Multimed Tools Appl (2015) 74:2143–2155
DOI 10.1007/s11042-013-1832-y

Steganographic method based on interpolation and LSB substitution of digital images

Ki-Hyun Jung · Kee-Young Yoo

Published online: 5 January 2014
© Springer Science+Business Media New York 2014

Abstract Steganography is the method of hiding secret data in other data, such as video or an image. A reversible data hiding method can extract the cover image from a stego-image without distortion after extracting the hidden data. In this paper a semi-reversible data hiding method that utilizes interpolation and the least significant substitution technique is proposed. First, interpolation methods are used to scale up and down the cover image before hiding secret data for a higher capacity and quality. Secondly, the LSB substitution method is used to embed secret data. Experimental results show that the proposed method can embed a large amount of secret data while keeping very high visual quality, where the PSNR is guaranteed to be 37.54 dB (k=3) and 43.94 dB (k=2).

Keywords Image security · Steganography · Data hiding · Reversible data hiding

1 Introduction

Multimedia data is easy to copy or destroy by unauthorized persons through the Internet. Therefore, it becomes important to be able to transmit data secretly. Steganography is the art and science of embedding secret data within other information without the existence of the hidden secret data. Recently, data hiding techniques have become important in a number of application areas. For example, many digital images, audio, and video now include distinguishing yet imperceptible marks that contain a hidden copyright notice or serial number to help prevent unauthorized copying [7, 15, 22]. There are both irreversible and reversible data hiding techniques, depending on what happens to the original image after recovering the data from the stego-image. Irreversible data hiding is called steganography or data hiding for short. The data hiding methods are classified in Fig. 1.

K.-H. Jung (✉)
School of Computer Information, Yeungjin College, 218 Bokhyun-Dong, Buk-Gu, Daegu 702-721, Republic of Korea
e-mail: kingjung@paran.com

K.-H. Jung
e-mail: hyunny.jung@gmail.com

K.-Y. Yoo
Department of Computer Engineering, Kyungpook National University, 1370 Sankyuk-Dong, Buk-Gu, Daegu 702-701, Republic of Korea
e-mail: yook@knu.ac.kr

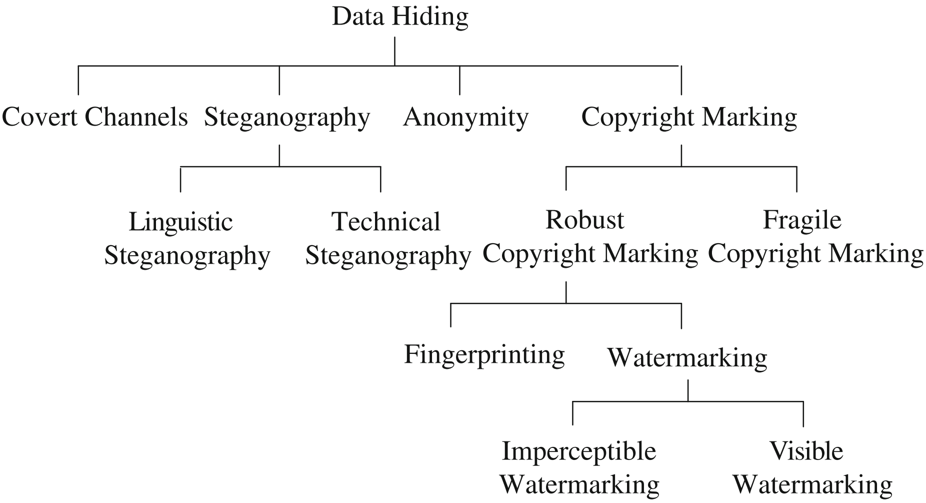


Fig. 1 Classification of data hiding methods

The well-known steganography methods are least significant bit (LSB) substitution and pixel-value differencing (PVD). LSB substitution replaces the least significant bit with a secret bit stream. LSB matching is either added or subtracted randomly from the pixel value of the cover data when the embedding bit does not match. The revised LSB matching was proposed to improve by lowering the number of modifications [13]. The PVD offers imperceptibility by calculating the difference of two consecutive non-overlapping pixels. Wu et al. took advantage of both the pixel-value differencing technique and the base decomposition scheme [20]. Lee et al.'s method embedded in a cover image using tri-way pixel-value differencing compressed by JPEG2000 on a secret image [11].

