The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 14, No. 2, pp.11-16, Apr. 30, 2014. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2014.14.2.11
JIIBC 2014-2-2

Data Hiding Based on BTC using EMD

EMD를 사용한 BTC 기반의 데이터 은닉

김천식*

Cheonshik Kim*

요 약 BTC는 단색 이미지 데이터의 압축을 위해서 사용되는 최근의 기술이다. BTC의 알고리즘은 평균과 표준편차를 사용하여 구현한다. 데이터 은닉을 위해, 이미지의 비트-구조를 변경하는 과정이 요구된다. 이러한 변경은 BTC 이미지의 질의 성능을 나쁘게 만든다. 따라서, 우리는 데이터 은닉의 성능 개선을 위해서 BTC를 개선한 IODBTC를 제한하였다. 실험 결과 복원한 비밀 메시지가 원본 비밀 메시지와 같음을 증명하였고 제안한 방법이 이전의 스킴에 비해서 좋은 BTC 이미지임을 증명하였다.

Abstract Block truncation coding (BTC) is a recent technique used for compression of monochrome image data. The original algorithm of BTC implement to use the standard mean and the standard deviation. For data hiding, it is needed to modify bit-planes of an images. These modifications yields unacceptable quality of BTC images. Thus, we propose IODBTC (Improved Ordered dithering BTC) improving BTC. In this paper, we improve this problem. Experimental results show that the reconstructed secret messages are the same as the original secret messages, and that the proposed scheme exhibits a good BTC images compared to that of previous schemes.

Key Words : BTC, data hiding, compression, bitmap, IODBTC

Ⅰ. Introduction

The image compression techniques are categorized into two category, i.e., lossy compression techniques and lossless compression techniques. Lossless compression ratio gives good quality of compressed images, but yields only less compression, however the lossy compression techniques guide to loss of data. For instance BTC (Block Truncation Coding)[1] and JPEG is a lossy image compression techniques. The truncated block of the BTC is the one-bit output of the quantizer for every pixel in the block. Many researchers have been investigated gray scaled images for data hiding, whereas BTC ones have been researched less.

In fact, data hiding techniques cannot provide safety of the messages themselves; these techniques only conceal the existence of the secret messages while cryptography protects their content. That is, the purpose of data hiding is only to conceal existence of the hidden data. Until now, various kinds of secret communication methods that can conceal the messages have been proposed[2-10,13].

*종신회원, 안양대학교 디지털미디어공학과
접수일자 : 2014년 2월 8일, 수정완료 : 2014년 3월 16일
게재확정일자 : 2014년 4월 11일

Received: 8 February, 2014 / Revised: 16 March, 2014 / Accepted: 11 April, 2014
*Corresponding Author: Cheonshik Kim
Dept. of Digital Medial Engineering, Anyang University, Korea
Tel : 82-31-467-0780, E-mail: mipsan@paran.com

Delp and *Mitchell* proposed Block truncation coding (BTC) in 1979, which is simple, efficient and has low computation complexity[1].

Wu et al.[11] proposed data hiding scheme based BTC using odd-even number. *Lin et al.*[12] presented a BTC based data hiding method which modified the bitmap with minimum distortion.

Shu-Fen Tu[4] showed a binary image combined with the watermark for constructing the ownership share with the help of the XOR operation. However, this method was not really hiding information in host images. It is expected that a large quantity of data is difficult to embed into BTC images considering visual quality degradation, for less information redundancy can be employed. In this paper, we suggest improving data hiding scheme for BTC images.

Ⅱ. Related Works

In this section, we explain EMD method, IODBTC (Improved Ordered dithering BTC)[2] and gray code.

1. EMD method

The EMD (Exploitation Modification Direction) is a novel method for hiding data in an image with schemes of modification directions. The main idea of EMD scheme is that each secret digit in a $(2n+1)$-*ary* notational system is carried by n cover pixels, when $n \geq 2$ and, only one pixel is increased or decreased by 1.

