Asian Journal of Information Technology, 5 (2) : 205-212, 2006

Digital Watermarking for Error-diffused Images

[1]Wei-yu Han and [2]Yea-jou Shiau
[1]Department of Computer Science and Information Engineering,
Ching Yun University, Jung-li, Taiwan
[2]The 202nd Arsenal, Mab, Mnd., Taipei, Taiwan

Abstract: In this study, a new approach for watermarking of the Error-Diffused images is proposed for hiding data in halftone images. This novel data hiding is by forcing the parity on the processing pixel and preceding halftoned pixels in a unit of data either even or odd. Here, the parity used to preserve the data by means of authentication and tampering detection. The error between the original halftoned bit and parity setting bit of the current pixel is propagated to the unprocessed neighboring pixels for maintaining good visual quality. The proposed approach is directly applied to the halftoning process without extra computations. Experimental results show that the proposed method has successfully hidden the watermark into the Error-Diffused images and the results are encouraging.

Key words: Digital, watermarking, erro diffused, images

INTRODUCTION

Halftoning is the process of rendering grayscale images so that they can be printed or displayed on bi-level output devices. Pixels are assigned to either black or white to create the illusion of continuous shades of gray. It is used in image display devices capable of reproducing two-level outputs such as laser printers and digital typewriters. Today, digital halftoning plays a key role in almost every discipline that involves printing and displaying [1]. All books, magazines and newspapers are printed with digital halftoning.

Error diffusion revolutionized the digital halftoning field and has given the spark for the development of a great number of new methods. Error diffusion is based on the simple principle that once a pixel has been quantized, thus introducing some error, this error should affect the quantization of the neighboring pixels. By diffusing the error, the system performs as a self-correcting, negative feedback system.

Digital watermark-hiding has been considered as a possible approach to address the problem for digital documents in copyright control and authentication.

This work was supported by the National Science Council, Republic of China, under contract NSC 94-2213-E-231 -001

Especially, digital watermarking recently draws a lot of attention since it hides desirable information in transmitted image files without affecting much the data quality. The present watermarking techniques are divided into two different classifications. One is applied to the spatial domain and the other is applied to the frequency domain[2]. Traditional watermarking techniques most are frequency domain technology and watermark embeds the information data in the coefficients of transformation domain of the cover image, such as Fourier transformation, discrete cosine transformation and wavelet transformation[3-5]. Watermark is hided by changing the coefficient after transformed, then transform back to original spatial domain, so that the action of watermarking hiding finishes. This method need huge amount of calculation, but it has better ability to prevent destroy from the signal processing. Spatial domain watermarking technique is by directly changing original cover-media. The advantages are simple and fast calculated but cannot protect itself from varied signal processing attacking. It is also the most simple, direct and common technique by using the least significant bit embedding. The theory is very simple. It hides the watermarking date into several last binary bits of cover-media[6]. A spatial watermarking method presented a block based on elementary perceptual criterion and adapts the embedding with regards to the content of the blocks[7]. The watermark is capable of carrying such information as authentication or authorisation codes, or a legend essential for image interpretation[2, 3, 4, 7, 8]. Traditionally, watermark techniques in tempering detection, most of researchers are focus on the digital signature that is a mechanical, computational process. Some entity in possession of a public/private key pair is

Corresponding Author: Wei-Yu Han, Department of Computer Science and Information Engineering, Ching Yun University, Jung-Li, Taiwan

willing to perform a computation on a set of data using this key pair, which permits someone who knows the public key of the key pair to verify that the data were known to and computed upon by an entity that held the key pair[9, 10]. A new type of watermark, called fragile has been recently proposed for digital images. A fragile mark is designed to detect slight changes to the watermarked image with high probability. The main application of fragile watermarks is in content authentication. Many important applications could benefit from the use of fragile watermarks[11, 12]. In above researches, most of the authors apply the turning continuous tone grayscale in digital images. Some other authors proposed halftoning methods in image processing researches[13-15]. Kimoto proposed a watermark hiding method that a digital image printed as a binary halftone image can have an optical watermark which becomes visible only if the associated halftone image is superimposed on it. In the scheme of template-dot halftoning, such pair of images can be generated by using different halftone cells on each image at a watermark dot. In this research,. template cells used for each halftone level are limited to two cells to reduce the degradation of halftone quality. Either one of the two template cells is randomly selected and used to generate a pair of halftone images with hiding optical watermarks in them. A set of two alternative template cells used for each halftone level which yields less noisy halftone quality is investigated through computer simulation.

