another kind of image information hiding techniques. In the transform domain, images are first transformed to another domain (such as DCT domain), and then secret messages are embedded into transform domain coefficients in Ref. [2]. The LSBs of transform coefficients have also the same characteristics, such as pseudo random and noise-like characteristics.

The capacity or embedding rate is an important characteristic of a steganographic algorithm which is defined as the number of information bits that can be embedded in each pixel of a cover image. The embedding rate is one bit per pixel (bpp) in the two mentioned steganographic methods of LSB-F and LSB-M. When the hidden messages contain a smaller number of bits than the number

* Corresponding author. Tel. +86 02887720101.
E-mail address: tang4415@126.com (M. Tang).

http://dx.doi.org/10.1016/j.aeue.2015.08.011
1434-8411/

of the cover-image pixels, we assume that the information hiding is distributed randomly throughout the cover image based on a secret key (or stego key) shared with the authorized users of the stego image. Some of the classic algorithms will be presented as follows.

Mielikain proposed an information hiding method based on LSB matching revisited (LSB-MR) which has also better performance than the powerful LSB [4]. Using a pair of pixels as an information hiding unit, the secret information is embedded in the image pixels in LSB-MR. The LSB of the first pixel hides one bit of message, and a function of the two pixel values embeds another bit of message. Experimental results demonstrate that the proposed method is with fewer revisions to the pixels of the cover image than LSB-M when embedding the same capacity messages. The embedding rate is 0.5 bit per pixel (bpp) in LSB-MR. Omoomi et al. proposed a novel efficient high payload ± 1 steganographic scheme based on a special two variable binary functions [5]. Embedding capacity is 1.00 bit per pixel (bpp) in the EPES method.

The proposed information hiding methods can also be classified into two kinds, such as irreversible information hiding schemes (e.g., [6–10]) and reversible information hiding algorithms (e.g., [11–20]). Irreversible steganographic techniques may generally obtain better embedding capacity and higher image quality. Reversible information hiding methods get the advantages of the exact recovery of the original images when extraction of the embedded information. The latter is the fundamental research content of this paper.

Image interpolation is a rather important technique in digital image processing by which a small image is scaled-up larger. High speed and low time complexity are two main advantages of image interpolation method. Based on the existence information of image to estimate unknown approximation pixel values at the adjacent pixel positions, the size of the image is magnified by image interpolating methods up to several times or more. An interpolated image will always lose some quality after image interpolation is performed each time [9]. Image interpolation is widely used in the medical imaging processing in Ref. [21]. Moreover, medical imaging processing requires enormous amounts of information and extreme precision. So, it is essential for a better interpolating technique to reduce the processing time and remain or improve good quality of reconstructed images. It is important for a speedy and efficient interpolating technique that provides extremely good image quality.

It is a hot topic for combination interpolation technology with information hiding in recent years. In 2009, Jung and Yoo first proposed the use of image interpolation to information hiding in the spatial domain in Ref. [11]. The interpolating method proposed by Jung and Yoo in [11] is Neighbor Mean Interpolation (NMI). Using image interpolation technique, Luo et al. presented a reversible image watermarking method [12]. In [13], Lee et al. presented an interpolation technique by Neighboring Pixels (INP). By the interpolation technique, INP method hides secret information based on maximum adjacent pixels difference values. Using optional prediction error histogram modification, Ou et al. put forward a reversible watermarking method which reduced the image distortion of high capacity in Ref. [14]. Using the idea of reference pixel and multilayer hiding, Zeng et al. presented a Reversible Data Hiding Scheme (RDHS) based on the pixel difference histogram shifting to spare space for embedding secret information [15]. Based on image interpolation and direction order mechanism, Wang et al. proposed a reversible data hiding for high quality images in spatial domain [16]. Qian et al. presented a framework of reversible information hiding method in an encrypted JPEG bitstream [17]. Utilizing a multi-layer information embedding technique, Tang et al. proposed a high Capacity Reversible Steganography (CRS) [18]. When the good visual quality being retained, Wu et al. presented a novel reversible digital images information hiding algorithm [19]. Based on the minimum rate criterion and optimized histograms modification, Hu et al. [20] designed a reversible information hiding scheme by applying a pixel prediction method to embed secret information. Depending on adjacent pixels when image interpolation, information hiding scheme produces the estimated pixel values to fill in the blanks and hides secret sub-messages within them. This research may contribute to the improvement of embedding capacity. But, image quality is affected by introducing an image interpolation by neighboring pixels.

Based on the above analysis and research, the paper proposed a high capacity, Reversible and Adaptive Steganographic (RAS) method based on a novel image interpolation and image compensation technique. The rest of the paper is organized as follows. Section 2 introduces the image interpolation technique and information hiding algorithm proposed by Jung and Yoo [11], Lee and Huang [13], Zeng et al. [15] and Tang et al. [18]. Section 3 describes the proposed information hiding scheme and shows how the embedding capacity in the image interpolating method can be improved as well as good image quality being retained. The experimental results and performance analysis are presented in Section 4. Conclusions are finally outlined in Section 5.

2. Theoretical background

In this section, some classic reversible information hiding algorithms using image interpolation are reviewed, including NMI method [11], INP on maximum difference values [13], High Capacity Reversible Steganography using multilayer embedding (CRS) [18] and Reversible Data Hiding Scheme (RDHS) [15]. Let an input image, original image, cover image (or scaling-up), and stego image be I_i, O_i, C_i and S_i, respectively.

2.1. Neighbor Mean Interpolation (NMI)

The NMI method calculates the mean based on the neighboring pixel values, and inserts it into the blanks of scaling-up image C_i as a pixel. The calculation process of NMI method is as follows: for a 3×3 overlapping sub-block, $C_i(0, 0) = O_i(0, 0)$, $C_i(0, 1) = (O_i(0, 0) + O_i(0, 2))/2$, $C_i(1, 0) = (O_i(0, 0) + O_i(2, 0))/2$ and $C_i(1, 1) = (C_i(1, 0) + C_i(0, 1) + O_i(1, 1))/3$. A large amount of secret information can be embedded by the NMI method while maintaining good image quality. The experimental results of NMI method show that the average stego image quality is 24.44 (dB) measured by peak signal-to-noise ratio (PSNR), which is superior to the similar algorithms proposed before. Meanwhile, the NMI method gets the advantages of high speed and low time complexity. Therefore, the NMI method is appropriate for application of interpolation calculation with a large number of images. Please refer to [11] for the more detailed descriptions and contents of embedding and extracting procedures.

