

<http://ansinet.com/itj>

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSI*net*

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

A Modified Histogram Shifting Based Reversible Data Hiding Scheme for High Quality Images

¹Wien Hong, ²Tung-Shou Chen, ¹Kai-Yung Lin and ¹Wen-Chin Chiang

¹Department of Information Management, Yu Da University, Miaoli, Taiwan

²National Taichung Institute of Technology,

Graduate School of Computer Science and Information Technology, Taichung, Taiwan

Abstract: The histogram-shifting method is a well-known method for reversible data hiding. To reach the goal of data hiding, this method shifts all pixel values between peak and zero points to leaves vacant spaces for data hiding. However, this method has no distortion-capacity control mechanism because the distortions are almost equally the same for large or small payload. In this study, we proposed a mechanism to control the image quality, for which small payload only needs to shift fewer pixels. Therefore, the proposed method produces better stego image quality and performs slightly efficient, especially for small payload. In comparison to the traditional histogram-shifting method, the proposed method significantly improves the stego image quality and computational cost without sacrificing the embedding capacity.

Key words: Reversible, data hiding, embedding capacity

INTRODUCTION

Data hiding is a technique that embeds secret data into digital media so that the existence of the embedded data is unnoticeable (Petitcolas *et al.*, 1999). Data hiding can be applied to protect copyrights, to authenticate digital contents and to communicate secretly (Lin and Tsai, 2004; Lin and Chen, 2000; Wu and Shih, 2006). In general, the digital media for which data are embedded are called carriers or cover media. Various media can be used for data hiding, for example, text files, audios, videos and images. Nowadays the most common carriers used for data hiding are digital images because they often spread over the Internet. Moreover, the rich redundancies provided by digital images are very suitable for data embedding because some redundancies can be easily replaced by the data bits. To conceal data into a cover image, pixel values are modified. The modified image with data embedded is called a stego image. In general, pixel values of cover images are changed so that data can be concealed; therefore, image distortion occurs. Usually, the distortion due to data hiding is not reversible. This means the original image cannot be recovered to its original state, even after the hidden data is extracted (Mielikainen, 2006). On the contrary, a reversible data hiding technique has the capability to restore the original image (Celik *et al.*, 2005; Hong *et al.*, 2008, 2009). Some times, it is very important to have the original image. For

example, a misreading of an x-ray picture may cause misdiagnosis of a patient.

Techniques used in reversible data hiding can roughly be categorized into two types; namely, the difference-expansion technique proposed by Tian (2003) and the histogram-shifting technique proposed by Ni *et al.* (2006). In Tian's (2003) studies, the differences of pixel pairs are expanded and message bits are embedded in the LSBs of the expanded values. In Tian's (2003) study, one data bit can be concealed into two pixels; therefore, the maximum bit-rate is 0.5 bpp. However, a relatively large amount of distortion could be introduced due to the pixel difference is doubled. Therefore, his method work is not suitable for applications where high image quality is demanded. Several variants of Tian's work can be seen in Alattar (2004), Thodi and Rodriguez (2007). In Ni *et al.* (2006) study, data bits are embedded by shifting the histogram bins. During embedding, pixel values are plus or minus one at most; therefore, a high stego image quality could be achieved. However, the payload is restricted by the distribution of pixel values. In general, as an image histogram has a greater peak height, the image should have a greater payload.

The histogram-shifting technique, proposed by Ni *et al.* (2006) embeds data by shifting the histogram bins. This method first constructs an image histogram of a cover image to obtain a pair of peak and zero points. Then, data are embedded by shifting the histogram bins.

Due to its simplicity, it has become one of the best popular techniques in the field of reversible data hiding. The detailed embedding procedures are listed below:

- **Input:** Original 8-bit grayscale image I with $M \times N$ pixels and the secret data S
- **Output:** Stego image I_s , the peak point a , the minimum point b , length of secret data $|S|$ and the location map L
- **Step 1:** Scan the cover image I and constructed its histogram $H_i(x)$, $x \in [0, 225]$. In the histogram, the gray value for which the histogram is highest is denoted the peak point a and the gray value for which the histogram is lowest is denoted the minimum point b . If $H_i(b) = 0$, then b is called a zero point. For simplicity, we assume $a < b$
- **Step 2:** Scan the image again and record the positions of those pixel value equal to b and place them into location map L . After that, shift the histogram $H_i(x)$, $x \in (a, b)$ to the right by 1 unit to vacate the histogram bin at $a+1$
- **Step 3:** Extract a data bit s from secret data S . Scan the image once more. If the scanned pixel value is a and the data bit to be embedded is 1, then set the pixel value to $a+1$. If the data bit to be embedded is 0, no change has to be done on the scanned pixel

