Data Hiding Scheme using Covering Codes in Halftone Images Based on Error Diffusion

Ruey-Ming Chao
Institute of Information & Social Science
National United University
Miaoli, Taiwan, R.O.C.
rueyming@nuu.edu.tw

Yu-An Ho
Department of Computer Science & Engineering
Chung Hsing University
Taichung, Taiwan, R.O.C.
yaho@cs.nchu.edu.tw

Yen-Ping Chu
Department of Computer Science & Information Engineer
Tunghai University
Taichung, Taiwan, R.O.C.
ypchu@ nchu.edu.tw

Abstract

This paper proposes a new data hiding scheme based on covering code in process of producing halftone images. The scheme is mainly to do error diffusion in gray-level images beforehand, and produce the fixed length sequence of the halftoning binary code according to the rule of covering code. Then, after embedding secret data in the binary code, the gray-level images renew to do the error diffusion by the new binary code. While all pixels of gray-level image have been processed, not only can achieve to render gray-level images to halftone images, but can embed secret data into halftone images. The experimental results prove the quality of stego-halftone image of our scheme better than the scheme that the secret data directly embed to halftone images using covering code. Moreover, the average of PSNR in our proposed scheme only degrades 4.77 dB between the stego-halftone image and original halftone image, and data hiding capacity can hold 42%.

1. Introduction

Digital halftoning [1] is a bi-level image which renders multi-tone images into two-tone images. There are a lot of halftone techniques that have been proposed, such as ordered dithering [2], error diffusion [3-4] and dot diffusion [5-6], among which error diffusion techniques have low computational complexity and can produce better visual quality for halftone images.

In recent years, data hiding techniques [7] have been playing a very important role in information transmission security and data authentication. Generally, data hiding works by delivering an encrypted secret message hidden in the cover image to be stego-image. Then, the sender sends the stego-image to the receiver via the Internet or other transmission media. The receiver receives the stego-image and extracts the secret message by using the corresponding decrypting method. Such secret data can be authentication data of the cover images or the important data. So far, quite a number of data hiding techniques [8-10] have been proposed, but unfortunately those methods are suitable for gray images only.

In comparison with gray images, halftone images have much less bit planes where secret data can be hidden. So far, some data hiding schemes have been proposed in halftone image. Fu et al. presented two methods in [11]. The first method is called data hiding self toggling (DHST), hides "0" (white) and "1" (black) bits in halftone images according to their pseudo random locations. The second method is called data hiding pair toggling (DHPT). It randomly picks out one among the neighbor pixels around the hiding place of secret data and checks out the pixel value. In addition, they introduced another scheme by the name of the data hiding smart pair toggling (DHSPT) scheme [12]. Then, they decided to take in both intensity selection (IS) and connection selection (CS) so as to refine the hiding techniques of DHST, DHPT and DHSPT and to acquire better visual quality [13]. Besides, in [14], they offered a data hiding error diffusion (DHED) scheme that can hide data in the error diffusion process where the halftone image is produced. Pei et al. have also proposed a hybrid method was proposed in [15]. This method combines noise-balanced error diffusion (NBEDF) with kernels-alternated error diffusion (KAEDF) and embeds the watermark into one or several error-diffused images. Then, they proposed another data hiding method by the name of the noise-balanced error diffusion technique (NBEDF) in [16] that does the job in the process of transforming an original gray-level image into a halftone image. In addition, to embed a watermark in a

978-0-7695-3473-2/08 $25.00 © 2008 IEEE
DOI 10.1109/APSCC.2008.154

dithered halftone image, a robust watermarking method, the paired sub-image matching ordered dithering (PSMOD) technique, was proposed in [17]. Recently, a high-capacity data hiding method for halftone images has been proposed in [19]. This method can hide one halftone image in several halftone images and keep high visual quality.

In this paper, we propose a new data hiding technique for halftone images. Our new method uses covering code to embed secret data in process of rendering gray-level images to halftone image. The rest of this paper is organized as follows. The data hiding procedure of the proposed method presents in Section 2. The experimental results are shown in Section 3. Finally, the conclusion will be presented in Section 4.