2.2. Interpolation by Neighboring Pixels (INP) on maximum difference values

At first, the INP scheme changes a $H \times G$ size input image I_i down to 1/4 (that is, $H/2 \times G/2$) of itself, and uses the reduced scale image as an original image O_i. Secondly, the INP method uses an interpolation method to enlarge O_i to form a four times image (that is a $H \times G$ cover image C_i). And then, after embedding secret information, a $H \times G$ stego image S_i comes into being from the cover image C_i. The authorized users can recover the original image O_i after the embedded secret information is extracted from the stego image S_i. Please refer to [13] for the more detailed descriptions and contents of embedding and extracting procedures.

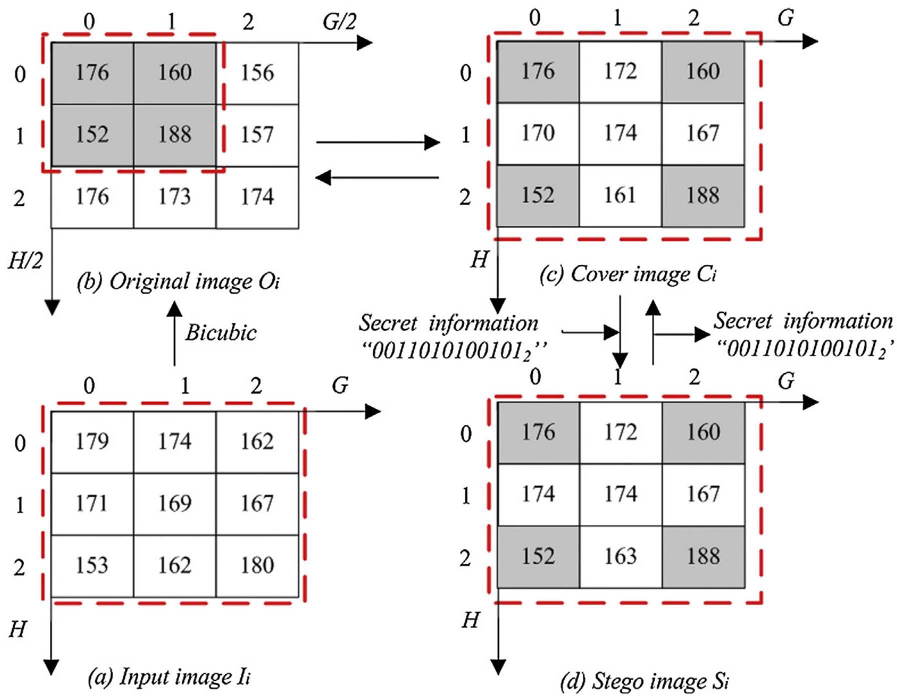

Fig. 1. 3 × 3 Overlapping blocks of interpolating image for embedding phase and embedding phase.

2.3. Reversible Data Hiding Scheme (RDHS) [15]

Zeng et al. presented a lossless information hiding method which is a reversible data hiding Scheme (RDHS) [15]. The pixel value difference histogram shifting is applied to spare space for information hiding in the proposed RDHS scheme. Adjacent pixels value differences are gained between a sub-block reference pixel and its neighboring pixels in a same sub-block. After the difference histogram shifting, a large number of secret information can be embedded into the cover image C_i, and multi-layer embedding technology is used to improve the embedding capacity. Different from previous works using histogram shifting, the RDHS scheme can extract the hidden information and recover the exact original image O_i by a small amount of related information which is the length of embedded information and the stego image itself. Experimental results show that the average capacity among eight commonly used grayscale images is up to 1.08 bits per pixel (bpp) while remaining lower image distortion. Please refer to [15] for the more detailed description of embedding and extracting procedures.

2.4. High Capacity Reversible Steganography using multilayer embedding (CRS) [18]

The *CRS* algorithm takes full advantages of the similar characteristics of neighboring pixels limiting value from a $H/2 \times G/2$ original image O_i. The proposed CRS method is applied to reproduce a scaling-up cover image C_i (that is a $H \times G$ interpolation image) to be used in the next phase of secret information embedded. $B_{Min} = Min\{C_i(u, v), C_i(u+2, v), C_i(u, v+2), C_i(u+2, v+2)\}$, $B_{Max} = Max\{C_i(u, v), C_i(u+2, v), C_i(u, v+2), C_i(u+2, v+2)\}$, $MD = (3 \times B_{Min} + B_{Max})/4$, $C_i(u, v) = I_i(u, v)$, $C_i(u, v+1) = (MD + (C_i(u, v) + C_i(u, v+2))/2)/2$, $C_i(u+1, v) = (MD + (C_i(u, v) + C_i(u+2, v))/2)/2$, $C_i(u+1, v+1) = ((C_i(u, v) + C_i(u+1, v) + C_i(u, v+1))/3$. Please refer to [18] for the more detailed description of embedding and extracting procedures.

In order to increase the embedding capacity, we design a novel image interpolating technique based on INP method [13] and *CRS* scheme [18], where a cover image C_i is reproduced by a novel extended image interpolating technique. So the performance of this method is closely related to that of the novel image interpolation technique. This method increases embedding capacity largely by changing the value difference between adjacent pixels. The embedding and extracting procedures are described in detail in Section 3.

3. The proposed method

This paper improved the Lee et al. and Tang et al.'s information hiding algorithm by inventing a novel image interpolating technique and the embedding capacity. Fig. 1 shows that the process of the use of interpolating technique to generate a cover image C_i from an original image O_i. And then, after secret messages are embedded the cover image C_i, a stego image S_i is output. Since the cover image C_i is produced by interpolation technique, the better performance for the interpolation technique is, the better image quality of a stego image S_i is after a large number of secret information is embedded. For practical application reasons, therefore, the resemblance between the cover image C_i and the input image I_i should be as maximal as possible. To achieve this objective, this proposed RAS method also considers the property of pixel localization to design image interpolating technique with better image quality as indicated in Section 3.1. Since images usually contain some redundancies of the image format, a slight image distortion can usually achieve to enhance the amount of embedding capacity. This research uses the satisfactory results of redundancy from an effective image interpolation to modify the difference values between neighboring pixels for improving embedding capacity up to the larger. The example of embedding and extracting phases are described in detail in Section 3.2.