A group of pixels is composed as $(\ \ , g_2, \cdots, g_n)$. If the secret message is a binary stream, it can be segmented into many pieces with L bits in each one, and the decimal value of each secret pieces represented by K digits in a $(2n+1)$-*ary* notational system, where

$$L = \lfloor K \bullet \log_2(2n+1) \rfloor \tag{1}$$

According to a secret key, all cover pixels are permuted pseudo-randomly and divided into a series of pixels-groups, each containing n pixels.

$$f(g_1, g_2, ..., g_n) = \left\lfloor \sum_{i=1}^{n} (g_i \bullet i) \right\rfloor \bmod (2n+1) \tag{2}$$

2. Improved Ordered dither BTC

Ordered dithering is an image dithering algorithm. It is commonly used by programs that need to provide continuous image of higher colors on a display of less color depth. In IODBTC coding method an image is divided into M×N blocks, and maximum value is set to x_{max} and minimum value is set to x_{min}(Eq.(3)):

$$o_{i,j} = \begin{cases} x_{\max}, & if \ x_{i,j} \geq LUT_{i \bmod M \ j \bmod N} + x_{\min} \\ x_{\min}, & if \ x_{i,j} < LUT^{(k)}_{i \bmod M \ j \bmod N} + x_{\min} \end{cases} \tag{3}$$

The o_{ij} denotes the output pixel value, and $k = x_{max} - x_{min}$. A feature of the IODBTC is the dither arrays *LUT*, where each specific dither array has its corresponding 255 different scaling versions. The 255 scaling versions are obtained as follows:

$$LUT^{(k)}_{m,n} = k \times \frac{LUT_{m,n} - LUT_{\min}}{LUT_{\max} - LUT_{\min}} \tag{4}$$

where $1 \leq k \leq 255$, $1 \leq m \leq M$, and $1 \leq n \leq N$; LUT_{min} and LUT_{max} denote the minimum and maximum values in dithered array. The dynamic range of $UT^{(k)}_{\min}$ must be added by x_{min} to provide a fair threshold for the pixel values in a block. Since the dither array $LUT^{(k)}_{\min}$ is calculated in advance, the complexity can be significantly reduced in practical application.

3. Gray code

Gray code is a code assigning to each of continuous set of integers, or to each member of a circular list, a sequence of symbols such that each two adjacent code sequences differ by one symbol. Table 1 shows an example of that gray code with according binary and decimal numbers.

1. 그레이 코드
Table 1. Gray code

Dec	Gray	Binary
0	000	000
1	001	001
2	011	010
3	010	011
4	110	100
5	111	101
6	101	110
7	100	111

III. Proposed Scheme

In this section, we suppose the size of host image is $P \times Q$ and it is dithered by IODBTC using Eq.(3) and Eq.(4).

1. Data Embedding

In this section, we illustrate data embedding method for a BTC image. Fig.1 shows the procedure of data embedding starting from converting gray-scale image into a BTC one. The step-by-step procedure is stated as follows.

Step 1: A BTC image is generated from gray-scale image using Eq.(5), where GI and HI denote gray-scale and BTC images respectively. $M \times N$ is a block size. $x_{m,n}$ is a pixel value in 4×4 block of gray-scale image. x_{max} is the largest value in a block and x_{min} is the smallest value in a block. $o_{m,n}$ takes the value of x_{min} or x_{max} depending on Eq.(5). If $o_{m,n}$ is greater than x_{min}, $b_{m,n}$ is assigned to '1', otherwise $b_{m,n}$ is assigned to '0'. Thus, we get a BTC as Fig.2.

Step 2: For using EMD scheme, the value of group bitmap pixels needs to be changed from gray code to decimal because of arithmetic operation. In Fig.3, it shown that the procedure of converting from gray code to decimal number is possible to be done for group of 8 pixels. In the figure, first and second value are 247 and 212 respectively.