Reversible data hiding methods allow data to be embedded inside a digital media and later retrieved as required, leaving an exact original image. It is mainly used for content authentication of multimedia data due to the emerging demand for it in various fields, where the original host signal is crucial in order to make the right decision [1]. Reversible data hiding methods can be classified into three types: spatial domain, frequency domain, and compressed domain. Most spatial domain reversible data hiding methods are developed based on difference expansion (DE) and histogram modification. Vleeschouwer et al. and Goaljan et al.'s methods were reversible, but the embedded data was not large [5, 17]. Xuan et al.'s method was based on the integer wavelet transform to improve the embedding capacity [21]. However, the PSNR of the stego-image was low due to histogram modification before embedding. Celik et al. utilized a CALIC lossless image compression algorithm to create high capacity [2]. Ni et al. proposed a lossless data hiding method based on a histogram modification, where the zero or minimum points of the image histogram were utilized [14]. Wang et al. classified all pixels into wall and non-wall pixels to enhance image quality [18]. The interpolation prediction method and histogram shifting are used to embed secret data. Huang et al. proposed histogram shifting for image blocks testing on 16-bit blocks with medical images [6]. Recently, interpolation algorithms were used to improve capacity and image quality and recover a cover image. Jung and Yoo proposed neighbor mean interpolation to enhance embedding capacity and image quality [8]. Lee and Huang improved upon that technique by introducing interpolation by neighboring pixels [10]. Jung and Yoo utilized interpolation and edge detection algorithms in data hiding [9]. A semi-reversible data hiding is firstly introduced.

In this paper we utilize an interpolation method that scales up and down the quality of the cover image before hiding secret data. And then, the LSB substitution method is used for embedding larger amounts of secret data with good quality.

The rest of this paper is organized as follows. Section 2 reviews LSB substitution and image interpolation methods. In Section 3, the details of the proposed steganographic scheme are described. In Section 4, the experimental results are presented and discussed. Finally, the conclusions are presented in Section 5.

2 Background and preliminaries

In this section, we explain common LSB substitution and image interpolation methods. LSB substitution methods utilize the least bits of pixels in a cover image not to present distortion to the human eyes. Image interpolation methods are used to reconstruct a scaled image. It is a trade-off between the embedding capacity and the image quality.

LSB substitution hides the secret data in some bits of each pixel of the cover image. We describe a simple LSB substitution method as follows [3].

Suppose that the secret data are to be embedded into the *k*-rightmost LSBs of the cover image. We can first retrieve the rightmost *k*-bit LSB from each pixel of the cover image and rearrange the secret data to a *k*-bit by decomposing each pixel. Finally, the embedding process is completed by replacing the *k*-bit rightmost LSBs, and the stego-image is obtained by replacing *k*-bit with cover image and secret data as shown Fig. 2.

In the extraction process, we can directly extract secret data without any information about the cover image. The *k*-bit rightmost LSBs of each pixel are selected for the stego-image and lined up to reconstruct the secret data. The drawback of these methods related to LSB substitution is that the image quality of the stego-image becomes poor when the number of least significant bits is greater than or equal to four. To improve the image quality, the optimal LSB substitution [4], the approximately optimal LSB substitutions based on genetic algorithm [19], and the modulus LSB substitution [16] were proposed.

We utilize interpolation methods to maintain a good image quality at first. It becomes possible to recover the image before scaling exactly.

Image interpolation methods, such as the nearest neighbor, bilinear, B-spline, cubic, bicubic, Langrange and Gaussian have been used for re-sampling [12]. The nearest neighbor method can find the closest corresponding pixels of the cover image for each block and set them to a new pixel value for the destination image using neighboring pixels. The bilinear

