AMBTC-Based Data Hiding Using Intra- and Inter-Block Embedding Strategy

Yu-Hsiu Lin
Dept. Electrical Engineering
Southern Taiwan University of Science and Technology
Tainan 710, Taiwan
email: yhlin1108@stust.edu.tw

Chih-Hsien Hsia
Dept. Computer Science and Information Engineering
National Ilan University
Ilan 260, Taiwan
email: chhsia625@gmail.com

Bo-Yan Chen
Graduate Inst. Automation Technology
National Taipei University of Technology
Taipei 106, Taiwan
email: t105618004@ntut.edu.tw

Yung-Yao Chen
Graduate Inst. Automation Technology
National Taipei University of Technology
Taipei 106, Taiwan
email: yungyaochen@mail.ntut.edu.tw

***Abstract*—This paper presents a novel data hiding approach for image compression with Absolute Moment Block Truncation Coding (AMBTC). Hiding data in digital images has widespread security uses, which include image authentication, prevention of malicious forgery, copyright protection, and so on. On the other hand, for transmission efficiency and storage space concerns, image compression techniques are commonly used in Internet-based applications. To achieve these two purposes simultaneously, we integrate AMBTC, a low computation complexity block-based compression technique, in the proposed data hiding scheme. First, five parameters are separately extracted from individual image blocks. By manipulating these parameters, secret data are embedded in the blocks without excessively degrading overall image quality. A halftoning method is incorporated to quickly identify optimal parameters. In addition, the interblock hiding scheme is proposed to embed extra data by exploiting the relevance between adjacent blocks. From the experimental results, it validates the effectiveness of the proposed method.**

Keywords-Absolute Moment Block Truncation Coding (AMBTC); inter- and intra-block embedding; direct binary search.

I. INTRODUCTION

With advances in wireless communication techniques and the popularity of personal smart phones, transmitting images over the Internet has become simple. However, the security of public networks such as those in hotels and coffee shops, which anyone can access, remains a great concern. Although there may be a password for specific users, such passwords are usually shared with other, unknown people. Data hiding methods address this problem by increasing the security level of Internet-based image itself. In addition, AMBTC is known as a high computation efficiency compression technique and has been improved by researchers in the past decade [1]. Therefore, the idea of combining AMBTC with data hiding, has received considerable research attention recently [2][3].

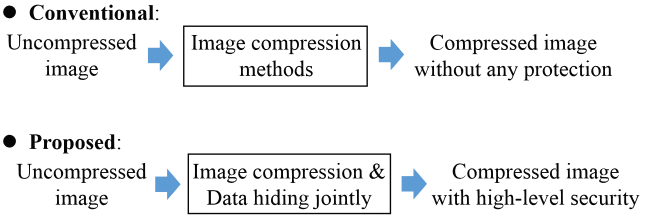


Fig. 1. Comparison between conventional compression methods (top) and the proposed method (bottom).

As shown in Figure 1, this work performs data-hiding and compression jointly. The AMBTC compression technique is selected because of its high compression efficiency. Therefore, this solution is suitable for real-time embedded system applications. By hiding data in the original image (usually referred to the host image), image quality is almost inevitably degraded. However, for applications, such as painting maintaining and photography preservation, image quality is regarded as paramount. Consequently, the aim of data hiding schemes is to not only embed additional secret data but also preserve host image quality.

Data hiding methods are usually classified into two categories, namely, frequency domain data hiding and spatial domain data hiding methods. In frequency domain data hiding, the host image is manipulated in its frequency domain to embed secret data. For example, Parah et al. [4] proposed a discrete cosine transform (DCT) modification scheme that utilizes the difference between DCT coefficients to hide data. In spatial domain data-hiding methods, the pixels of the host image are manipulated to embed authentication data. For example, Wahed and Nyeem [5] proposed a least significant bits substitution scheme to embed authentication data in the host image, where the correlation between those embeddable pixels is utilized to avoid the use of flag bits. In addition, their method has the advantage of reversible data hiding. The proposed method belongs to the spatial domain category because of its use of AMBTC.

 ISBN: 978-1-61208-674-3

II. PROPOSED METHOD

This section presents the proposed method, which hides data using two methods (namely, intra- and interblock embedding) sequentially, to increase payload as much as possible.