2. The proposed data hiding technique

In this section, we shall present the proposed data hiding method for halftone images. Our new method uses covering code to embed secret data in process of rendering gray-level images to halftone image. Finally, we will see how in the proposed scheme we can extract the secret data in the proposed scheme.

2.1. Covering codes

Covering codes [19-20] take a binary stream to transfer another unique binary stream using the parity check matrix. Let $x=[x_1,x_2,...,x_n]$ is a binary stream, and decide the covering radius ρ and a parity check matrix ***H***. The ***H*** can express a $COV(\rho,n,k)$ [19], on the other hand, it can take *k* bits data $s=[s_1,s_2,...,s_k]$ embed into *n* bits matrix $x=[x_1,x_2,...,x_n]$, and only modify matrix with the most ρ bits. The transferred manner [20] is as Equation (1):

$$[s_1,s_2,...,s_k]^T=\boldsymbol{H}\cdot[x_1,x_2,...,x_n]^T \quad (1)$$

Hamming code is a universal adopting the parity check matrix, and can satisfy $COV(1,7,3)$. The party check matrix of hamming code as the following Equation (2):

$$\boldsymbol{H}=\begin{bmatrix}1&0&0&1&1&0&1\\0&1&0&1&0&1&1\\0&0&1&0&1&1&1\end{bmatrix} \quad (2)$$

Let $x=[x_1,x_2,...,x_7]$, according to Equation (2) can get $[s_1,s_2,s_3]$.

$$\begin{cases}s_1=x_1\oplus x_4\oplus x_5\oplus x_7\\s_2=x_2\oplus x_4\oplus x_6\oplus x_7\\s_3=x_3\oplus x_5\oplus x_6\oplus x_7\end{cases} \quad (3)$$

For example, assume there is a binary stream $x=[1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0]$ which can get another binary stream $s'=[1\ \ 1\ \ 0]$ by Equation (3). If the secret data s equates s', then we do not modify x's bits. Otherwise, if the secret data s unequaled s', then compute $s'\oplus s$ and refer to ***H***, we can get to modify which one bits satisfied $s=s'$. For instance, while $s=[1\ \ 0\ \ 1]$ and we compute $[1\ \ 1\ \ 0]\oplus[1\ \ 0\ \ 1]=[0\ \ 1\ \ 1]$. Therefore, we can embed s into x only modify x_6 enabled $x=[1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0]$.

2.2. Error diffusion

In the transform techniques of the halftone image, error diffusion [3-4] provides good visual quality and uses the low complex operation. Suppose the size of gray-level images are $H\times W$ and the pixel of gray-level images is $x_{j,i}$, where $j\in 1,2,...,H$ and $i\in 1,2,...,W$ are the coordinates of images pixel $x_{j,i}$. By scanning the $x_{j,i}$ of the image from top to button and from left to right and adding the error value $e'_{j,i}$, $x_{j,i}$ becomes $x'_{j,i}$ (see Equation (4)). The $e'_{j,i}$ is the result that the $e_{j,i}$ operate the error diffusion by kernel *k*. The $e_{j,i}$ is the difference between the prior gray-level value transform into binary value by threshold and the prior gray-level value. The error diffusion kernel *k* adopts Jarvis' error diffusion kernel [3] and is shown in Figure 1. Equation (4-6) explains how the computation can be done.

$$x'_{j,i}=x_{j,i}+e'_{j,i} \quad (4)$$

$$\frac{1}{48}\times\begin{bmatrix}&&\bullet&7&5\\3&5&7&5&3\\1&3&5&3&1\end{bmatrix}$$

Figure 1. The Jarvis' error diffusion kernel

$$e'_{j,i} = e_{j,i} \otimes k$$
(5)

Here $\otimes$ stands for the error diffusion operation.

Then, if $x'_{j,i}$ is smaller than the threshold value, this output pixel should be a black pixel; otherwise, if $x'_{j,i}$ is greater than or equal to the threshold value, this output pixel should be a white pixel (see Equation (3)).

$$b_{j,i} = \begin{cases} 0, & \text{if } x'_{j,i} < \text{Threshold} \\ 1, & \text{if } x'_{j,i} \geq \text{Threshold} \end{cases}$$
(6)

Here b is the halftone image composed of white and black pixel.

