Journal of Imaging Science and Technology® 50(5): 424–426, 2006.

New Steganographic Method of Pixel Value Differencing

Hui-Chieh Lu and Yen-Ping Chu
Institute of Computer Science, National Chung Hsing University, 250 Kuo Kuang Road,
402 Taichung, Taiwan, Republic of China

Min-Shiang Hwang[†]
Department of Management Information System, National Chung Hsing University 250 Kuo Kuang Road,
402 Taichung, Taiwan, Republic of China
E-mail: mshwang@nchu.edu.tw

Abstract. *In this paper, we present a new steganographic method based on the pixel value differencing approach. The previous research of pixel value differencing can provide a better visual quality after embedding secret data than the well-known least-significant-bit (LSB) method but the embedding data capacity is much less than LSB method. We propose a new steganographic method by using pixel value differencing that hide secret data only in smooth areas, and this new method can provide much more hiding capacity than the previous research. The experimental results show the proposed method can hide much more data and keep a good visual quality of the stegoimage.* ***©*** *2006 Society for Imaging Science and Technology.* [DOI: 10.2352/J.ImagingSci.Technol.(2006)50:5(424)]

INTRODUCTION

The steganography technique hides information by embedding messages within other, seemingly harmless messages. In general, this technique can be applied to secret data sharing,[1–3] content protection, digital rights management,[4] etc. Some steganographic methods in the spatial domain have been proposed for embedding data in images.[5–11] Many data hiding techniques are based on the (LSB) least-significant-bit replacement method.[6,7,9,10] There are two drawbacks in LSB steganography. First, the LSB stegoimage can be detected easily by many steganoanalytic methods.[12–15] Second, the distortion of some LSB stegoimages can be perceptible by human vision. Therefore, Wu and Tsai proposed another scheme to hide data in the pixel value differencing variable between pixels. The data embedding capacity is adaptively decided by the pixel value contiguity of the near pixels. According to the principles of human vision, the change in edged areas of an image is not noticeable to an observer. The pixels in edged areas can embed more data than the smooth areas in the pixel value differencing method. Thus the average quality of stegoimages is much better than LSB steganography.[8] However, the embedding capacity of the secret data in Wu and Tsai's method is less than that in the LSB methods by very much. In average cases, its capacity is about a factor of two less than the LSB method.

In this paper, we propose a new scheme which can increase the hiding capacity against the method of Wu and Tsai[8] and it is also based on the pixel value differencing approach. Although the quality of stegoimage is somewhat poorer than in the method of Wu and Tsai,[8] it is still imperceptible.

EMBEDDING ALGORITHM

Here we use the 8-bit gray scale 512×512 image as a cover image in the proposed method. The following are the embedding steps.

1. Divide the cover image into nonoverlapping 2×2 blocks in a zigzag manner consecutively, and every block has four pixels, say p_{i1}, p_{i2}, p_{i3}, and p_{i4}, as shown in Fig. 1. We assume that these gray values are g_1, g_2, g_3, and g_4, respectively. Then d_{jk} represents $g_k - g_j$, where $j,k = 1,2,3,4$.

2. Build a pixel value differencing range table. In this step, we refer to the method of Wu and Tsai.[8] We consider the absolute values of d_{jk} (from 0 to 255) and then classify them into a number of contiguous ranges, which are R_i, where $i = 1,2,\ldots,n$. The lower and upper bound values of R_i are denoted as l_i and u_i, respectively, where l_1 is 0 and u_n is 255. The width of R_i is $u_i - l_i + 1$, and the width of each range is to be the power of 2. The selected range width of the table is used to adjust the length (bits) of data which need to be embedded between the two pixels, and it is computed as $\log_2(u_i - l_i + 1)$.

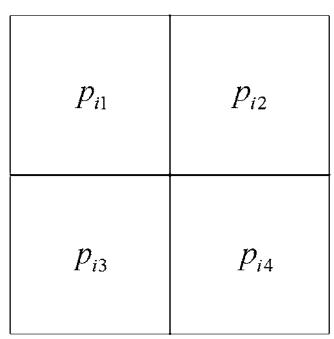

Figure 1. The nonoverlapping 2×2 block.

[†]Author to whom correspondence should be addressed.

Received Jan. 7, 2005; accepted for publication Mar. 9, 2006.
1062-3701/2006/50(5)/424/3/$20.00.

3. Partition every block into three pairs of pixels, and they are (p_{i1},p_{i2}), (p_{i2},p_{i4}), and (p_{i3},p_{i4}), respectively.