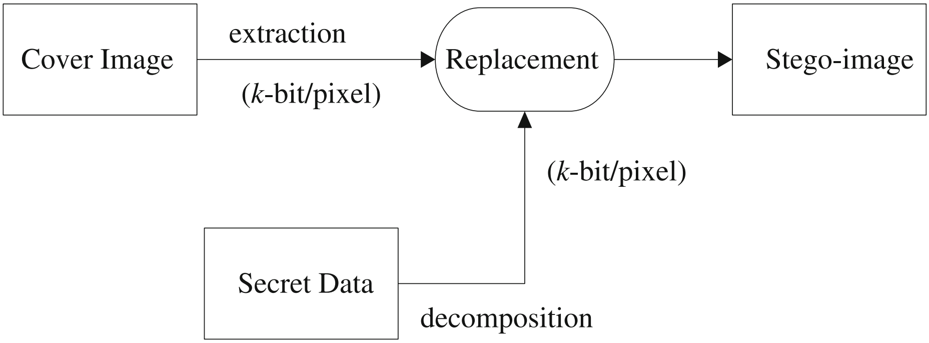


Fig. 2 The embedding process of LSB substitution

interpolation method determines the new value from the weighted average of the four closest pixels. These methods are used to change the size of images to estimate unknown values of pixels. Recently, the Interpolation by Neighboring Pixels (INP) method was proposed to increase the payload in data hiding [10]. The concept of INP is that pixels at near neighboring locations tend to have similar intensity values. It means that we can improve the image quality with less distortion. Suppose that a cover image has four pixels, as shown in Fig. 3. We can calculate the new pixels for up-scaling the image 2 times as follows.

$$\begin{aligned} x'_{10} &= (140 + (140 + 120)/2)/2 = 135 \\ x'_{01} &= (140 + (140 + 195)/2)/2 = 153 \\ x'_{11} &= (135 + 153)/2 = 144 \\ x'_{21} &= (120 + (120 + 188)/2)/2 = 137 \\ x'_{12} &= (195 + (195 + 188)/2)/2 = 193. \end{aligned} \tag{1}$$

For a cover image of four pixels (140, 120, 195, 188), new pixels (x'_{00}, x'_{20}, x'_{02}, x'_{23}) are retained. But new intermediate pixels (x'_{10}, x'_{01}, x'_{11}, x'_{12}) are calculated by Eq. (1).

There are also some previous works using interpolation methods to improve image quality and embedding capacity. We define a semi-reversible data hiding which is introduced by Jung and Yoo to analyze the proposed method [9].

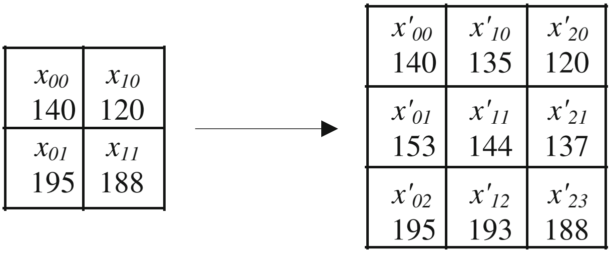
Definition 1 (Semi-reversible data hiding). For the cover image C with X x Y, it is called a semi-reversible data hiding if the cover image can be recovered with the scaled down size from the stego-image without extra information. It is defined as follows.

$$C' = C \times \frac{X \times Y}{x \times y}, \quad 0 < x < \mathrm{X}, 0 < y < \mathrm{Y}$$

The scale-down recovered image C' can be seen as whole image and must be difficult to find the distortion to the human eyes.

3 Proposed method

In this section, we propose a semi-reversible data method based on interpolation and least significant bit substitution. Let F_x and F_y be scaling factors for horizontal and vertical direction. The sequence of data hiding is ordered by zig-zag for F_x x F_y block, left-to-right and up-to-down direction. The left-upper pixel is reserved for each F_x x F_y block. Before secret



x_{00} 140	x_{10} 120
x_{01} 195	x_{11} 188

x'_{00} 140	x'_{10} 135	x'_{20} 120
x'_{01} 153	x'_{11} 144	x'_{21} 137
x'_{02} 195	x'_{12} 193	x'_{23} 188

Fig. 3 Example of the Interpolation by Neighboring Pixels method

data is embedded, the host image is partitioned into a size of F_x x F_y that satisfies non-overlapping and consecutive blocks by zig-zag scanning.

Let C be the cover image of W x H pixels and S be the n-bit secret data. For the pixel value of C, x and the secret bit of S, s is represented as Eqs. (2) and (3) respectively.

$$C = \left\{ x_{ij} \middle| 0 \leq i < W, 0 \leq j < H, x_{ij} \in \{0, 1, \ldots, 255\} \right\}. \tag{2}$$

$$S = \{ s_l | 0 \leq l < n, s_l \in \{0, 1\} \}. \tag{3}$$

The stego-image that results from embedding the secret data can be represented by Eq. (4).

$$C^r = C + \alpha \cdot S, \tag{4}$$

where α controls the embedding resistance. In order to resist other attacks, the embedding resistance can be regulated to be as high as possible. It can be used for any algorithm not only the proposed method, so we do not consider in the following equation to simplify. It is obvious that the higher the embedding capacity, the lower the quality of the stego-image will be.