Then, each pixel $b_{j,i}$ may be adjusted to white "1" or black "0", and the error value $e_{j,i}$ can be subtracting $b_{j,i}$ from $x'_{j,i}$ and figured out by Equation (4). Then, the error value $e_{j,i}$ obtained by Equation (2) can be compensated by the neighboring gray-level pixels according to the kernel k.

$$e_{j,i} = x'_{j,i} - b_{j,i} \tag{7}$$

Finally, a halftone image can be outputted when all $x_{j,i}$ have been processed.

2.3. Proposed method

In this paragraph, we introduce the covering codes scheme based on error diffusion. Here, the hamming code hiding of $COV(1,7,3)$ is used in proposed scheme. As a result, the secret data transform into binary stream, and combine three bits into a set, expressed by s. Assume there is a $H \times W$ image I and backup a unique duplicate image I'. The proposed scheme processes seven times error diffusion in I' beforehand, which can get a binary stream $b_{j,i}, b_{j,i+1}, ..., b_{j,i+7}$. The $b_{j,i}, b_{j,i+1}, ..., b_{j,i+7}$ can compute a binary stream s' according to Equation (3).

Due to the secret data is s, and the s equates s', then we do not modify $b_{j,i}, b_{j,i+1}, ..., b_{j,i+7}$. Otherwise, if the secret data s unequaled s', then compute $s' \oplus s$ and refer to $\boldsymbol{H}$, we can get to modify which one bits satisfied $s = s'$. After modifiying $b_{j,i}, b_{j,i+1}, ..., b_{j,i+7}$, it can result in a new stream $b'_{j,i}, b'_{j,i+1}, ..., b'_{j,i+7}$, and the most one bit is different among the two streams. According to $b'_{j,i}, b'_{j,i+1}, ..., b'_{j,i+7}$, we do the error diffusion in I and produce a new image I. Then, we backup a unique duplicate I' using the new image I, and process next seven pixels in I', until all pixels is done in I. Finally, the output b' is the stego-halftone image including secret data, and the whole stages are as algorithm ***CC_ED***.

***Algorithm CC_ED*( )**
for (j=1 to H)
  for each $x_{j,i}, x_{j,i+1}, ..., x_{j,i+7}$
    $I' = I$
    Get the three bits of the secret data expressed by s.
    Do seven times the error diffusion in I'.
    Product $b_{j,i}, b_{j,i+1}, ..., b_{j,i+7}$.
    $[s'_1, s'_2, s'_3]^T = \boldsymbol{H} \cdot [b_{j,i}, b_{j,i+1}, ..., b_{j,i+7}]^T$.
    if $s' = s$
      $b'_{j,i}, b'_{j,i+1}, ..., b'_{j,i+7} = b_{j,i}, b_{j,i+1}, ..., b_{j,i+7}$.
    Else
      Modified the most one bits in $b_{j,i}, b_{j,i+1}, ..., b_{j,i+7}$ according to $s' \oplus s$.
      Product $b'_{j,i}, b'_{j,i+1}, ..., b'_{j,i+7}$.
      Do seven times the error diffusion in I according to the $b'_{j,i}, b'_{j,i+1}, ..., b'_{j,i+7}$.

In process of extracted secret data, we only scan the stego-halftone images, and take each seven pixels into Equation (3), then can extract the all secret data.

3. Experimental results

In this section, we discuss the experiments we have conducted and let the experimental results demonstrate the practicability and effectiveness of the proposed method. In the experiments, we used six 512×512 gray-level images (Lena, Baboon, Sailboat, Pepper, Boat, and Tiffany). The six test images were transformed by Jarvis' error diffusion into the six halftone images shown in Figure 3. Then, in order to compare the stego-halftone image with the original halftone image, we utilize the least-mean square (LMS) filter proposed in [18] to define PSNR. The main purpose is to evaluate the visual quality if the halftone image is transformed into the gray-level image. The PSNR value can be derived as follows:

$$PSNR = \frac{H \times W}{\sum_{i=1}^{H}\sum_{j=1}^{W}\left[x_{j,i} - \sum_{m}^{f_m}\sum_{n}^{f_n} w_{m,n} b_{j+m,i+n}\right]}$$

(8)

Here, H and W stand for the host image's height and width, respectively. Besides, $x_{j,i}$ represents the pixel of the original gray-level image in position (j, i), and $b_{j,i}$ is the pixel of the halftone images in the same position. The notations f_m and f_n stand for the height and width of the filter window size, respectively, and $w_{m,n}$ is the LMS filter value acquired through experiments in [18] and Table 1 shows an example [18].