4. Embed data into (p_{i2},p_{i4}) first. We assume that the two pixels are p'_{i2} and p'_{i4} of the stegoimage with the new gray values g'_2 and g'_4 after embedding. The calculation of the new gray values is based on a function $f[(g_2,g_4),m]$ defined as follows:

$$f[(g_2,g_4),m] = (g'_2,g'_4) = \begin{cases} (g_2-\lceil m/2\rceil, g_4+\lfloor m/2\rfloor), & \text{if } d_{24} \text{ is odd;} \\ (g_2-\lfloor m/2\rfloor, g_4+\lceil m/2\rceil), & \text{if } d_{24} \text{ is even;} \end{cases} \tag{1}$$

where $m=d'_{24}-d_{24}$, and d'_{24} is denoted as

$$d'_{24} = \begin{cases} l_a+b, & \text{for } d \geqslant 0; \\ -(l_a+b), & \text{for } d \leqslant 0, \end{cases} \tag{2}$$

where a is the index of the differencing range table of the pair of (g_2,g_4), and b is the value of the embedding substream. In the above calculation, some pair of (g_2,g_4) may cause the resulting to fall off the boundaries of the range $[0,255]$. Before the embedding process, we must justify if the embedding pair is falling-off boundary. Here we must run a filter process in advance. Consider a pair of $(\hat{g}_2,\hat{g}_4)$ which is solved by Eq. (1), $f[(g_2,g_4),u_a-d_{24}]$. If one of the $(\hat{g}_2,\hat{g}_4)$ values out of the range $[0,255]$, we say the pair of (g_2,g_4) is falling-off boundary and this pair will not be embedded bit stream.

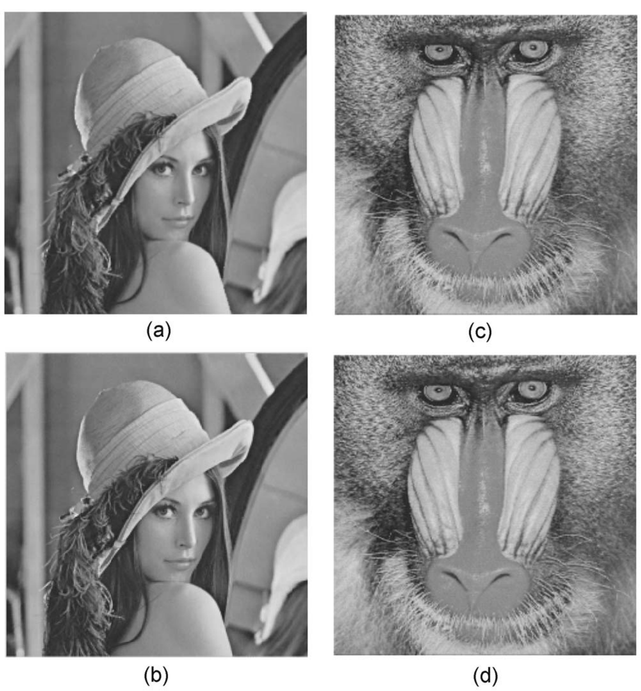

Figure 2. Resulting images: (a) Lena cover image; (b) Lena stegoimage, (c) baboon cover image, and (d) baboon stegoimage.

5. Embed data into (p_{i1},p_{i2}) and (p_{i3},p_{i4}). We assume that p'_{i1}, p'_{i2}, p'_{i3}, and p'_{i4} are the pixels of the stegoimage, and their gray values are g'_1, g'_2, g'_3, and g'_4 respectively. Because the gray values g'_2 and g'_4 have been embedded in some data bits in step 4, we do not change their values in this step. The calculation of the new gray values is based on a function $h[(g_j,g'_k),m]$, where $(j,k)=(1,2),(3,4)$ are defined as follows:

$$h((g_j,g'_k),d'_{jk}) = (g'_j,g'_k) = (g'_k-d'_{jk},g'_k), \tag{3}$$

where d'_{jk} is denoted as

$$d'_{jk} = \begin{cases} l_a+b, & \text{for } d \geqslant 0; \\ -(l_a+b), & \text{for } d < 0, \end{cases} \tag{4}$$

where a is the index of the differencing range table of the pair of (g_j,g_k), and b is the value of the embedding substream. Since this method may cause the edge area sharp, we set a threshold "T" in the proposed method. Before embedding data to the (p_{i1},p_{i2}) and (p_{i3},p_{i4}) pairs, we must filter some pixels in advance by the following rule:

If $(u_a > T)$ then
do not embed data bit(s) to this pair
else
embed data bit(s) to this pair

6. Repeat steps 3–5, until all secret data bits are embedded.

In step 5, we use a threshold T. It is the trade-off by tuning this value. The larger T is good for image quality but bad for capacity, and it is contrary when T is smaller. In our experiments, the image quality and capacity are good when T is 16.

RECOVERING ALGORITHM

To recover the embedded data, there is no need of the cover image but we need the original the pixel value differencing range table which is used in the embedding process. The following are the recovering steps.