Before embedding secret data, the target image that can embed secret data is generated by two preprocessing steps. First, the output image C^T that is obtained by preprocessing on the first step, C^T is calculated by Eq. (5).

$$C^T = F_x^{-1} \times F_y^{-1} \times C \tag{5}$$

For x_{ij} pixels belonging to the C image, the corresponding pixel $x^T{}_{ij}$ is calculated by

$$x^T{}_{ij} = \left\{ x_{i'j'} \middle| i' = i \middle/ F_x, j' = j \middle/ F_y \right\}. \tag{6}$$

Secondly, the C' image is obtained by Eq. (7), where the C' image is obtained by the scaling up method.

$$C' = F_x \times F_y \times C^T. \tag{7}$$

In details, a new pixel is decided by

$$x'_{ij} = (1-t)(1-u)x^T{}_{ij} + t(1-u)x^T{}_{(i+1)j} + (1-t)u\, x^T{}_{i(j+1)} + tu\, x^T{}_{(i+1)(j+1)}. \tag{8}$$

In here, $x^T{}_{(i+1)j}$ satisfies $x^T{}_{ij}<x'_{ij}<x^T{}_{i(j+1)}$ and t, u are given by

$$t = \frac{\left(x'_{ij}-x^T{}_{ij}\right)}{\left(x^T{}_{i(j+1)}-x^T{}_{ij}\right)}, \quad u = \frac{\left(x'_{ij}-x^T{}_{ij}\right)}{\left(x^T{}_{(i+1)j}-x^T{}_{ij}\right)}. \tag{9}$$

Next, secret data S is embedded into the generated image C'. Suppose that the secret data is to be embedded into the k-rightmost least significant bits of the cover image. For the stego-image C'', the secret data S is rearranged to form k-bit array S', which is represented as

$$S' = \left\{ s'_l | 0 \leq l < n, s'_l \in \left\{0, 1, \ldots, 2^k-1\right\} \right\}, \tag{10}$$

where s'_l can be defined as

$$s'_l = \sum_{j=0}^{k-1} S_{l \times k+j} \times 2^{k-1-j}. \tag{11}$$

The embedding process is completed by replacing the k-rightmost least significant bits of x'_{ij} by s'_l, which is calculated by Eq. (12).

$$x''_{ij} = x^T{}_j – x^T{}_{ij} \mod 2^k + s'_l. \tag{12}$$

The embedding procedure of the proposed method is summarized as follows.

The data embedding procedure:

Input: The cover image C with W x H pixels and the n-bit secret data S
Output: The stego-image C''

Step 1 Obtain the image C^T by Eq. (5) for F_x x F_y block
Step 2 The C' is obtained by Interpolation by scaling up method Eq. (8)
Step 3 The secret data S is rearranged as k-bit array S'
Step 4 Secret bits are embedded into the k-rightmost least significant bits of the image C'
Step 5 Repeat Step 4 until all secret bits are embedded.

In the extraction process, the embedded secret data can be directly extracted from the stego-image without referring the cover image. The k-rightmost least significant bits of the selected pixels are extracted by embedding sequentially and accumulated to reconstruct the secret data bits, which is calculate by Eq. (13).

$$s'_l = x''_{ij} \mod 2^k. \tag{13}$$

The extracting procedure of the proposed method is summarized as follows.

The data extracting procedure:

Input: The stego-image C'' and the parameters k, F_x, and F_y
Output: The secret data S with n-bit

Step 1 Obtain the stego-image C'' and parameters from the sender
Step 2 Secret bits are extracted the k-rightmost least significant bits of pixel
Step 3 Construct the secret bits in the zig-zag order
Step 4 Repeat Step 2 through Step 3 until all secret bits are extracted.