Table 1: Training results of LMS filter

LMS filter size	5×5				
Error diffusion (Floyd-Steinberg)	0.001	0.031	0.038	0.021	0.002
	0.031	0.080	0.099	0.062	0.016
	0.036	0.096	0.122	0.080	0.024
	0.016	0.052	0.071	0.046	0.013
	0	0.012	0.019	0.010	0.001

In Figure 2 and 3, the quality of the stego-halftone image can be discovered in our proposed scheme close to the original halftone image after embedded the secret data. Figure 2 shows six halftone image produced by Floyd-Steinberg error diffusion, and PSNR value equal to 29.84, 23.45, 27.88, 29.46, 28.21, and 29.38 dB. Figure 3 shows the stego-halftone image of our proposed scheme and PSNR value equal to 24.29, 21.18, 23.60, 23.69, 23.65, and 23.17 dB after embedded the secret data and the PSNR average only degrades 4.77 dB. The proposed scheme can embed three bits in seven halftone pixels, therefore, the data hiding capacity can over 42%. In visual observation, it also satisfies the character of imperceptible.

Here, we use directly the hamming code hiding in original halftone image and the results show in Figure 4 (b). In visual observation, Figure 4 (b) can discover the low image quality obviously. For this reason, the process of the gray-level image transformed halftone image embedded the secret data can improve the image quality, as show in Figure 4 (c). The experimental results demonstrate that the stego-halftone image is high in our proposed scheme, and can achieve the effect of steganographic.

4. Conclusions

In this paper, we propose a new data hiding scheme in process of producing halftone images. The scheme embedded the secret data using the covering code in the error diffusion. The experimental results show the image quality of stego-halftone image better than embedded directly the secret date using the covering code in halftone image. Moreover, the PSNR degrades average 4.77 dB between the stego-halftone image in our proposed scheme and original halftone image. The data hiding capacity can embed three bits in seven pixels, and over whole image 42%. The experimental results have demonstrated that it is extremely hard for any potential attacker to tell the difference between the stego-halftone image and the original halftone image through the naked eye.

5. Rerferences

[1] R. Ulichney, *Digital halftoning*. Cambridge, MA: MIT Press, 1987.

[2] E. Bayer, "An optimum method for two level rendition of continuous tone pictures", *In IEEE International Conference on Communications, Conference Record*, Seattle, Washington, USA, June 11-13 1973, pp. 11-15.

[3] J. F. Jarvis, C. N. Judice and W. H. Ninke, "A survey of techniques for the display of continuous-tone pictures on bilevel displays", *Computer Graphics and Image Processing*, vol. 5, 1976, pp. 13-40.

[4] R. W. Floyd and L. Steinberg, "An adaptive algorithm for spatial gray scale", *Proceedings of the Society for Information Display*, 1975, pp. 36–37.

[5] D. E. Knuth, "Digital halftones by dot diffusion", *ACM Transactions on Graphics*, vol. 6, no. 4, October 1987, pp. 245-273.

[6] M. Mese and P. P. Vaidyanathan, "Optimized halftoning using dot diffusion and methods for inverse halftoning", *IEEE Transactions on Image Processing*, vol. 9, no. 4, April 2000, pp. 691-709.

[7] W. Zeng, "Digital watermarking and data hiding: technologies and applications", *in Proc. Int. Conf. Inf. Syst., Anal. Synth*., vol. 3, 1998, pp 223-229.

[8] C. C. Thien and J. C. Lin, "A Simple and High-Hiding Capacity Method for Hiding Digit-by-Digit data in images based on Modulus function", *Pattern Recognition*, vol. 36, no. 13, 2003, pp. 2875-2881.