3.1. High capacity and adaptive steganographic algorithm based on novel image interpolation (RAS)

Let I_i be an input image sized $H \times G$. I_i is resized to be an original image O_i whose size is $H/2 \times G/2$. The RAS method makes full use of similar properties of adjacent pixels in the original image O_i to reproduce a $H \times G$ cover image C_i. After embedding the secret information into the cover image C_i, a stego image S_i is formed. Let the $O_i(h, g)$ denote a pixel value in (h, g) in the original image O_i and the $C_i(u, v)$ describe a pixel value in the pixel location (u, v) of the cover image C_i. The above course of the cover image C_i formed in RAS is outlined in Eq. (1).

$$\begin{aligned} &C_i(u, v) = O_i(h, g)\\ &C_i(u, v+1) = (C_i(u, v) + ((C_i(u, v) + C_i(u, v+2))/2)/2\\ &C_i(u+1, v) = (C_i(u, v) + ((C_i(u, v) + C_i(u+2, v))/2)/2\\ &C_i(u+1, v+1) = (C_i(u, v) + (C_i(u+1, v) + C_i(u, v+1))/2)/2\\ &u = 2h, v = 2g\\ &h, g = 0, 1, 2, \ldots 127. \end{aligned} \tag{1}$$

The pixel value $C_i(u, v)$ and $O_i(h, g)$ are seen as a perpetual pixel as Eq. (1) (shown in Fig. 1b and c). So, the perpetual pixel value $C_i(u, v)$ will remain unchanged in the whole process of secret messages embedded. That is, $S_i(u, v) = C_i(u, v) = O_i(h, g)$, where $u = 2h$ and $v = 2g$.

Please notice that the maximum value B_{Max} and minimum value B_{Min} are obtained from a same $K \times K$ (such as K=3) sub-block of cover image C_i (shown in Fig. 1c). After calculating the value B_{Max} and value B_{Min}, respectively, median value *Midpoint* between B_{Max} and B_{Min} can be given in the same sub-block. The difference values of f_1, f_2 and f_3 are also calculated between pixels $C_i(u, v+1)$, $C_i(u+1, v)$, $C_i(u+1, v+1)$, B_{Max} and B_{Min} based on Eq. (2). But, the difference values are only calculated from three adjacent pixels of the permanent pixel $C_i(u, v)$, the minimum value B_{Min} and maximum value B_{Max}. That is to say, f_1, f_2 and f_3 are calculated according to Eq. (2).

$$\begin{aligned} &B_{Min} = Min\{C_i(u, v), C_i(u+2, v), C_i(u, v+2), C_i(u+2, v+2)\}\\ &B_{Max} = Max\{C_i(u, v), C_i(u+2, v), C_i(u, v+2), C_i(u+2, v+2)\}\\ &Midpoint = (B_{Min} + B_{Max})/2\\ &f_1 = \begin{cases} C_i(u, v+1) - B_{Min}, & C_i(u, v+1) \geq Midpoint,\\ B_{Max} - C_i(u, v+1), & \text{otherwise.} \end{cases}\\ &f_2 = \begin{cases} C_i(u+1, v) - B_{Min}, & C_i(u+1, v) \geq Midpoint,\\ B_{Max} - C_i(u+1, v), & \text{otherwise.} \end{cases}\\ &f_3 = \begin{cases} C_i(u+1, v+1) - B_{Min}, & C_i(u+1, v+1) \geq Midpoint,\\ B_{Max} - C_i(u+1, v+1), & \text{otherwise.} \end{cases} \end{aligned} \tag{2}$$

And then, f_t will be used to determine how many bits of secret sub-messages can be embedded into a pixel value of corresponding position in the cover image C_i. L_t describes the amount of information in bits and it is calculated by f_t based on Eq. (3). The function $INT(real - number)$ represents an integer which is not more than "$real - number$".

$$L_t = INT(\log_2(f_t)) \tag{3}$$

Let N_t be a bit string of L_t secret messages bits to be embedded. The average value *Avg* is calculated by a summation of $C_i(u, v)$, $C_i(u+2, v)$, $C_i(u, v+2)$, and $C_i(u+2, v+2)$ based on Eq. (4). The neighboring interpolation pixels $C_i(u, v+1)$, $C_i(u+1, v)$ and $C_i(u+1, v+1)$ of each unchanged pixel $C_i(u, v)$ can transmit the secret sub-information N_t, where t = 1, 2 and 3, respectively. Thus, the corresponding stego pixels $S_i(u, v+1)$, $S_i(u+1, v)$ and $S_i(u+1, v+1)$ can be calculated by Eq. (4).

$$\begin{aligned} &Avg = Sum\{C_i(u, v), C_i(u+2, v), C_i(u, v+2), C_i(u+2, v+2)\}/4\\ &S_i(u, v) = C_i(u, v)\\ &S_i(u, v+1) = \begin{cases} Min\{C_i(u, v+1), Avg\} + N_1, & I_i(u, v+1) \geq Min\{C_i(u, v+1), Avg\},\\ MinC_I(u, v+1), Avg - N_1, & \text{otherwise.} \end{cases}\\ &S_i(u+1, v) = \begin{cases} Min\{C_i(u+1, v), Avg\} + N_2, & I_i(u+1, v) \geq Min\{C_i(u+1, v), Avg\},\\ Min\{C_i(u+1, v), Avg\} - N_2, & \text{otherwise.} \end{cases}\\ &S_i(u+1, v+1) = \begin{cases} Min\{C_i(u+1, v+1), Avg\} + N_3, & I_i(u+1, v+1) \geq Min\{C_i(u+1, v+1), Avg\},\\ Min\{C_i(u+1, v+1), Avg\} - N_3, & \text{otherwise.} \end{cases}\\ &u = 2h, v = 2g\\ &h, g = 0, 1, 2, \ldots, 127. \end{aligned} \tag{4}$$

The procedure of embedding scheme in RAS algorithm is sketched as follows.

Algorithm 1. Procedure of reversible and adaptive information hiding algorithm (RAS).

Algorithm 1: Procedure of reversible and adaptive information hiding algorithm (RAS)

Input:
An input image I_i with size $H \times G$ is provided, where $I_i(u, v)$ represents a pixel value in the position (u, v) of the input image I_i, $h = 0, 1, \ldots, (H/2) - 1$, $g = 0, 1, \ldots, (G/2) - 1$.
Output:
A stego image S_i of size $H \times G$.

begin
- **Step 1.** Initialize the set index variables: $u \leftarrow 0$, $v \leftarrow 0$;
- **Step 2.** Produce an original image O_i size of $H/2 \times G/2$ based on a $H \times G$ input image I_i by image processing tools;
- **Step 3.** A $H \times G$ cover image C_i is provided using Eq. (1);
- **Step 4.** If all of image pixel values have been used over in cover image C_i, Go to Step 8. Otherwise, continue with Step 5;
- **Step 5.** Choose a pixel sub-block size of $k \times k$. Calculate f_k based on Eq. (2) and L_k based on Eq. (3);
- **Step 6.** Embed secret messages in $C_i(u, v+1), C_i(u+1, v)$ and $C_i(u+1, v+1)$ in cover image C_i based on Eq. (4);
- **Step 7.** If all of secret messages have been depleted, output a stego image S_i and go to Step 8. Otherwise, go to Step 4;
- **Step 8.** End

end

3.2. Example

To continue with the example of the original image O_i, the cover image C_i and the stego image S_i by RAS in Fig. 1.