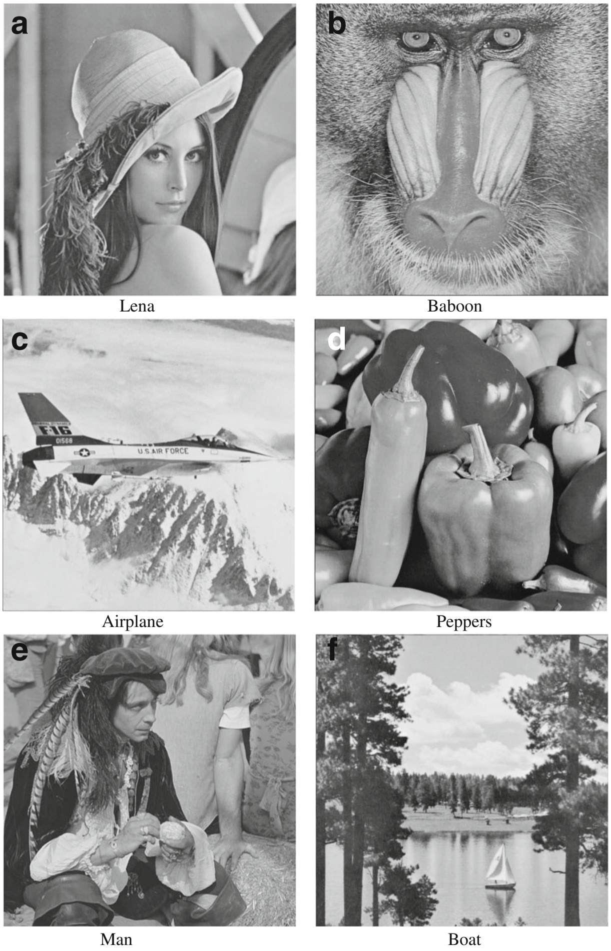
In addition, the cover image can be accumulated for the reserved pixel for each F_x x F_y block by sequence. It means that the proposed method can recover the cover image with the scaled down image. The proposed method can skip the step of Eq. (5) that is used to manipulate the cover image. Then the cover image can only be replaced according to an interpolation algorithm. We insert the step on Eq. (5) to emphasize that the difference cannot be determined whether or not applying interpolation method when the PSNR is sustained above 30 dB to the human visual system.

The recovering procedure of the cover image is summarized as follows.

The cover image recovery procedure:

Input: The stego-image C'' and the parameters F_x and F_y
Output: The cover image with $(W\times H)/(F_x\times F_y)$

Step 1 Obtain the stego-image C'' and parameters of sub-block
Step 2 Extract the reserved pixel of F_x x F_y sub-block
Step 3 Reconstruct the reserved pixel for each sub-block
Step 4 Repeat Step 2 through Step 3 until the cover image is extracted.



Lena

Baboon

Airplane

Peppers

Man

Boat

Fig. 4 Six cover images

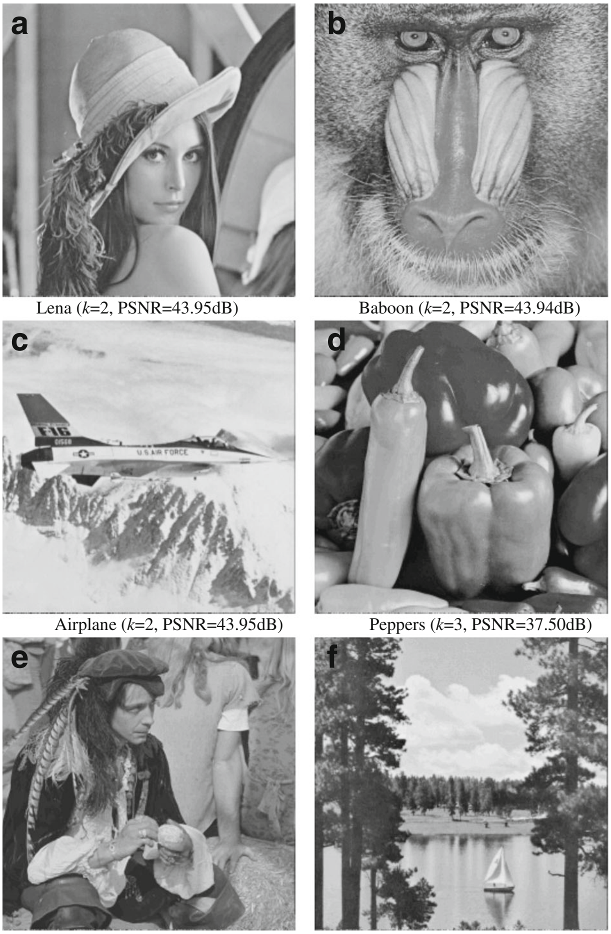
4 Experimental results

In this section we present and discuss the experimental results of the proposed method. The imperceptibility and capacity of the data hiding are contradictory. So, the best method is to take the human visual system into account to measure a data hiding method. In this paper, peak signal-to-noise ratio (PSNR) is used for the measurement of imperceptibility and capacity for the amount of embedded data.