Data embedding can be done by repeating step 3 until S is completely embedded. The outputs of Ni *et al.* (2006) study are a stego image I_s , a peak point a , a minimum point b , the location map L and the length of the secret data $|S|$. These outputs are then served as a key and transmitted to the receiver via a secret channel. When receivers have both key and the stego image I_s , they can use the following procedures to find the secret data and the original image. The procedures of data extraction and original image recovery are given below:

- **Input:** Stego image I_s , the peak point a , the minimum point b , the location map L and the length of the secret data $|S|$
- **Output:** Original 8-bit grayscale image I and the secret data S
- **Step 1:** Scanned the image in the same order as in the embedding phase. If the scanned value is a , then a bit 0 is extracted. If the scanned value is $a+1$, then a bit 1 is extracted
- **Step 2:** Scan the image again and shift $H_i(x)$, $x \in (a, b)$ to the left by one unit
- **Step 3:** Set the value of those pixels recorded in L to b

The embedding and extraction procedures use one pair of peak and minimum point to perform data hiding. However, Ni *et al.* (2006) method can be generalized to two pairs of peak and zero. Note that in the embedding phase, the cover image is scanned three times; therefore, the computational cost of Ni *et al.* (2006) method is $O(3M \times N)$.

PROPOSED METHOD

Although, a higher stego image quality can be obtained in Ni *et al.* (2006) method, it has no mechanism to control the capacity-distortion relationship; namely, equally distortion will occurs for large or small payload. This is because almost equally amount of pixels has to be shifted in order to conceal data, no matter the size of the payload.

Embedding: Here, we proposed a modified version of Ni *et al.* (2006) method to solve the major drawback of their scheme. Instead of shifting all the pixels between the peak and minimum point before embedding, we combine the shifting and embedding processes together so that just amount of pixels is shifted for a given payload. Therefore, no extra amount of pixels will be shifted compare to Ni *et al.* (2006) method. The detailed embedding procedure is given below:

- **Input:** Original 8-bit grayscale image I with $M \times N$ pixels and the secret data S
- **Output:** Stego image I_s , the peak point a , the minimum point b , length of secret data $|S|$ and the location map L
- **Step 1:** Scan the cover image I and constructed its histogram $H_i(x)$, $x \in [0, 255]$. In the histogram, obtain the peak point a and the minimum point b . Without loss the generality, we assume $a < b$
- **Step 2:** Set $k = 0$. The variable k is used to indicate the amount of embedded data bits
- **Step 3:** Scan the cover image I again. If the scanned pixel value is equal to a , a data bit s is extracted from S , set $k = k+1$ and go to step 4 to embed the data bit s ; otherwise, go to step 5
- **Step 4:** If the data bit s is 1, then the value of scanned pixel is set to $a+1$; otherwise no change has to be made for this pixel. Go to step 3 to continue the embedding processes
- **Step 5:** If the scanned pixel value is within the range (a, b) , then the pixel value is add by one. Record the position of pixels whose pixel values is equal to b

Extraction and restoration: The extraction and restoration procedures are similar to that of Ni *et al.* (2006) scheme. The detailed procedure is listed below:

- **Input:** Stego image I_s , the peak point a , the minimum point b , the location map L and the length of the secret data $|S|$
- **Output:** Original 8-bit grayscale image I and the secret data S
- **Step 1:** Set $k = 0$
- **Step 2:** Scanned the image in the same order as in the embedding phase. If the scanned value is a , let $k = k+1$ and a bit 0 is extracted. If the scanned value is $a+1$, let $k = a+1$ and a bit 1 is extracted. If the scanned value is within the range (a,b) then subtract one from the scanned pixel values. If the position of the scanned pixel is recorded in L , then the value of scanned pixel is set to b
- **Step 3:** Repeat step 2 until $k = |S|$

The proposed method has combined both pixel-shifting and data-embedding in a single loop. By doing this, no extra work is required on processing small amount of payload. Therefore, a better quality for stego image and lower computational cost could be achieved.

RESULTS AND DISCUSSION

Here, we compare Ni *et al.* (2006) method to ours to demonstrate the applicability and effectiveness of the

proposed method. Six 8-bit grayscale images, Lena, Baboon, Boat, Girl, Sailboat and Peppers sized 512×512 , are selected as test images, as shown in Fig. 1a-f. The secret data is generated by a Pseudo Random Number Generator (PRNG). We use Peak Signal-to-Noise Ratio (PSNR) for evaluating the quality of stego image. The definition of PSNR is given by:

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE}$$

where, MSE is the mean square error between the original image and the stego image. The definition of MSE is given by:

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (x_{i,j} - x'_{i,j})^2$$

where, $x_{i,j}$ and $x'_{i,j}$ are the pixel values of the original image and the stego image, respectively. A higher PSNR value means that the quality of stego image is closer to the original image.