In this study, we propose a new method based on parity check and error diffusion for hiding image/data in halftone images. At the receiver, the image/data is extracted in the same check way as the image/data generated.

A REVIEW OF ERROR DIFFUSION (ED)

ED is a popular halftoning technique to generate high quality halftone image. In an ED algorithm, each pixel of the input image is compared with a fixed threshold value, if the current pixel's gray value is greater than the threshold value, the output is assigned as one, otherwise, a zero is placed. The error between the input and output of the current pixel is propagated to the unprocessed neighboring pixels (the propagation ratios among these neighbors are determined by an weight matrix). Fig. 1a depicts the block diagram and the associated parameters of a typical ED, with the weight matrix used in Fig. 1a being the well-known weight matrix (Fig. 1b) proposed by Floyd and Steinberg[16]. Since there are so many versions of ED and almost all of them are derived from[16], the error-diffused images mean that the images are halftoned by the method proposed by Floyd and Steinberg[16] in this study.

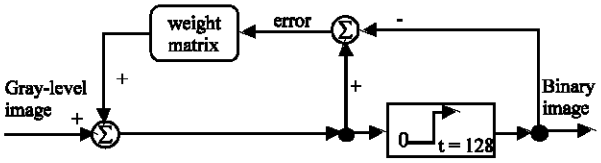

Fig. 1a: The typical error diffusion algorithm

$$\frac{1}{16}\begin{bmatrix} & x & 7 \\ 3 & 5 & 1 \end{bmatrix}$$

Fig. 1b: The weight matrice (x is the location of the current pixel) proposed by Floyd and Steinberg

THE PROPOSED WATERMARKING ERROR DIFFUSION ALGORITHM

In order to be advantageous for the following explanation, the proposed method is formed by the following theoretical analysis. G image represents the original gray scale image, W is the watermark image and WED represents the watermark image joins into the ED image. Before a further discussion, we first observe that ED procedure will convert each pixel's gray value (0~255) of the G image, left to downward right, into a sequence of 0/1 bits; those output bits are similar to series transmission. In the communication system, parity check is a popular technique to detect the mistake in series transmission for the resistance disturbance, by means of join the parity check bit in each ending of a string of bits, for example 8 bits. There are two types of parity, name odd parity and even parity, according to the number of high bits in a string of bits is odd or even, respectively. Base on the concept of parity, we can use the parity of a series of bit-string in ED output to record it when any information needs to hide in the ED image,, for example even parity represents information bit 0 and the other one represents bit 1. The information may hide within the watermark.

In the experiment, a parity-bit-string length uses the fixed value to be able to create the WED image to have clear straight strip lines. To break this strip lines, the length of the parity-bit-string is in variation. This length is decided by a random number generator with a fixed seed. Because the data hiding process needs extra time to compute the parity-bit-string length, the visual quality of the WED image is no different between using fixed lengths and variable length to hide bits in one row. Therefore the parity-bit-string length will adopt the same value in each row. In order to hide the W image into the ED image entirely, the range on parity-bit-string length is needed to decide. For easily to know how to make the decision, it is important to define the relationship

between parity-bit-string length with the watermark size, the G image size and the random number first. It is well know, the output of random number generator is uniform distribution, may deliver real number between 0 to 1, its mean value is 0.5. Let the size of G image is $N_{row} \times N_{row}$ and the W image has N_w bits, then the upper bound S_{upper} and lower bound S_{lower} of the parity-bit-string length are obtained by Eq (1):

$$S_{upper} = \left(\frac{N_{row} \times N_{col}}{N_W} - S_{lower}\right) \times 2 \quad \cdots\cdots(1)$$

In this study, S_{lower} equals 8. S_{upper} is generated according to Eq. (1). Each row i, the random number Rn(i) is calculated first, then the parity-bit-string length SL (i) used for hiding material is obtained by Eq. (2).