In our experiments, an 8-bit grayscale image is used. So the PSNR is utilized as an objective distortion measurement and calculated as

$$PSNR = 10 \times \log_{10} 255^2 / MSE, \tag{14}$$

where *MSE* is the mean square error that is defined as



Lena (k=2, PSNR=43.95dB)

Baboon (k=2, PSNR=43.94dB)

Airplane (k=2, PSNR=43.95dB)

Peppers (k=3, PSNR=37.50dB)

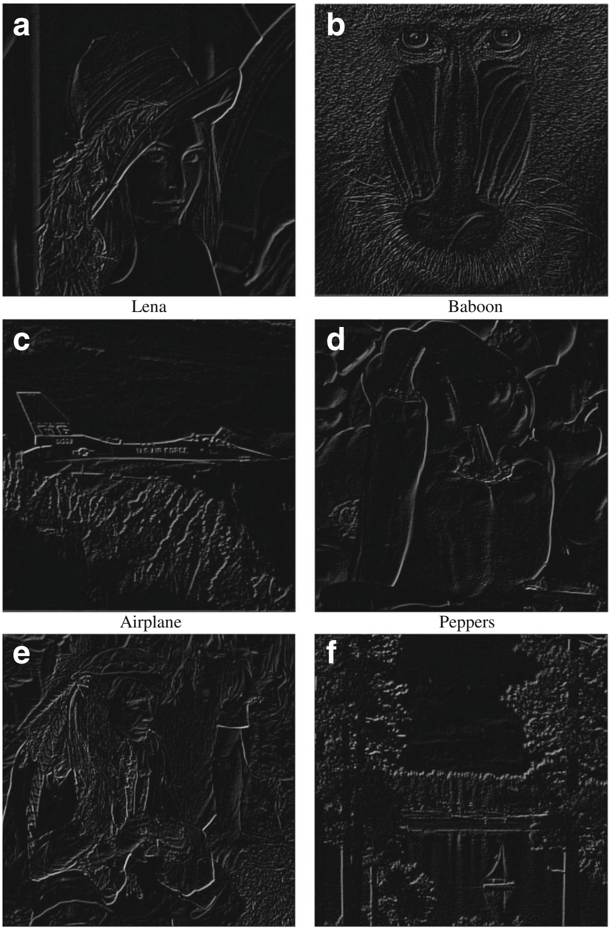
Man (k=3, PSNR=37.46dB)

Boat (k=3, PSNR=37.48dB)

Fig. 5 Six stego-images

Table 1 The results of the proposed method on capacity and PSNR

Cover Image	Proposed (k=2)		Proposed (k=3)	
	Capacity(bit)	PSNR(dB)	Capacity(bit)	PSNR(dB)
Lena	393,216	43.95	589,824	37.56
Baboon	393,216	43.94	589,824	37.54
Airplane	393,216	43.95	589,824	37.68
Peppers	393,216	43.93	589,824	37.50
Man	393,216	43.92	589,824	37.46
Boat	393,216	43.93	589,824	37.48



Lena

Baboon

Airplane

Peppers

Man

Boat

Fig. 6 Difference image between *C* and *C′* images (*k*=2)

$$MSE = \sum_{i=0}^{W-1}\sum_{j=0}^{H-1}\left(x^{T}{}_{ij} - x''{}_{ij}\right)^{2} / W \times H. \tag{15}$$

The images tested in our experiment are shown in Fig. 4, where the six 512×512 gray images are used as cover images. The secret data is generated randomly and sets the value to F_x=2 and F_y=2.

Figure 5 shows the stego-image after embedding the secret data. The average PSNR is 43.94 dB when *k*=2 and 37.54 dB when *k*=3. Since all of the PSNR is higher than 30 dB, it cannot be seen by the human visual system.

Table 1 shows the result of the proposed semi-reversible data hiding method when *k*-rightmost LSB substitution is used. Note that capacity represents amount of maximal capacity. Since the LSB substitution method is adopted, the capacity is the same and PSNR is almost the same for each cover image. Just only the difference of PSNR is 0.02 dB for *k*=2 and 0.12 dB for *k*=3 maximum when compared with 2-LSB and 3-LSB substitution.