In Ni *et al.* (2006) histogram-shifting method, when two pairs of peak and minimum points are used to embed data, all pixels are plus or minus one grayscale unit at most, resulting the MSE between the original image and the stego image is close to 1. Therefore, the lower bound of PSNR is given by:

$$PSNR \geq 10 \times \log_{10} 225^2 = 48.13 \text{ db}$$



Fig. 1: Six 8-bit grayscale image as test image. (a) Lena, (b) baboon, (c) boat, (d) girl, (e) sailboat and (f) peppers

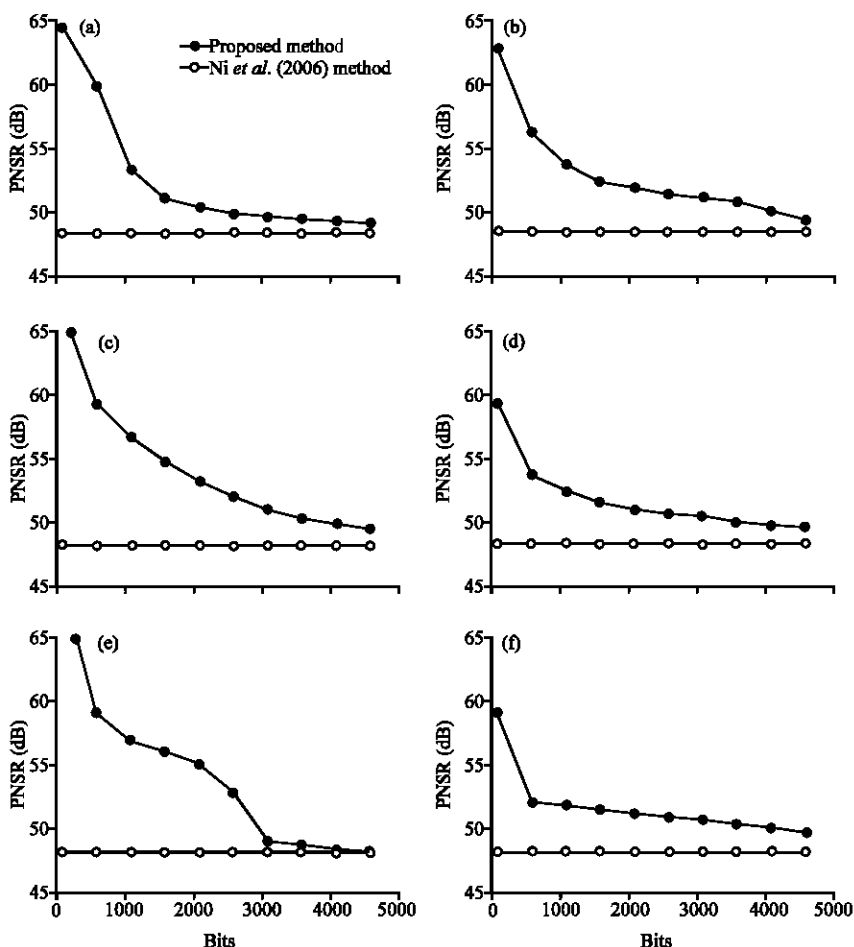


Fig. 2: Comparison for the PSNR-payload between Ni *et al.* (2006) method and the proposed method. (a) Lena, (b) baboon, (c) boat, (d) girl, (e) sailboat and (f) peppers

The maximum payload of Ni *et al.* (2006) method is determined by the most frequent pixel values occur in a cover image. To demonstrate the undesirable pixel shifting in Ni *et al.* (2006) method, we define the embedding rate as follows:

$$E_R = \frac{\text{No. of embedded bits}}{\text{Maximum payload}}$$

Therefore, a $E_R = 0.5$ indicates that there are 50% of embeddable space has been embedded with data bits. Table 1 shows a comparison between the numbers shifted pixels under various embedding rate for the proposed method and Ni *et al.* (2006) method. Note that the more the number of shifted pixels, the lower the stego image quality is. As can be seen from Table 1, the number of shifted pixels is roughly the same as in Ni *et al.* (2006) method, regardless the embedding rates. However, the proposed method significantly reduces the number of

Table 1: Number of shifted pixels under different embedding rates

Test image	Ni <i>et al.</i> (2006) method			Proposed method		
	$E_R = 0.2$	$E_R = 0.5$	$E_R = 1.0$	$E_R = 0.2$	$E_R = 0.5$	$E_R = 1.0$
Lena	187,195	187,774	188,689	96,848	143,255	188,530
Baboon	102,708	103,164	103,910	34,089	51,694	103,865
Boat	145,322	146,723	148,201	22,451	63,444	148,155
Girl	209,359	209,949	210,877	107,529	154,162	210,779
Sailboat	39,863	40,505	41,578	3,062	9,806	41,543
Peppers	93,713	94,163	94,826	43,920	54,553	94,590

shifted pixels at low embedding rate and therefore, a higher stego image quality can be obtained.