$$SL(i) = Rn(i) \times S_{upper} + S_{lower} \quad \cdots\cdots(2)$$

Starting to carry out ED procedure to G image, regarding to each row i, we could set the parity consist with the hiding bit by means of changing the output of the last pixel after processing each SL (i) pixels. In the receiver, by the same random number generator with the same seed used in embedding stage, the extracted process can verify the watermark and the tampered watermarked image by inspecting parity one by one. The proposed watermarking method for Error Diffusion is summarized as follows:

Algorithm 1. Watermark embedding part

Input: The gray-level image G, the watermark image W which has been halftoned.
Output: WED image, the watermarked ED image of G.
Step:

1. In Eqs. (1) and (2), the value of S_{upper} and bits-string length *SL(i)* can calculate for each row i, respectively.
2. Convert the image W to one dimension array list AL.
3. Error-diffuse the image G, row by row,. every *SL(i)* pixels, names bits-string, have be halftoned for each row i. The parity of this bits-string is assigned even or odd according to the related binary values (0 or 1) in the AL which being embedded now. The parity of each bits-string is control by the output of the last pixel in the bits-string.

Figure 2a shows the WED image after applying algorithm 1 to the gray-level image G shown in Fig. 2b, for comparison, Fig. 2c depicts the original ED image of G, whereas Fig. 2d is the halftoned watermark image W with size 64×64.

Algorithm 2. Watermark detection part.

Input: The WED image.
Output: The reconstructed watermark image Wr.
Step:

1. By the random number generator which same as in algorithm 1 and the Eqs. (1) ~ (2), we can get Supper and bits-string length *SL(i)* for each row i.
2. Processing the input image WED, row by row,, every *SL(i)* pixels, reconstructa the embedded bit (0 or 1) according to the parity of each bits-string is even or odd for each row i, then put the bit into the array list AL.
3. Mapping one dimension array list AL form the image Wr.

Figure 3a shows the Wr image after applying algorithm 2 to the WED image shown in Fig. 2a. The image depicted in Fig. 3b is the result with the input image that has no watermark (Fig. 2).

Algorithm 3. Tamper detection part.

Input: The WED image.
Output: The WED image with tamper mark.
Step:

1. By the random number generator which same as in algorithm 1 and the Eqs. (1) ~ (2) and bits-string length *SL(i)* can calculate from each row i.
2. Processing the input image WED, row by row,, every *SL(i)* pixels, names bits-string, detect the tamper bit (0 or 1) for each row i according to the parity of each bits-string is even or odd. If tamper bit is 1 then mark this bits-string.

Fig. 2a: The output image after apply algorithm 1 to the gray-level image LENA

Fig. 2b: The gray-level image LENA (512¡Ñ512)

Fig. 2c: The output image after apply standard ED to the gray-level image LENA

Fig. 2d: The halftoned watermark image

Fig. 3a: The reconstructed watermark image

Fig. 3b: The reconstructed watermark image after applying algorithm 2 to the input image without hiding data

Fig. 4a: The output image which hiding 128×128 bits

Fig. 4b: The tamper version of Fig. 4a

Figure 4a was similar to Fig. 2a except the input watermark image (size was 128×128 and the value of each pixel was 1). Figure 4b depicts the tamper version of Fig. 4a. Figure 4c shows the detecting and localizing modification after applying algorithm 3 to Fig. 4b.

Fig. 4c: The output after applying algorithm 3 to Fig. 4b

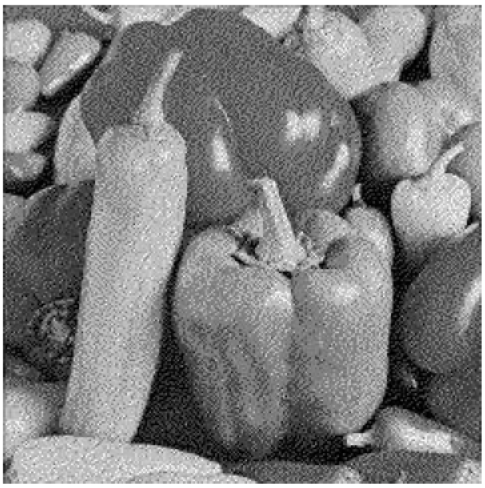

Fig. 5c: The image after applying Algorithm 1 (the watermark size was 64×64) to the image depicted in Fig. 5a