Let S_M be a bitstream of secret messages. Assume S_M = “001101010101_2” which is to be embedded into a cover image C_i without loss of generality. First, let $u = v = 0$ and determine the maximum value $B_{Max} = Max$ $\{C_i(0, 0), C_i(0, 2), C_i(2, 0), C_i(2, 2)\} = Max\{176, 160, 152, 188\} = 188$, the minimum value $B_{Min} = Min\{C_i(0, 0), C_i(0, 2), C_i(2, 0), C_i(2, 2)\} = Min\{176, 160, 152, 188\} = 152$, $Avg = 169$ and $Midpoint = 170$ of the four pixels $C_i(u, v)$, $C_i(u, v+2)$, $C_i(u+2, v)$ and $C_i(u+2, v+2)$ in a 3×3 overlapping sub-block.

Calculate the difference values f_t to ascertain the number of bits, L_t, of secret information to embed into the cover selected pixels from the RAS based on Eqs. 2 and 3. Calculate the difference values f_1, f_2 and f_3 to determine the amount of secret messages embedded. The difference values L_1, L_2 and L_3 are determined as follows: $L_1 = 172 - 152 = 20$, $L_2 = 170 - 152 = 18$ and $L_3 = 174 - 152 = 22$.

$$
\begin{aligned}
L_1 &= \lfloor \log_2 f_1 \rfloor = \lfloor \log_2 20 \rfloor = 4 \\
L_2 &= \lfloor \log_2 f_2 \rfloor = \lfloor \log_2 18 \rfloor = 4 \\
L_3 &= \lfloor \log_2 f_3 \rfloor = \lfloor \log_2 22 \rfloor = 4
\end{aligned} \tag{5}
$$

Because $L_1 = 4, L_2 = 4$ and $L_3 = 4$, the length of secret sub-message L_1 is 4 bits, 4 bits for L_2 and L_3, too. Because of the determination of the length L_t (t = 1, 2 and 3) of embedding secret information, their values are $N_1 = \text{“}0011_2^{''} = 3_{10}$, $N_2 = \text{“}0101_2^{''} = 5_{10}$ and $N_3 = \text{“}0101_2^{''} = 5_{10}$, respectively. Finally, the secret sub-information can be embedded using Eq. (4) and the stego image pixels are produced as shown in Fig. 2c, such as $S_1 = Avg + 3 = 169_{10} + 3_{10} = 172_{10}$.

The extraction procedure is a reversible process of the embedding procedure described in RAS method.

In the extracting procedure, every nine stego pixels within a same sub-block are $S_i(u, v), S_i(u+1, v), S_i(u+2, v), S_i(u, v+1), S_i(u+1, v+1), S_i(u+2, v+1), S_i(u, v+2), S_i(u+1, v+2)$ and $S_i(u+2, v+2)$. The B_{Max} and B_{Min} are computed by determining the maximum value of the four unchanged pixels $S_i(u, v), S_i(u+2, v), S_i(u, v+2)$ and $S_i(u+2, v+2)$, for each 3×3 same sub-block, i.e., $B_{Max} = Max\{S_i(u, v), S_i(u+2, v), S_i(u, v+2), S_i(u+2, v+2)\}$, $B_{Min} = Min\{S_i(u, v), S_i(u+2, v), S_i(u, v+2), S_i(u+2, v+2)\}$, Avg and $Midpoint$.

$$
\begin{aligned}
N_1 &= \begin{cases} S_i(u, v+1) - Min\{C_i(u, v+1), Avg\}, & S_i(u, v+1) \geq Min\{C_i(u, v+1), Avg\}, \\ MinC_I(u, v+1), Avg - S_i(u, v+1), & \text{otherwise.} \end{cases} \\
N_2 &= \begin{cases} S_i(u+1, v) - Min\{C_i(u+1, v), Avg\}, & S_i(u+1, v) \geq Min\{C_i(u+1, v), Avg\}, \\ Min\{C_i(u+1, v), Avg\} - S_i(u+1, v), & \text{otherwise.} \end{cases} \\
N_3 &= \begin{cases} S_i(u+1, v+1) - Min\{C_i(u+1, v+1), Avg\}, & S_i(u+1, v+1) \geq Min\{C_i(u+1, v+1), Avg\}, \\ Min\{C_i(u+1, v+1), Avg\} - S_i(u+1, v+1), & \text{otherwise.} \end{cases} \\
& u = 2h, v = 2g \\
& h, g = 0, 1, 2, \ldots, 127.
\end{aligned} \tag{6}
$$

The next step is to compute the difference value between each selected pixel, B_{Max} and B_{Min} to determine the amount of embedded secret sub-information. In Fig. 1b, the original image O_i recovered can remain perpetual. This is because the four perpetual pixels of cover image C_i are equal to original image $O_i(0, 0)$, $O_i(0, 1)$, $O_i(1, 0)$ and $O_i(1, 1)$ as shown in Fig. 1b and c. Once the original image O_i is recovered, the maximum value $B_{Max} = 188$ and minimum value $B_{Min} = 152$ from the four unchanged pixels of $C_i(0, 0)$, $C_i(0, 2)$, $C_i(2, 0)$ and $C_i(2, 2)$ in the same 3×3 sub-block. Afterwards, the receiver can compute the other interpolating pixels $C_i(0, 1) = 172$, $C_i(1, 0) = 170$, and $C_i(1, 1) = 174$ by RAS method. And then, we can calculate the difference values between B_{Max} and B_{Min}, Avg, $Midpoint$ and interpolating pixel values to judge the amount of secret information embedded. The difference values f_1, f_2 and f_3 are 20, 18 and 22. The number bits of secret sub-message L_1, L_2 and L_3, are 4, 4 and 4, respectively. The difference values N_1, N_2 and N_3 are 3, 5 and 5 based on Eq. (6), respectively. According to f_t and L_t, the sub-message “0111_2”, “0010_2” and “1100_2” are formed by N_t. At last, the secret information is extracted, such as $S_M = \text{“}0011_2^{''} \| \text{“}0101_2^{''} \| \text{“}0101_2^{''} = \text{“}001101010101_2^{''}$.

Fig. 2. Input image I_i and stego image S_i for eight images.

4. Experimental evaluation and performance analysis

In this section, we will demonstrate the experimental evaluation and performance analysis of the proposed method. The experimental tools are *Matlab R*2009*a* and *Adobe Photoshop CS*6.0. All of test images which are downloaded from [22,23] and the Internet are 512×512 and 512×384 (or 384×512) in size, respectively. The experimental process was divided into two steps. The detailed experiments, results and performance analysis are as follows.