[9] C. K. Chan, L. M. Cheng, "Hiding data in images by simple LSB substitution", *Pattern Recognition*, vol. 37, no. 3, 2004, pp. 469-474.

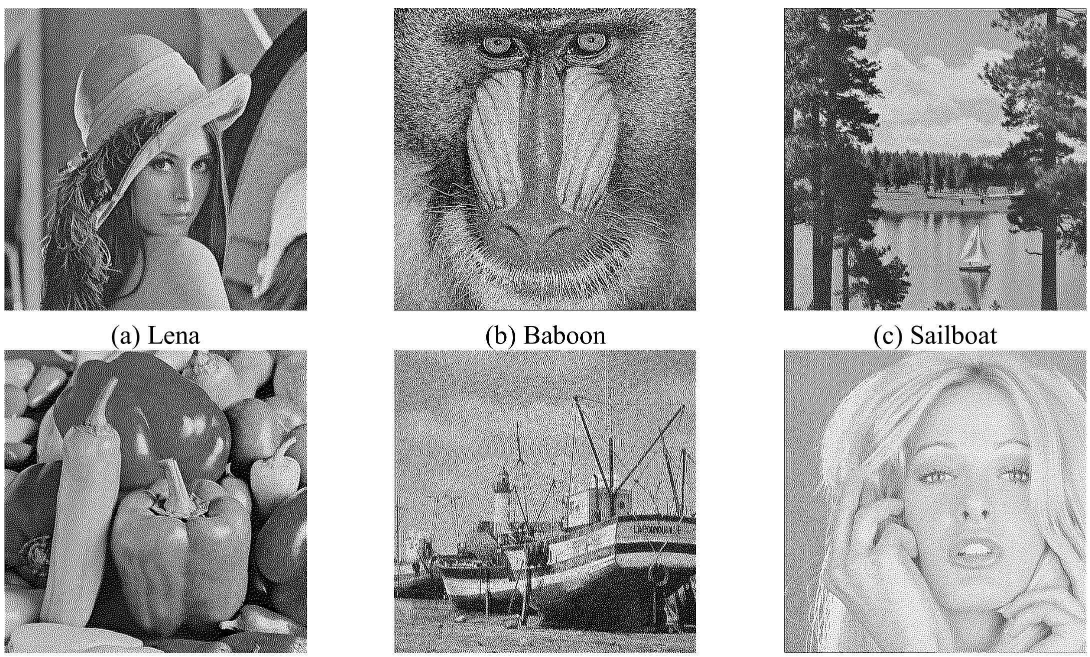
[10] S. L. Li and K. C. Leung, L. M. Cheng, C. K. Chan, "A novel image-hiding scheme based on block difference", *Pattern Recognition*, vol. 39, no. 6, 2006, pp. 1168-1176.

[11] M. S. Fu and O. C. Au, "Data hiding for halftone images", *In Proceedings of SPIE Conference on Security and Watermarking of Multimedia Contents II*, January 2000.

[12] M. S. Fu and O. C. Au, "Data hiding by smart pair toggling for halftone images", In Proceedings of *IEEE International Conference on Acoustics, Speech and Signal Processing*, June 2000.