1. Divide the stegoimage into nonoverlapping 2×2 blocks in a zigzag manner consecutively, and every block has four pixels, say p'_{i1}, p'_{i2}, p'_{i3}, and p'_{i4}. We assume that the gray values of them are g'_1, g'_2, g'_3, and g'_4, respectively.

2. Partition every block into three pair of pixels, and they are (p'_{i1},p'_{i2}), $(p'_{i2},p'_{i4}$, and (p'_{i3},p'_{i4}).

3. Recover data from (p'_{i2},p'_{i4}) first. Here we need to adjust if it is falling off boundary by calculating $(\hat{g}'_2,\hat{g}'_4)$ values in advance. If it is not falling off boundary, these two pixels indeed embedded the data bits. Now we can obtain the value of embedded data bits from these two pixels by calculating $(|g'_4-g'_2|-l_a)$, where a is the index of the differencing range table of the pair of (g'_2,g'_4). The total number of bits embedded can also be retrieved by the range table index, so the embedded data bits can be recovered.

4. Recover data from (p'_{i1},p'_{i2}) and (p'_{i3},p'_{i4}). First we must justify if (g'_1,g'_2) or (g'_3,g'_4) can be embedded data bits. We consider the condition of $(u_a > T)$, where a is the index of the differencing range table of the pair of (g'_j,g'_k) and $(j,k)=(1,2),(3,4)$. If embedded data bits are really present,

Table I. Experimental results.

Images (512×512)	Wu and Tsai's scheme (Ref. 8)		Our scheme	
	Capacity (bytes)	PSNR (dB)	Capacity (bytes)	PSNR (dB)
Lena	50801	41.79	70154	37.54
Baboon	56889	40.97	62208	31.82
Peppers	50769	41.73	70497	35.35
Jet	51242	37.90	70520	37.10

we can obtain their value by calculating $(|g'_j - g'_k| - l_a)$. The total number of bits embedded also can be retrieved by the range table index, so the embedded data bits can be recovered.

5. Repeat steps 2–4, until all secret data bits are recovered.

EXPERIMENTAL RESULTS

In our experiments, four images "Lena," "baboon," "peppers," and "jet" were used, and each comprised 512 $\times$512 pixels. The widths of ranges of gray values to be used in the experiments were 8, 8, 16, 32, 64, and 128. The two sets of cover and stegoimages are shown in Fig. 2.

Finally, the capacities of embedded data and the peaks of the signal-to-noise of the stegoimages were produced by the scheme of Wu and Tsai[8] and our scheme as shown in Table I. From the table the capacity is 1.5 times greater than their scheme and the image quality is only a little poorer than theirs. Furthermore, the computational complexity of our method is $O(n^2)$ which is equal to the scheme of Wu and Tsai.

CONCLUSION

We propose a new steganographic method for information hiding based on the pixel value differencing approach. The proposed method not only can provide a larger embedding capacity than Wu and Tsai's method but also has an acceptable stegoimage quality.

REFERENCES

1. R. Lukac and K. N. Plataniotis, "Bit-level based secret sharing for image encryption," Pattern Recogn. **38**, 767–772 (2005).
2. R. Lukac and K. N. Plataniotis, "Colour image secret sharing," Electron. Lett. **40**, 529–530 (2004).
3. C. C. Chang and J. C. Chuang, "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy," Pattern Recogn. Lett. **23**, 931–941 (2002).
4. E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. D. Delp, "Advances in digital video content protection," Proc. IEEE **93**, 171–183 (2005).
5. D. C. Lou and J. L. Liu, "Steganographic method for secure communications," Computers and Security **21**, 449–460 (2002).
6. M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," IEEE Trans. Image Process. **14**, 253–265 (2005).
7. S. Walton, "Image authentication for a slippery new age," Dr. Dobb's J. **20**, 18–26 (1995).
8. D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel value differencing," Pattern Recogn. Lett. **24**, 1613–1626 (2003).
9. C.-K. Chan and L.-M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recogn. **37**, 469–474 (2004).
10. C.-C. Chang, J.-Y. Hsiao, and C.-S. Chan, "Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy," Pattern Recogn. **36**, 1583–1595 (2003).
11. Y.-C. Tseng, Y.-Y. Chen, and H.-K. Pan, "A secure data hiding scheme for binary images," IEEE Trans. Commun. **50**, 1227–1231 (2002).
12. J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color and gray-scale images," IEEE Multimedia **8**, 22–28 (2001).
13. S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," IEEE Trans. Signal Process. **51**, 1995–2007 (2003).
14. X.-Y. Luo, B. Liu, and F.-L. Liu, "Detecting LSB steganography based on dynamic masks," *Proceedings of ISDA'05* (ISDA, Wroclaw, Poland, 2005) pp. 251–255.
15. T. Zhang and X.-J. Ping, "Reliable detection of LSB steganography based on the difference image histogram," IEEE International Conference on Acoustics, Speech, and Signal Processing (Hong Kong, 2003), Vol. III, pp. 545–548.