Step 3: The first value is assigned to g_1 and second value is assigned to g_2, and these values, i.e., g_1 and g_2, become a group of pixels, e.g., [247, 212].

Step 4: No modification is needed if a secret digit d equal to the extraction function of the original pixel-group. When $d \neq f$, calculate $s = d - f \bmod (2n+1)$. If s is less than n, increase the value of g_s by s, otherwise, decrease the value of $g_{2n+1-abs(s)}$ by 1. If d is 0, then the result becomes as shown in Fig.3. That is, group of pixels becomes [246, 212].

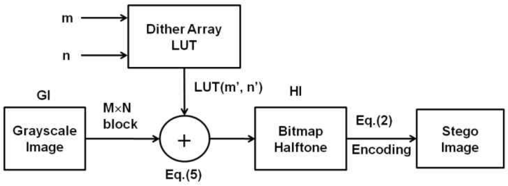


그림 1. IODBTC를 위한 인코딩 절차
Fig. 1. Encoding procedure for IODBTC image

(a)

160	50	50	50
160	160	50	50
160	50	160	160
160	160	160	50

(b)

1	0	0	0
1	1	0	0
1	0	1	1
1	1	1	0

그림 2. (a) 이미지의 한 블록, (b) 비트 평면
Fig. 2. (a) a block of image, (b) bit plane

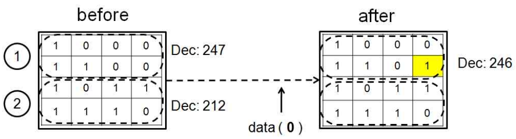
Fig.2 and Fig.3 show the procedure of encoding in a BTC image. Since the quality of a BTC image can be distorted easily, a small change of value in a BTC is essential requisition.

$$HI_{i,j}=\left\{\sum_{i=1}^{width(GI)}\sum_{j=1}^{height(GI)}\left\{\sum_{m=1}^{4}\sum_{n=1}^{4}b_{m,n}\right\}\right\} \qquad (5)$$

Where,

$$o_{m,n}=\begin{cases}x_{max}, if\ x_{m,n}\geq LUT_{i \bmod M\ j \bmod N}+x_{min}\\ x_{min}, if\ x_{m,n}< LUT^{(k)}_{i \bmod M\ j \bmod N}+x_{min}\end{cases},$$

$$b_{m,n}=\begin{cases}1, if\ o_{m,n}\geq x_{min}\\ 0, if\ o_{m,n}< x_{min}\end{cases},$$



$f = (247_{g1} \times 1 + 212_{g2} \times 2) \bmod 5 = 1$

$f = 1,\ s = d - f = -1,\ s < n,\ g_s = g_s + s = 246$

그림 3. 데이터 은닉을 위한 절차
Fig. 3. The procedure for data embedding

When $d \neq f$, calculate $s = d - f \bmod (2n+1)$. If s is less than n, increase the value of g_s by 1, otherwise, decrease the value of $g_{2n+1-abs(s)}$ by 1.

Example 1: g = [137 139], n = 2, f=0. Let d = 4. Since s = 4, an encoder will decrease the gray value of the first pixel by 1 to produce the stego-pixels [136 139]. At the decoder, f=4. Therefore, decoder can extract secret message 4.

Example 2: g = [141 140], n = 2, f = 1. Let d = 0. Since s = −1, an encoder will increase the gray value of the first pixel by g_s = g_s+s to produce the stego-pixels [140 140]. At the decoder, f=0. Therefore, decoder can extract secret message 0.

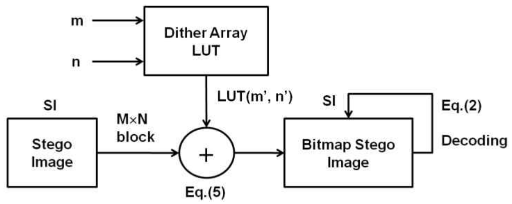
2. Data extraction

In this section, we describe the procedure of data extraction as diagram (show Fig.4).