Fig. 5a: The gray-level image Pepper (512×512)

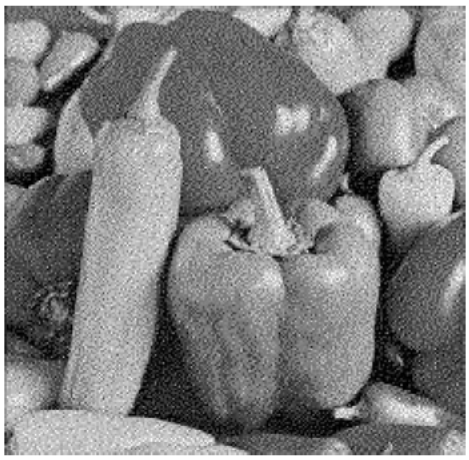

Fig. 5d: The output after applying Algorithm 1 (watermark size 128×128) to Fig. 5a

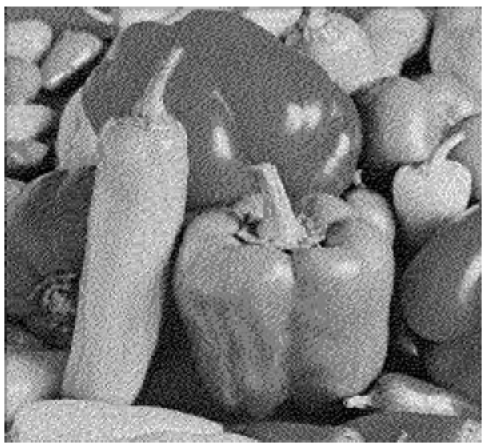

Fig. 5b: The output image after apply standard ED to the gray-level image Pepper

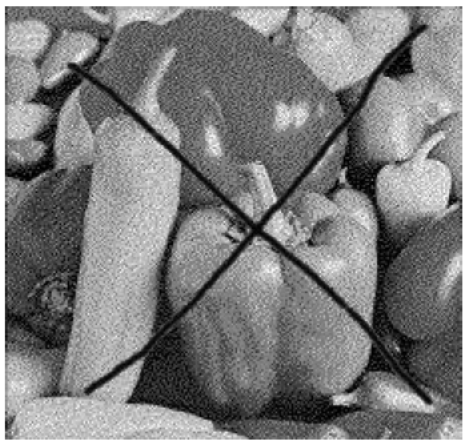

Fig. 5e: The corrupt version of image original shown in Fig. 5c

Fig. 5f: The corrupt version of image original shown in Fig. 5d

Fig. 5g: The output after applying Algorithm 2 to the image shown in Fig. 5e

Fig. 5h: The result after applying Algorithm 2 to the image shown in Fig. 5f

Fig. 6a: The gray-level image Boat (512×512)

Fig. 6b: The result after apply standard ED to the gray-level image Boat

Fig. 6c: The result after applying Algorithm 1 (watermark size 128×128) to Fig. 6a

MORE EXPERIMENTAL RESULTS

For more confirmations of results, more images had been tested. Figure 5a and 5b are the original gray-level image and its ED image. Fig. 5c~5d were the image after applying Algorithm 1 (the watermark size was 64×64 and 128×128, respectively) to the image depicted in Fig. 5a. Figure 5e and Fig. 5f were the corrupt version of images and the original shown in Fig. 5c and Fig. 5 d,