In the RAS experiment, each 512×512 or 512×384 (or 384×512) input gray-scale image I_i is firstly reduced down to 256×256 or 256×192 (or 192×256) using image processing tools, such as *Adobe Photoshop CS*6.0, and taken it is as an original image O_i. Secondly, using Eq. (1), a cover image C_i is reproduced to hide secret information whose size is 512×512 or 512×384 (or 384×512).

In the first experiment, eight 8-bit gray scale test images (shown in Fig. 2) selected randomly with 512×512 size are used in the next group of experiments. Firstly, eight 8-bit gray images are randomly selected as input images I_i (shown in Fig. 2). The input images I_i are the images marked by (a) "Lena", (b) "Airplane", (c) "Tiffany", (d) "Peppers", (e) "Baboon", (f) "Boat", (g) "Zelda" and (h) "Goldhill", respectively. The stego images S_i are the images marked by (i) "Lena_s", (j) "Airplane_s", (K) "Tiffany_s", (l) "Peppers_s", (m) "Baboon_s", (n) "Boat_s", (o) "Zelda_s" and (p) "Goldhill_s", respectively. The PSNR (peak signal-to-noise ratio) is used to evaluate the image quality of the input images I_i and the stego images S_i (shown

Table 1
A comparison of payload (bpp) and image quality (PNSR) between INP, NMI and CRS methods.

Test image	*RAS method*			*INP method*		
	Payload		PSNR (dB)	Payload		PSNR (dB)
	Payload (bits)	Payload (bpp)		Payload (bits)	Payload (bpp)	
Lena	434,130	1.6561	37.8689	317,959	1.2129	37.1407
Airplane	412,990	1.5754	37.0148	307,134	1.1716	36.6408
Tiffany	376,746	1.4372	37.8654	271,764	1.0367	37.4476
Peppers	427,287	1.6300	37.3711	313,716	1.1967	36.9355
Baboon	690,097	2.6325	31.3577	528,666	2.0167	30.9864
Boat	501,895	1.9146	35.2349	360,828	1.3764	34.7524
Zelda	344,227	1.3131	42.7275	241,590	0.9216	43.3870
Goldhill	711,871	2.7156	34.1212	549,575	2.0965	33.6624
Test image	*NMI method*			*CRS method*		
	Payload		PSNR (dB)	Payload		PSNR (dB)
	Payload (bits)	Payload (bpp)		Payload (bits)	Payload (bpp)	
Lena	193,642	0.7387	35.6691	410,871	1.5673	37.1282
Airplane	155,655	0.5938	35.6761	394,152	1.5036	36.7394
Tiffany	141,234	0.5388	36.4454	358,308	1.3668	37.5732
Peppers	161,894	0.6176	35.8331	404,725	1.5439	37.0731
Baboon	331,435	1.2643	30.6744	654,828	2.4980	31.3098
Boat	200,003	0.7630	34.0807	474,199	1.8089	34.9859
Zelda	115,432	0.4403	40.2723	326,152	1.2442	42.5804
Goldhill	359,626	1.3719	32.2505	676,234	2.5796	33.7749
Test image	*RDHS method*					
	Payload[a]		PSNR (dB)	*Payload*[b]		PSNR (dB)
	Payload (bits)	Payload (bpp)		Payload (bits)	Payload (bpp)	
Lena	310,931	1.1861	30.5420	310,267	1.1835	30.5420
Airplane	345,188	1.3168	31.4113	345,188	1.3168	31.4113
Tiffany	354,734	1.3532	30.9621	354,734	1.3532	30.9621
Peppers	341,985	1.3046	31.1672	269,817	1.0293	31.1672
Baboon	141,553	0.5400	28.9462	136,857	0.5221	28.9462
Boat	300,321	1.1456	30.5863	299,545	1.1427	30.5815
Zelda	327,867	1.2507	30.5912	290,467	1.1080	30.5913
Goldhill	249,719	0.9526	29.9105	249,719	0.9526	29.9105

in Fig. 2). If peak signal-to-noise ratio is more than 30 dB, it is usually imperceptible to human eyes for the stego image S_i distortion [13]. The experimental results of image quality between each input image I_i and the corresponding stego image S_i are shown in Table 1.

An example is considered by the "(e) Baboon" image. Firstly, the image marked by "(e) Baboon" is used as an input image I_i (shown in Fig. 2). Secondly, we create an original image O_i by image processing tools, such as *Adobe Photoshop CS*6.0. Thirdly, a cover image C_i is produced depending on Eq. (1) on the basis of original image O_i. Then, a stego image S_i comes into being, such as "(m) *Baboon*$\_s''$ (shown in Fig. 1(m)) after the secret information is embedded. The image distortion in the stego image C_i is imperceptible to human eye as shown in Fig. 1 because PSNR is 31.3577 (dB) and greater than 30 (dB).

There are six kinds of image information hiding methods which are "*RAS method*″, "*INP method*″, "*NMI method*″, "*CRS method*″, "*RDHS method* (*Payload*^{a})″ and "*RDHS method* (*Payload*^{b})″, (shown, respectively, in Table 1). The capacity obtained by "*RAS method*″ is the largest one of the six kinds of image processing ways. However, if PSNR is smaller than 30 dB, image distortion in the stego image usually may be more easily perceived by human eyes. If the capacity and image quality are comprehensively considered at the same time, the results obtained from the method of "RAS scheme" is the best one of the six kinds of methods.

For example, the capacity of "*Lena*″ is 1.6561 (bpp) (or 434,130 (bits)) in our proposed method using "*Bicubic*″ from Table 1. Under the same conditions, the capacity of "*Lena*″ is 1.2129 (bpp) in INP method, 0.7387 (bpp) in NMI method, 1.5673 (bpp) in CRS method, 1.1861(bpp) in RDHS method (*Payload*^{a}) and 1.1835 (bpp) RDHS method (*Payload*^{b}) using "*Bicubic*″, respectively. Clearly, the capacity of RAS is higher than that of others substantially for eight test images in Table 1. PSNR of "*Lena*″ is 37.8689 (dB) using "*Bicubic*″ in RAS method. Under the same conditions, PSNR of "*Lena*″ is 37.1407 (dB) in INP method, 35.6691 (dB) in NMI method, 37.1282 (dB) in CRS method, 30.5420 (dB) in RDHS method (*Payload*^{a}) and 30.5420 (dB) in RDHS method (*Payload*^{b}) using "*Bicubic*″, respectively. Furthermore, the image quality of the proposed scheme (RAS) is superior to that of the INP scheme by Lee and Huang [13] for seven test images in Table 1. It demonstrates that the novel image interpolation technique of the proposed method can be better applied to information hiding with the improved capacity and maintain the image quality.