[13] M. S. Fu and O. C. Au, "Halftone image data hiding

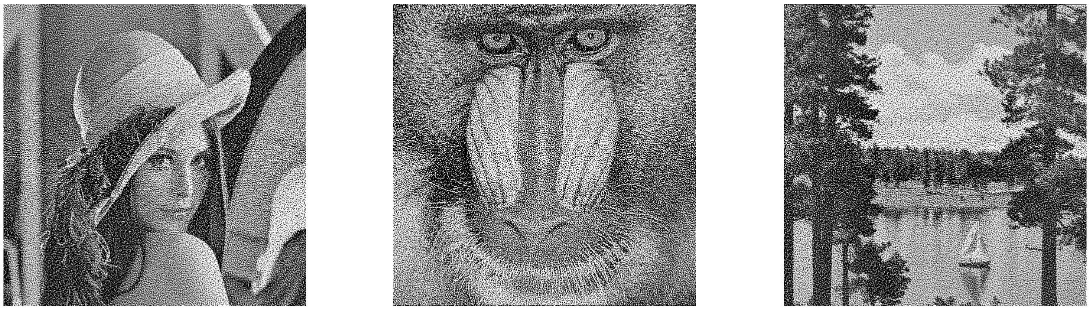
with intensity selection and connection selection", *Signal Processing: Image Communication,* vol. 16, no 10, August 2001, pp. 909-930.
[14] M. S. Fu and O. C. Au, "Data hiding watermarking for halftone images", *IEEE Transactions on Image Processing*, vol. 11, no. 4, April 2002, pp. 477-484.
[15] S. C. Pei and J. M. Guo, "Hybrid pixel-based data hiding and block-based watermarking for error-diffused halftone images", *IEEE Transaction on Circuits and Systems for Video Technology*, vol. 13, no. 8, August 2003, pp. 867-884.
[16] S. C. Pei and J. M. Guo, "Data hiding in halftone images with noise-balanced error diffusion", *IEEE Signal Processing Letters*, vol. 10, no. 12, December 2003, pp. 349-351.



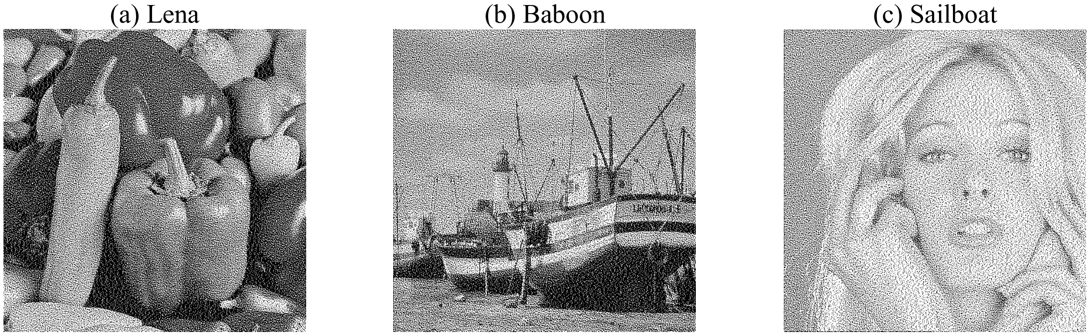
(a) Lena (b) Baboon (c) Sailboat
(d) Pepper (e) Boat (f) Tiffany

Figure 2: The six halftone images transformed by Jarvis' error diffusion. (a) PSNR= 29.84 dB, (b) PSNR=23.45 dB, (c) PSNR=27.88 dB, (d) PSNR=29.46 dB, (e) PSNR=28.21 dB, (f) PSNR=29.38 dB.

[17] S. C. Pei, J. M. Guo and H. Lee, "Novel robust watermarking technique in dithering halftone images", *IEEE Signal Processing Letters*, vol. 12, no. 4, April 2005, pp. 333-336.
[18] S. C. Pei and J. M. Guo, "High-capacity data hiding in halftone images using minimal-error bit searching and least-mean square filter", *IEEE Transactions on image processing*, vol. 15, no. 6, June 2006, pp.1665-1679.
[19] J. Bierbrauer and J. Fridrich, "Constructing good covering codes for applications in steganography", available: http://www.ws.binghamton.edu/fridrich/ (2008).
[20] W. Zhang, S. Wang, and X. Zhang, "Improving embedding efficiency of covering codes for applications in steganography", *IEEE communication letters*, vol. 11, no. 8, August 2007, pp. 680-682.



(a) Lena (b) Baboon (c) Sailboat



(d) Pepper (e) Boat (f) Tiffany

Figure 3: The six stego-halftone images of our proposed scheme. (a) PSNR= 24.29 dB, (b) PSNR=21.18 dB, (c) PSNR=23.60 dB, (d) PSNR=23.69 dB, (e) PSNR= 23.65 dB, (f) PSNR=23.17 dB.

(a) (b) (c)

Figure 4: We use directly the hamming code hiding in original halftone image (b) and our proposed scheme (c). (a) PSNR= 29.84 dB, (b) PSNR=19.84 dB, (c) PSNR=24.29 dB.