Step 1: Divide the stego image into blocks of size 4×4. These blocks are non-overlapped.

Step 2: For decoding, the BTC is changed into the bitmap as shown in Fig.5.

Step 3: Blocks of bitmap need to be changed into decimal numbers. And then, we apply these values to Eq.(2) as shown in Fig.5. First value is assigned to g_1 and second value is assigned to g_2, so g_1 and g_2 become a group, i.e., [246, 212]. Next, we can calculate f value. In this case, f becomes 0.



4. BTC 이미지를 위한 디코딩 절차
Fig. 4. decoding procedure for BTC images

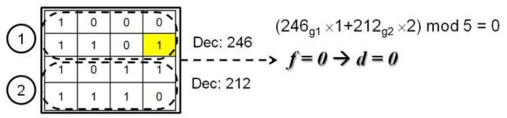


그림 5. EMD 메소드에서 디코딩 처리
Fig. 5 The process of decoding in EMD method

Fig. 5 shows the procedure of decoding with BTC image. As Fig.5, decoding procedure is a simple.

Ⅳ. Experimental Results

We experimented data hiding with nine 512×512 gray-scale images. To accurately measure a perceptual quality, the qualities of the stego images are measured by the peak-signal-to-noise ratio (PSNR)[7]. The PSNR is the most popular criterion for measuring distortion between the original image and shadow images. It is defined as follows:

$$SNR \quad 10\times\log_{0}(255^2/MSE) \tag{6}$$

where MSE is the mean square error between the original gray-scale image and the shadow image:

$$MSE = \frac{1}{m\times n}\sum_{i}^{m}\sum_{j}^{n}[I(i,j)-I'(i,j)]^2 \tag{7}$$

The symbols $I(i,j)$ and $I'(i,j)$ represent the pixel values of the original gray-scale image and the stego image at position(i,j), respectively, and m and n are the width and height of the original image.

For example, Table 2 shows that PSNR between our proposed scheme and previous schemes (BTC, *Wu et al.*'s scheme, and *Lin et al.*'s scheme). As can be seen from the Table 2, the PSNRs of our proposed scheme is better than that of previous schemes.

$$R = \frac{\log_2(2n+1)}{n} \tag{8}$$

On the other hand, our proposed method is able to embed about 32,768 bits into 512×512 image, with ability to hide 2 bits per a block. Eq.(8) measure embedding rate of data hiding. In order for us to show the capacity of the method proposed in this paper, we compare it with the one proposed by *Wu et al.*'s scheme (show Table 3). As one can seen from this table, our method is better than that of *Wu et al.*'s scheme.

2. 기존의 방법과 제안한 방법 간의 PSNR 비교
Table 2. Comparison of PSNR between our proposed scheme and previous schemes

Name \ Method	BTC	Proposed Scheme	Wu's Scheme	Lin's Scheme
Lena	33.63	35.13	32.89	32.63
Baboon	26.72	27.69	26.30	26.24
Pepper	33.52	35.31	32.91	32.76
Boat	31.56	33.34	31.37	31.36
Airplane	32.02	33.52	31.82	31.76
Bridge	31.17	32.82	30.81	30.66
Goldhill	28.38	33.12	28.12	28.03
Tiffany	35.59	38.40	35.43	35.28

표 3. Wu 등의 스키과 본 논문의 스킴 간에 은닉 비율을 비교
Table 3. Comparison of embedding rate between Wu et al.'s and our proposed scheme

Name \ Method	Capacity(bit)	
	Wu's Scheme	Proposed Scheme
Lena	0.031	0.125
Airplane	0.031	0.125
Baboon	0.031	0.125
Boat	0.031	0.125
Pepper	0.031	0.125
Barbara	0.031	0.125

Therefore, we can conclude that our proposed method produces a very significant result.