And then, there are 1338 8-bit gray scale randomly selected test images (512×384 or 384×512) used in the second experiment, which involves the comparison of capacity and PSNR for image interpolation and information hiding schemes.

There are the pure payloads (bits) of 300 images selected at random which are listed in Fig. 3 for a comparison between RAS and other reversible methods, such as CRS, INP and NMI methods. The sizes of test images are 512×384 or 384×512. From the Fig. 3, we can refer to the experimental results which prove a better pure capacity than other methods. The maximum and minimum values of pure payloads (bits) are from 663,718 and 171,784 (bits), respectively. The maximum and minimum values of pure payloads (bits)

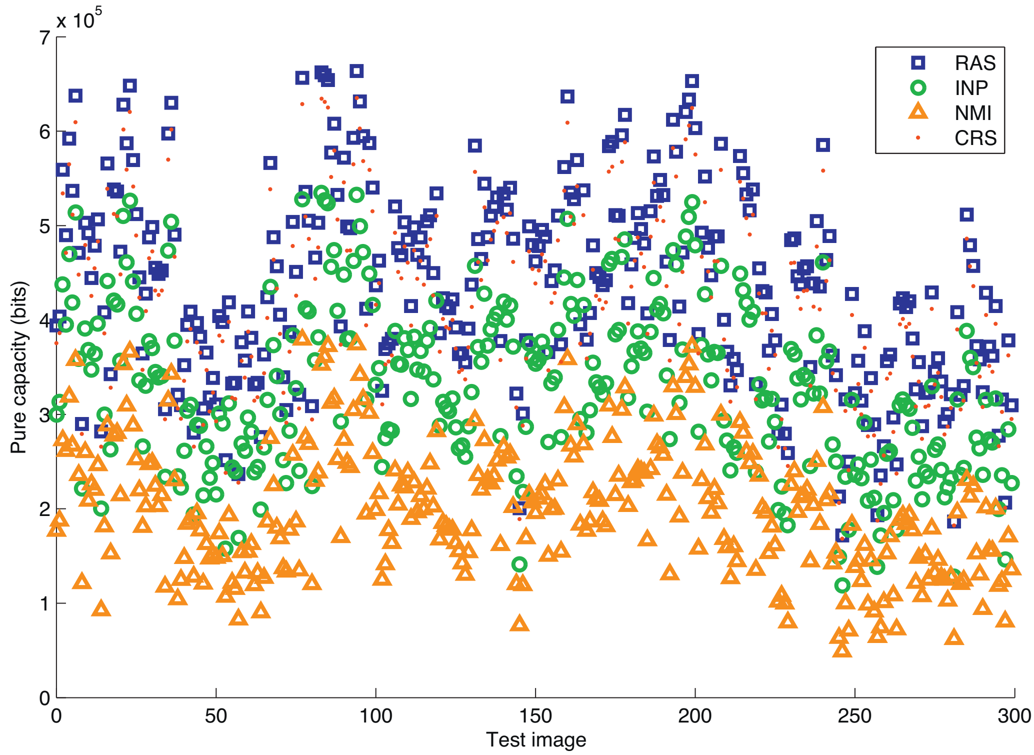

Fig. 3. A comparison of pure capacity (bits) between the four interpolation methods.

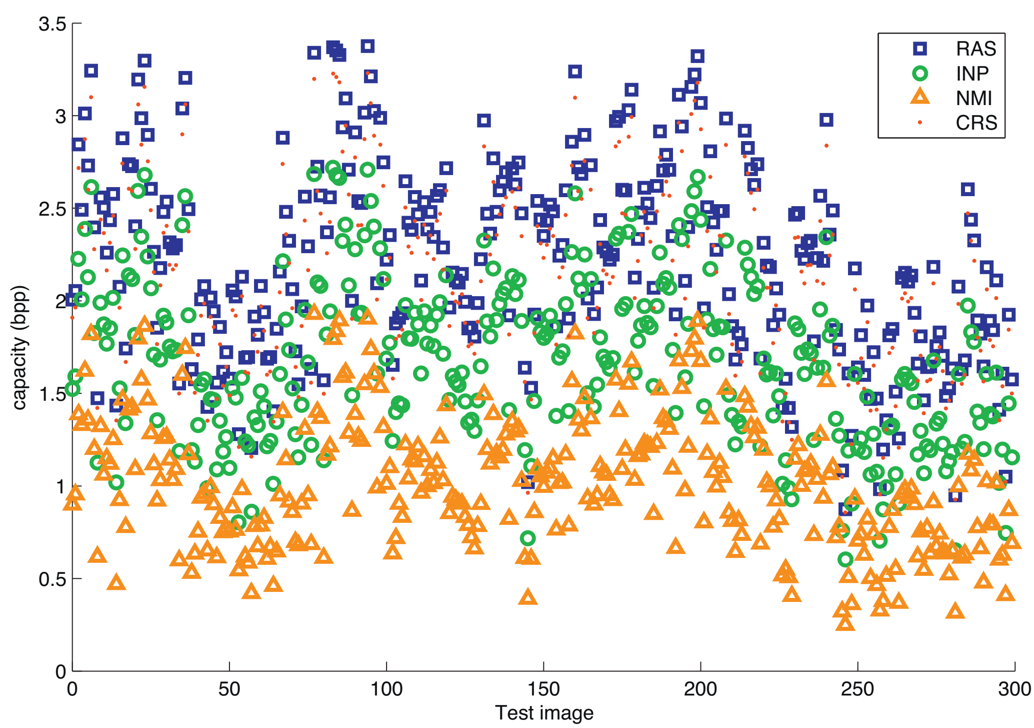

Fig. 4. A comparison of payload (bpp) between the four interpolation methods.

are from 534,644 and 118,627 (bits) in INP method, respectively. The maximum and minimum values of pure payloads (bits) are from 379,377 and 49,059 (bits) in NMI method, respectively. The maximum and minimum values of pure payloads (bits) are from 635,159 and 168,446 (bits) in CRS method, respectively. Note that the pure payload represents the largest amount of pure payload.

The payloads (bpp) of 300 images selected at random are listed in Fig. 4 for a comparison between RAS and other reversible methods. The sizes of test images are 512 × 384 or 384 × 512. The maximum and minimum values of payloads (bpp) are from 3.3758 (bpp) and 0.8737 (bpp), respectively. Note that the payload represents the highest amount of payload.