Figure 2a-f show the comparison results of stego image quality vs. payload for the proposed method and Ni *et al.* (2006) method. These figures show that with fewer payloads, the proposed method significantly improves the stego image quality over Ni *et al.* (2006) method. When the payloads approach the maximum embedding capacity, the PSNR of the proposed method is close to the theoretical value, 48.13 dB. Moreover, since

the number of shifted pixels is significantly reduced under low embedding rate, the proposed method provides stronger security against statistical analysis than Ni *et al.* (2006) method. Besides, although the PSNR at maximum embedding capacity of the proposed method is roughly the same as that of Ni *et al.* (2006) method, our method still have a better computation efficiency. In Ni *et al.* (2006) study, the time complexity is $O(3M \times N)$ whereas ours is $O(2M \times N)$. This is because our method combines data-embedding and pixel-shifting in a single loop; however, Ni *et al.* (2006) method has to evacuate a histogram bin in advance and data embedding can then be performed. Therefore, the whole cover image needs an extra scan in Ni *et al.* (2006) study, resulting a slightly degrade in the embedding performance.

The purpose of data hiding is to transmit secret information under the cover of digital media to elude the attention of someone who is interested in it (Hong *et al.*, 2009). Generally, a data hiding method should have the capability of distortion-capacity control mechanism, i.e., smaller payload only distort the cover image smaller (Thodi and Rodriguez, 2007). The proposed method meets this requirement. On the contrary, the undesirable distortion may occur in Ni *et al.* (2006) method. Besides, a good data hiding method should distort the cover image as small as possible to prevent the embedment detectable (Zhang and Wang, 2006). In the proposed method, we reduce the embedding distortion significantly at small payload. Thus, the proposed method supports the essential requirement of data hiding and provides a more secure and flexible data hiding method than that of Ni *et al.* (2006) method.

CONCLUSION

In this study, we proposed a modified reversible data hiding method based on Ni *et al.* (2006) histogram-shifting method. A distortion control mechanism is introduced in the proposed method to significantly reduce the number of modified pixels, because just amount of pixels is shifted for a given payload. Besides, the proposed method slightly improves the computational cost due to the evacuation of histogram bin is no longer necessary. The experimental results show that the proposed method

has better PSNR than that of Ni *et al.* (2006) method, especially for low embedding rate.

REFERENCES

- Alattar, A.M., 2004. Reversible watermark using the difference expansion of a generalized integer transform. *IEEE Trans. Image Process.*, 13: 1147-1156.
- Celik, M.U., G. Sharma, A.M. Tekalp and E. Saber, 2005. Lossless generalized-LSB data embedding. *IEEE Trans. Image Process.*, 14: 253-266.
- Hong, W., T.S. Chen and C.W. Shiu, 2008. Lossless steganography for AMBTC-compressed images. *Int. Congress Image Signal Process.*, 2: 13-17.
- Hong, W., T.S. Chen and C.W. Shiu, 2009. Reversible data hiding for high quality images using modification of prediction errors. *The J. Syst. Software* (In Press). 10.1016/j.jss.2009.05.051
- Lin, S.D. and C.F. Chen, 2000. A robust DCT-based watermarking for copyright protection. *Consumer Electron IEEE Trans.*, 46: 415-421.
- Lin, C.C. and W.H. Tsai, 2004. Secret image sharing with steganography and authentication. *J. Syst. Software*, 73: 405-414.
- Mielikainen, J., 2006. LSB matching revisited. *IEEE Signal Process. Lett.*, 13: 285-287.
- Ni, Z., Y.Q. Shi, N. Ansari and W. Su, 2006. Reversible data hiding. *IEEE Trans. Circ. Syst. Video Technol.*, 16: 354-362.
- Petitcolas, F.A.P., R.J. Anderson and M.G. Kuhn, 1999. Information hiding-a survey. *Proc. IEEE*, 87: 1062-1078.
- Thodi, D.M. and J.J. Rodriguez, 2007. Expansion embedding techniques for reversible watermarking. *IEEE Trans. Image Process.*, 16: 721-730.
- Tian, J., 2003. Reversible data embedding using a difference expansion. *IEEE Trans. Circ. Syst. Video Technol.*, 13: 890-896.
- Wu, Y.T. and F.Y. Shih, 2006. Genetic algorithm based methodology for breaking the steganalytic system. *IEEE Trans. Syst. Man Cybernet*, 36: 24-31.
- Zhang, X. and S. Wang, 2006. Efficient steganographic embedding by exploiting modification direction. *IEEE Commun. Lett.*, 10: 781-783.