Ⅴ. Conclusion

Many researchers have been interested in data hiding to hide information in gray-scale images. Thus, they proposed a lot of methods in various kinds of the journals. We also interested in data hiding in BTC images, so proposed new method to increase image quality and to hide more bits of data. In general, BTC images are sensitive property, because if pixels are changed in a BTC image, noises are increased in an image. Reducing such a problem, we applied gray code into EMD method. As a result, our proposed scheme shows very good result, that is, image quality is increased and embedding quantity is increased.

References

[1] E. Delp and O. Mitchell, "Image compression using block truncation coding," IEEE Transactions on Communications, vol. 27, no. 9, pp. 1335 - 1342, 1979.

[2] Guo, J.-M., "Watermarking in dithered halftone images with embeddable cells selection and inverse halftoning," Signal Processing, vol. 88, 1496-1510, 2008.

[3] J.-S. Pan, H. Luo and Z.-M. Lu, "Look-up Table Based Reversible Data Hiding for Error Diffused Halftone Images," Informatica, vol. 18, No. 4, 615-628. 2007.

[4] S. F. Tu and C. S. Hsu, "A BTC-based watermarking scheme for digital images," Information & security, vol.15, no.2, 2004,216-228.

[5] Tseng, H.W., and C.C. Chang, "Hiding data in halftone images," Informatica, 16(3), 419 - 430, 2005.

[6] X. Zhang, S. Wang, "Efficient Steganographic Embedding by Exploiting Modification Direction," Communications Letters, IEEE, vol.10, Issue: 11, pp. 781-783, 2006.

[7] C. Kim, "Data hiding by an improved exploiting modification direction," Multimedia Tools and Appl., vol.69, no.3, pp.569-584, 2014.

[8] P. T. Huy, N. H. Thanh, C. Kim, C.-N. Yang, "Data-Hiding for Halftone Images Using an Improved CPT scheme," KSII Transactions on Internet and Information Systems, vol.7, no.2, pp.405-424, 2013

[9] C. Kim, Y.-S. Hong, C.-P. Han, and S. Oh, "Binary and Halftone Image Data Hiding Technique using Run-Length," The Journal of The Institute of Webcasting, Internet Television and Telecommunication, vol.9, no.3, pp.37-43, 2009.

[10] Y.S. Im, E.Y. Kang, "Watermarking and QR Code in Digital Image Coding," The Journal of The Institute of Webcasting, Internet Television and Telecommunication, vol.12, no.6, pp.99-104, 2012.

[11] X. Wu, W. Sun, "Data Hiding in Block Truncation

Coding," 2010 International Conference on Computational Intelligence and Security, pp.406-410, 2010.

[12] M. Lin and C. Chang, "A novel information hiding scheme based on BTC," The 4th International Conference Computer and Information Technology, pp. 66 - 71, 2004.

[13] Boo-Hyung Lee, "Technique for production and encoding of New dot-type Print Watermark Pattern," Journal of the Korea Academia-Industrial cooperation Society, vol.10, no.5, pp.979-984, 2009.

소개

천 식 (종신회원)

• 1997년 : 한국외국어대학교 컴퓨터 및 정보통신공학과 (공학석사)
• 2003년 : 한국외국어대학교 컴퓨터 및 정보통신공학과 (공학박사)
• 2010년~2012년 : 세종대학교 교수
• 2013년~현재 : 안양대학교 교수
• 2007년~2009년 : 대한전자공학회 컴퓨터소사이어티 멀티미디어 분과위원장
• 2012년 : TACT 영문 저널 - 위원
• 2012년 : UMAS 워크샵 프로그램 의장
• 2013년 : GPC 2013 프로그램 의장
• 2014년 : FutureTech 2014 프로그램 의장
• 주관심분야 : 데이터베이스, 데이터마이닝, Steganography, 영상처리, e-Learning