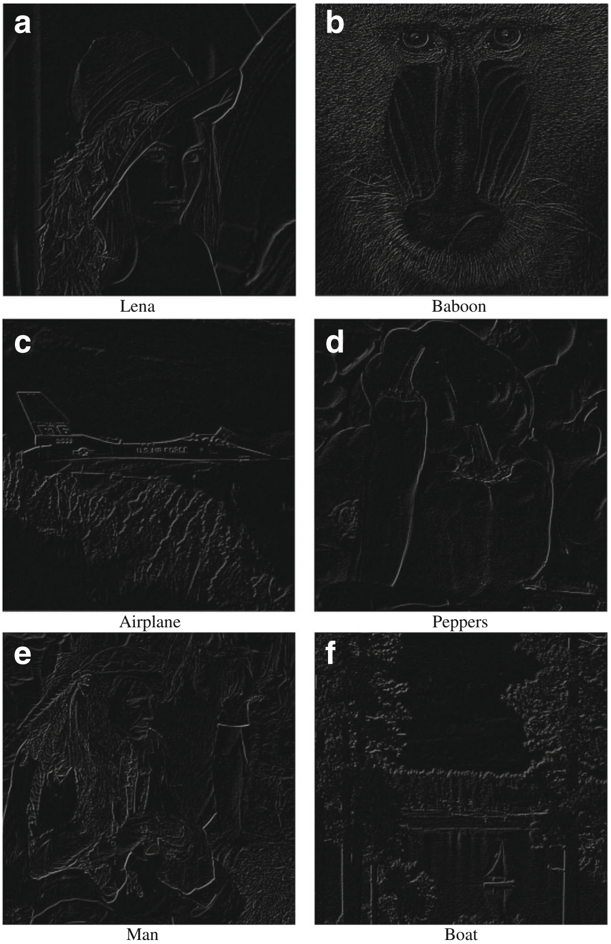


Fig. 7 Difference image between C and C″ images (k=2)

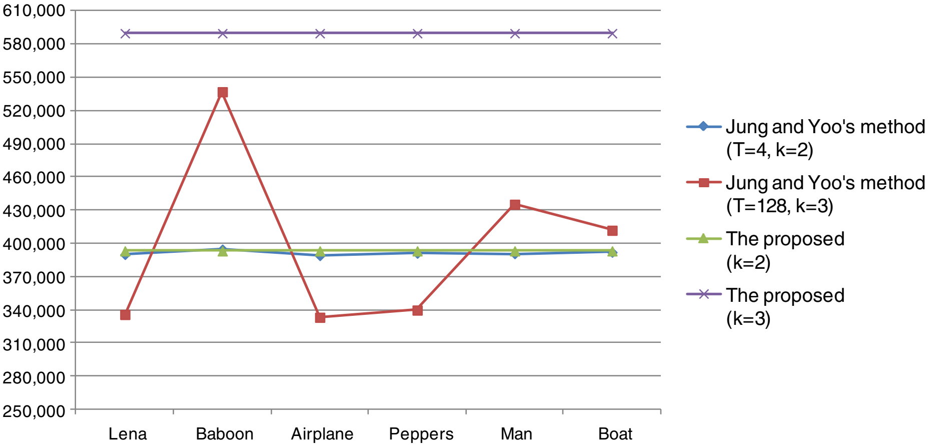


Fig. 8 Comparison of the embedding capacity (bits)

We demonstrate the capacity of the proposed method. Let B be the divided block size and E be embedding the pixel count in one block. The capacity of embedding bits A_k can be deduced by

$$A_k = \frac{W \times H}{B} \times \mathrm{E} \times k. \tag{15}$$

For example, in the case of k=2, A_2=(512×512)/4×3×2=393,216 bits is produced. And, A_3=(512×512)/4×3×3=589,824 bits for k=3. It means that the cover image can recover from the stego-image for the size of $(W \times H)/(F_x \times F_y)$.

Figures 6 and 7 show the difference image C with C′ and C″. The results demonstrate that all of the secret data is embedded on the edge areas. It means that it is difficult to detect the distortion of the interpolated image and stego-image.

Figure 8 demonstrates that the proposed method has a higher embedding capacity. The proposed method can 393,216 bits (k=2) and 589,824 bits (k=3) on average while the previous work could embed 391,280 bits (T=4, k=2) and 398,816 bits (T=128, k=3). It means that the proposed method can hide 1,936 bits and 191,008 bits more while keeping 43.9d dB and 37.54 dB on average for the parameter k because the parameter k decides the embedding capacity.

5 Conclusions

We have proposed the semi-reversible data hiding method based on interpolation and LSB substitution. The interpolation method has been preprocessed before hiding secret data for the purpose of higher capacity and good quality. Then, the LSB substitution method was applied for embedding secret data. The cover image with the scaled down size and secret data could be extracted from the stego-image without the need of any extra information. The experimental results showed that the average PSNR was 43.94 dB and the capacity was 393,216 bits when k=2. In the case of k=3, we demonstrated that the PSNR and capacity were 37.54 dB and 589,824 bits, respectively.