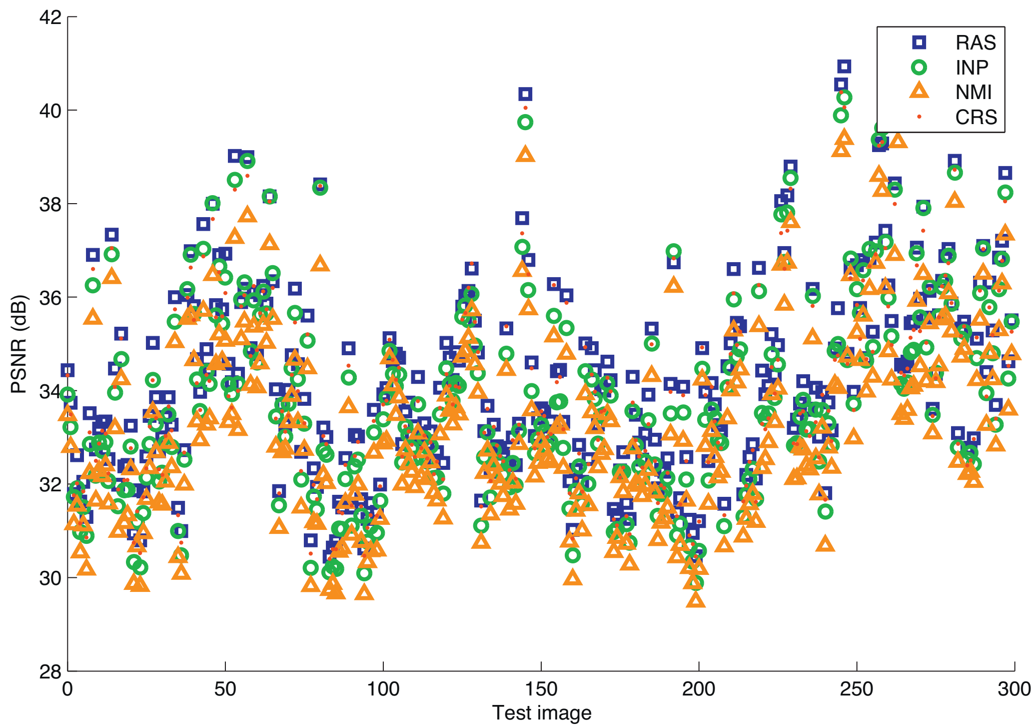

Fig. 5. A comparison of PSNR values between the four interpolation methods.

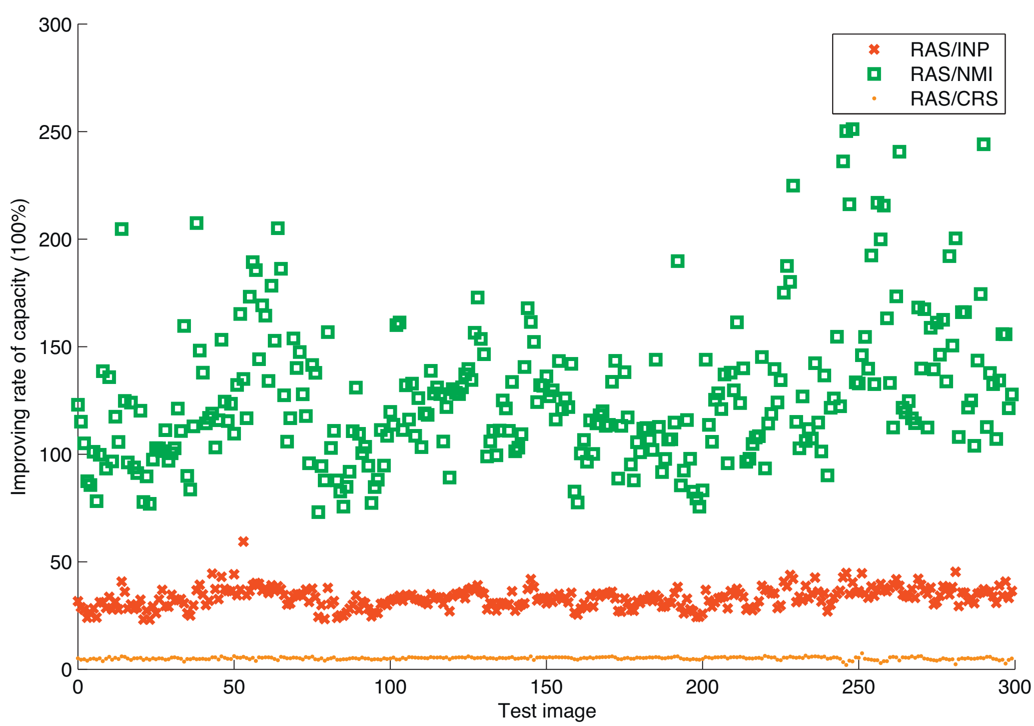

Fig. 6. The payload increasement rate comparison of RAS with INP, NMI and CRS, respectively.

There are the PSNRs (dB) of 300 images selected randomly which are listed in Fig. 5 for a comparison between RAS and other reversible methods. The maximum and minimum values of PSNRs (dB) are from 40.9356 (dB) and 30.4454 (dB) in RAS method, respectively. The number of images whose PSNRs (dB) are less than 30 (dB) is zero in RAS. The maximum and minimum values of PSNRs (dB) are from 40.3882 (dB) and 30.3981 (dB) in CRS method, respectively. The number of images whose PSNRs (dB) are smaller than 30 (dB) is zero in CRS. The maximum and minimum values of PSNRs (dB) are from 40.5576 (dB) and 29.8811 (dB) in INP method, respectively. The number of images whose PSNRs (dB) are less than 30 (dB) is one in INP. The maximum and minimum values of PSNRs (dB) are from 39.3842 (dB) and 29.4890 (dB) in NMI method, respectively. The number of images whose PSNRs (dB) are less than 30 (dB) is 10 in NMI method. Figs. 4 and 5 show that the proposed method RAS has larger information embedding capacity and higher PSNR. Note that PSNR is the amount of best PSNR.

The number of images whose PSNRs (dB) are smaller than 30 (dB) is 8 in RAS, 26 in INP, 61 in NMI and 20 in CRS in 1338 test images. Under the same conditions, the RAS could embed more information compared with other reversible methods and contain highest capacity and keep good visual quality as shown in Fig. 5, which the PSNR is guaranteed to be higher than 30 dB.

The Fig. 6 shows that RAS has a larger improvement in the capacity or payload compared with the scheme of NMI, INP and CRS. For 1338 test images, compared to the scheme of Lee and Huang, the experimental results of the proposed information hiding scheme present the payload improved by up to 23.11–59.42% without increasing image distortion. Compared to the scheme of NMI method, the experimental results of proposed information hiding scheme presents the payload improved by up to 73.07–251.15% without increasing image distortion for 1338 test images. Compared to the scheme of the CRS method, the experimental results of the proposed information hiding scheme presents the payload improved by up to 1.98–7.43% without increasing image distortion for 1338 test images.