Fig. 6d: The tamper version of Fig. 6c

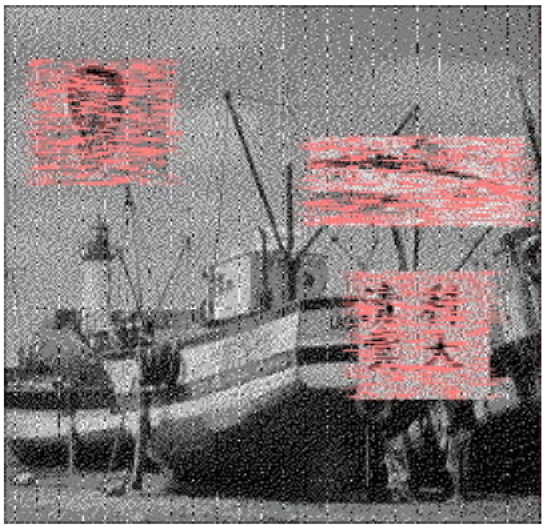

Fig. 6e: The result after applying algorithm 3 to Fig. 6d

respectively. Figure 5g~5h exposed the detected watermark after applying Algorithm 2 to the image shown in Fig. 5e and Fig. 5f, respectively. Other tested images of tamper detection and their results were given in Fig. 6. It is for sure that the proposed Watermark technique can be used in the application of watermark as well as tamper detection.

CONCLUSIONS

A new approach for watermarking and tamper detection of the error-diffused[16] images has been developed. The major contributions of this paper include:

- Both the watermark embedding and tamper detection are directly cooperating with the error-diffusion process;
- The proposed watermark detection method can work with corrupted error-diffused images;
- The proposed tampering method can directly find the location of the tampers in the meddled error-diffused images;
- Those methods are very simple and quick, therefore suitable for real-time applications. As a future work, the watermarked image quality can be improved further, especially when the watermark images are large enough such as 128×128, by means of adjusting the position of the parity check bits.

REFERENCES

1. Ulichney, R.A., 1987. Digital Halftoning, MIT Press, Cambridge, MA.
2. Ingemar, J., M. Cox, L. Miller, A. Jeffrey and Bloom, 1999. Digital Watermarking, Morgan kaufmann publishers.
3. Cox, I.J., J. Kilian, F.T. Leighton and T. Shamoon, 1687. Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Processing, 6: 1673-1687.
4. Kutter, M. and S. Winkler, 2002. A vision-based masking model for spread-spectrum image watermarking, IEEE Trans. Image Processing, 11: 16-25.
5. Solachidis, V. and I. Pitas, 2004. Watermarking polygonal lines using Fourier descriptors, Computer Graphics and Applications, IEEE, 24: 44-51.
6. Benedens, O. and C. Busch, 2000. Towards blind detection of robust watermarks in polygonal models, Computer Graphics Forum, 19: 199-208.
7. Van Schyndel, R.G., A.Z. Tirkel, N. Mee and C.F. Osborne, 1994. A digital watermark, Proc. IEEE Int. Conf. Image Processing, Austin, 2: 86-90.
8. Darmstaedter, V., J.F. Delaigle, I.J. Quisquater and B. Macq, 1998. Low cost spatial watermarking, Computer and Graphics, 22: 417-424.
9. Hsieh, M.S., D.C. Tseng and Y.H. Huang, 2001. Hidden digital watermarks using multiresolution wavelet transform, IEEE Trans. Industrial Electronics, 48: 875-882.
10. Stinson, D.R., 1995. Cryptography: Theory and Practice , Boca Raton, Fl: CRC Press.
11. Hongtao Lu, Ruiming Shen, Fu-Lai Chung, 2003. Fragile watermarking scheme for image authentication, Electronics Lett.. 39: 898-900.

12. Junquan, H., J. Huang, D. Huang and Q. Yun Shi, 2002. Image fragile watermarking based on fusion of multi-resolution tamper detection, Electronics Lett., 38: 1512-1513.
13. Ming Sun Fu and O.C. Au, 2002. Data hiding watermarking for halftone images, IEEE Tran. on Image Processing, 11: 477-484.
14. Ming Sun Fu, O.C. Au, 2003. Self-conjugate watermarking technique for halftone images, Electronics Letters, 39: 356-358.
15. Kimoto, T., 2003. Hiding optical watermarks in hard copy images with reducing degradation of halftone quality, in Proc. SPIE, Visual Communications and Image Processing, Lugano, Switzerland, 3: 1895-1904.
16. Floyd, R.W. and L. Steinberg, 1976. An adaptive algorithm for spatial gray scale. Proc. SID 17: 75-77.