References

1. Awrangjeb M (2003) An overview of reversible data hiding. ICCIT 75–79
2. Celik MU, Sharman G, Tekalp AM & Saber E (2002) Reversible data hiding, Proceedings of IEEE 2002 International Conference on Image Processing 2, 157–160
3. Chan CK, Cheng LM (2004) Hiding data in images by simple LSB substitution. Pattern Recogn 37:469–474
4. Chang CC, Lin MH, Hu YC (2002) A fast and secure image hiding scheme based on LSB substitution. Int J Pattern Recog 16(4):399–416
5. Goljan M, Fredrich F & Du R (2001) Distortion-free data embedding, Proceedings of 4th Information Hiding Workshop, 27–41
6. Huang LC, Tseng LY, Hwang MS (2013) A reversible data hiding method by histogram shifting in high quality medical images. J Syst Software 86:716–727
7. Johnson NF & Jajodia S (1998) Exploring steganography: seeing the unseen. Comput Pract 26–34
8. Jung KH, Yoo KY (2009) Data hiding method using image interpolation. Comput Standards Interfaces 31: 465–470

9. Jung KH & Yoo KY (2013) Data hiding using edge detector for scalable images. Multimedia Tools and Appl doi:10.1007/s11042-012-1293-84
10. Lee CF, Huang YL (2012) An efficient image interpolation increasing payload in reversible data hiding. Expert Syst Appl 39:6712–6719
11. Lee YP, Lee JC, Chen WK, Chang KC, Su IJ, Chang CP (2012) High-payload image hiding with quality recovery using tri-way pixel-value differencing. Information Sciences 191:214–225
12. Lehmann TM, Gonner C, Spitzer K (1999) Survey: interpolation methods in medical image processing. IEEE Trans Med Imaging 18(11):1049–1075
13. Mielikainen J (2006) LSB matching revisited. IEEE Signal Processing Letters 13:285–287
14. Ni Z, Shi YQ, Ansari N, Su W (2006) Reversible data hiding. Circ Syst for Video Technol IEE 16:354–362
15. Swanson M, Kobayashi M, Tewfik A (1998) Multimedia data embedding and watermarking technologies. Proc IEEE 86(6):1064–1087
16. Thien CC, Lin JC (2003) A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recogn 36:2876–2881
17. Vleeschouwer C, Delaigle JF, Macq B (2001) Circular interpretation on histogram for reversible watermarking. IEEE IMSP Workshop 345–350
18. Wang XT, Chang CC, Nguyen TS, Li MC (2013) Reversible data hiding for high quality images exploiting interpolation and direction order mechanism. Digital Signal Process 23:569–577
19. Wang RZ, Lin CF, Lin JC (2001) Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recogn 34(3):671–683
20. Wu NI, Wu KC, Wang CM (2012) Exploring pixel-value differencing and base decomposition for low distortion data embedding. Appl Soft Comput 12:942–960
21. Xuan G, Zhu J, Chen J, Shi YQ, Ni Z, Su W (2002) Distortionless data hiding based on integer wavelet transform. IEE Electronics Letters 38:1646–1648
22. Zeng XT, Li Z, Ping LD (2012) Reversible data hiding scheme using reference pixel and multi-layer embedding. Int J Electron Commun 66:532–539

Ki-Hyun Jung received his B.S. degree in Computer Engineering from Kyungpook National University in 1995 and the M.S. degree in Computer Engineering from Kyungpook National University in 1997, South Korea. He had been employed as a senior researcher at Agency of Defense Development, South Korea. He received the Ph.D. degree in Computer Engineering from Kyungpook National University in 2007, South Korea. Currently, he is an Assistant Professor at the School of Computer Information, Yeungjin College, South Korea. He has selected his biography in the Marquis Who's Who in the world 2011. His current research interests are information hiding, watermarking, cryptography, network security, game & mobile programming, and virtual reality.

Kee-Young Yoo received his B.Sc. degree in Education of Mathematics from Kyungpook National University in 1976 and the M.Sc. degree in Computer Engineering from Korea Advanced Institute of Science and Technology in 1978, South Korea. He received the Ph.D. degree in Computer Science from Rensselaer Polytechnic Institute in 1992, New York, USA. Currently, he is a Professor at the Department of Computer Engineering, Kyungpook National University, South Korea. His current research interests are cryptography, authentication technologies, smart card security, network security, DRM security, and steganography. He has published over a hundred technical and scientific international journals on a variety of information security topics.