Finally, the proposed method is compared with other three state-of-the-art reversible watermarking or data hiding methods in payload increasement rate (shown in Fig. 6). From Table 1, Figs. 3 and 4, we can see that the RAS method provides a better payload (bpp) than other three methods. In comparison with other reversible information hiding methods, the experimental results have shown that the proposed method provides a better capacity to hide secret information.

5. Conclusions

The paper has proposed a high payload, reversible and adaptive information hiding method using a novel image interpolation. The proposed method has still lower time complexity and faster calculation speed. And then, the information hiding method, based on the difference values between neighboring pixels and image quality compensation method, was proposed. The proposed RAS method may be applicable to secret messages embedded and reversible information hiding method.

The RAS method improved the Lee and Huang's and CRS's approach to develop a novel information hiding scheme based on the RAS image interpolation. Like the Lee and Huang's scheme and CRS's method, interpolating images are produced according to the similarities between neighboring pixels. Therefore, the proposed scheme still maintains the advantage of low computing complexity and has better performance in interpolating pixels to reduce false effects, reproduced enlarged images that were the most visually pleasing. In addition, using image quality compensation method, the RAS yields higher PSNRs than other methods, such as NMI, INP and CRS, which shows the performance of the proposed image interpolating method in image quality is superior to others. Compared to the scheme of NMI, INP and CRS, the experimental results of proposed information hiding scheme presents the payload improved to different degrees without increasing image distortion. So, this substantial performance improvement shows the effectiveness of the proposed scheme. In future work, we will apply these techniques in the image compressed domain.

Acknowledgments

This work is supported by Natural Science Foundation of China (No. 61402376), the Key of Scientific Research Funds Project of Educational Department of Sichuan Province (No. 13ZA0019), the Key of Scientific Research Funds Project of Xihua University (No. Z1222623, Z1322622), the Scientific Research Funds Project of Science and Technology Department of Sichuan Province (No. 2013JY0089, 15JC0117), the Fundamental Research Funds for the Central Universities (No. SWJTU12BR045), the Key Funds Project of Sichuan Provincial Department of Education (13zA0019), the Scientific Research Funds Project of "Chun Hui" plan of Ministry of Education of China (No. z2014051) and the Foundation of Cyberspace Security Key Laboratory of Sichuan Higher Education Institutions (No. sjzz2014-077).

References

[1] Fridrich J, Goljan M, Du R. Reliable detection of LSB steganography in color and grayscale images. In: Proceedings of the 2001 Workshop on Multimedia and Security: New Challenges. ACM; 2001. p. 27–30.
[2] Petitcolas F, Anderson R, Kuhn M. Information hiding – a survey. Proceedings of the IEEE 1999;87(7):1062–78.
[3] Ker A. Improved detection of LSB steganography in gray-scale images. In: Proc. Information Hiding Workshop, LNCS 3200. Springer; 2004. p. 97–115.
[4] Mielikainen J. LSB matching revisited. IEEE Signal Process Lett 2006;13(5):285–7.
[5] Omoomi M, Samavi S, Dumitrescu S. An efficient high payload ±1 data embedding scheme. Multimed Tools Appl 2011;54(2):201–18.
[6] Chan C, Cheng L. Hiding data in images by simple LSB substitution. Pattern Recognit 2004;37(3):469–74.
[7] ChengHsing Yang, ChiYao Weng, ShiuhJeng Wang. Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Trans Inf Forensics Secur 2008;3(3):488–97.
[8] Chen W, Chang C, Le THN. High payload steganography mechanism using hybrid edge detector. Expert Syst Appl 2010;37(4):3292–301.
[9] Lee C, Chang W. Recovery of color images by composed associative mining and edge detection. J Inf Hiding Multimed Signal Process 2010;1(4):310–24.
[10] Sun H, Weng C, Lee C, Yang C. Anti-forensics with steganographic data embedding in digital images. IEEE J Sel Areas Commun 2011;29(7):1392–403.
[11] Jung K, Yoo K. Data hiding method using image interpolation. Comput Stand Interfaces 2009;31(2):465–70.
[12] Luo L, Chen Z, Chen M, Zeng X, Xiong Z. Reversible image watermarking using interpolation technique. IEEE Trans Inf Forensics Secur 2010;5(1):187–93.
[13] Lee C, Huang Y. An efficient image interpolation increasing payload in reversible data hiding. Expert Syst Appl 2012;39(8):6712–9.
[14] Ou B, Zhao Y, Ni R. Reversible watermarking using optional prediction error histogram modification. Neurocomputing 2012;93:67–76.
[15] Zeng X, Li Z, Ping L. Reversible data hiding scheme using reference pixel and multi-layer embedding. AEÜ – Int J Electron Commun 2012;66(7):532–9.
[16] Wang X, Chang C, Nguyen T, Li M. Reversible data hiding for high quality images exploiting interpolation and direction order mechanism. Digit Signal Process 2013;23(2):569–77.
[17] Qian Z, Zhang X, Wang S. Reversible data hiding in encrypted JPEG bitstream. IEEE Trans Multimed 2014;16(5):1486–91.
[18] Tang M, Hu J, Song W. A high capacity image steganography using multi-layer embedding. Optik 2014;125(15):3972–6.
[19] Wu H, Dugelay J, Shi Y. Reversible image data hiding with contrast enhancement. IEEE Signal Process Lett 2015;22(1):81–5.
[20] Hu X, Zhang W, Li X, Yu N. Minimum rate prediction and optimized histograms modification for reversible data hiding. IEEE Trans Inf Forensics Secur 2015;10(3):653–64.
[21] Thevenaz P, Blu T, Unser M. Interpolation revisited. IEEE Trans Med Imaging 2000;19(7):739–58.
[22] T. U. of Southern California, USC-SIPI Image Database, http://sipi.usc.edu/services/database/database.html [02/01/2013].
[23] L. University, UCID Image Dataset, http://homepages.lboro.ac.uk/cogs/datasets/ucid/data/ucid.v2.tar.gz [03/01/2013].

Mingwei Tang is an associate professor with the School of Mathematics and Computer Science Technology of Xihua University. He received a Ph.D. degree at the School of Computer Science and Engineering from University of Electronic Science and Technology of China in 2011. His current research interests include network security and information hiding.

Jie Hu is currently pursuing the Ph.D. degree at the School of Information Science and Technology of Southwest Jiaotong University from 2011. Her current research interests include network security and data mining.

Wen Song is a professor of Xihua University since 2005 and senior member of Petri net Special Commission. His main research interests are theory of Petri nets and mathematical logic.

Shengke Zeng is an associate professor with the School of Mathematics and Computer Science Technology of Xihua University. She received a Ph.D. degree at the School of Computer Science and Engineering from University of Electronic Science and Technology of China in 2013. His current research interests include network security, digital signature and information hiding.