First, in intrablock embedding, five parameters are extracted from each block: high mean (*HM*), low mean (*LM*), number of high-mean bits (*NH*), number of low-mean bits (*NL*), and block size (*BS*). By tuning the parameters of this parameter set, a weighted function (namely, the secret data function f_{sd}) is defined as follows:

$$f_{sd} = (HM \times 1) + (LM \times 2) + (NH \times 3) + (NL \times 4) + (BS \times 5). \quad (1)$$

Meanwhile, the secret bits to be embedded are converted to their decimal representation S, e.g., $S = (10011)_2 = 19$ in the case of 5-bit secret data. The goal of intrablock embedding is to adjust the parameter set so that:

$$f_{sd} \bmod 2^n = S, \quad (2)$$

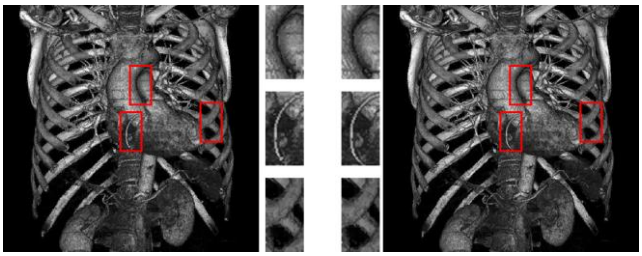
where n is the size of the secret bits hidden in each block. In this work, n is set as 5.

However, it is difficult to identify an optimal parameter set that simultaneously satisfies (2) and retains sufficient image quality. Many combinations of the parameters can lead to the result of (2) for a given 5-bit secret data. However, most of them might degrade the image quality severely. To solve this problem, a two-step search scheme is proposed. First, we set search constraints for the variation of *HM*, *LM*, and *BS*, because compared with *NH* and *NL*, these three parameters usually have a considerable effect on output image quality. Second, we adopt a halftone method, namely Direct Binary Search (DBS) method [6], to improve quality by applying a swap operation to adjust the location of high-mean and low-mean bits. In addition, also inspired by [6], the cross-correlation function is applied to accelerate the computation speed of the search procedure.

Subsequently, in interblock embedding, the difference between adjacent high-mean and low-mean values is calculated as follows:

$$\begin{cases} DH_i = HM_i - HM_{i+1} \\ DL_i = LM_i - LM_{i+1} \end{cases}, \quad (3)$$

where the subscripts i and $i+1$ denote the locations of two adjacent blocks. An additional two-bit payload is achieved by controlling the odd–even parity of DH_i and DL_i. That is, if the parity of DH_i (or DL_i) is odd, the secret code "1" is indicated, and if it is even, code "0" is indicated. Unlike using intrablock embedding alone, integration with interblock embedding can prevent discontinuity among adjacent blocks and provide extra payload with negligible quality loss.



(a) (b)

Fig. 2. Experimental results of the proposed methods using the *Artifix* test image in [7]. (a) Original grayscale image. (b) Result of the proposed method.

III. PRELIMINARY EXPERIMENTAL RESULTS

This section presents the evaluation and the experimental results of the proposed method. Six test images were selected from the online medical image database [7]. For the preliminary experiments, our experiment involved hiding data in medical images because such images are confidential and usually require security protection. As shown in Figure 2, compared with the original grayscale image (Figure 2a), the output data-embedded AMBTC image (Figure 2b) exhibits a very close visual resemblance. For the result of Fig. 2b, the Peak Signal-to-Noise Ratio (PSNR) value is 51.23. As can be seen in the enlarged version, the details are preserved and the image distortion is hardly distinguished, which validates the effectiveness of the proposed method.

IV. CONCLUSION

This paper presents a novel data hiding scheme for the AMBTC compressed images. In the past, "seeing is believing" may have been a disputable claim. Today, however, tampering or counterfeiting digital images using current technologies presents no difficulty. Large numbers of digital images are transmitted over public and non-secure networks every day, thus increasing the risk of image tampering and the scatter of untrue information. This study provided a solution for increased security in image signal transmission. In our further research, we plan to select other test image types (other than medical images) and conduct more experiments on state-of-the-art comparison methods.

REFERENCES

[1] Y. Liu, J. Guo, and Y. Cheng, "Adaptive block truncation coding image compression technique using optimized dot diffusion," IEEE Int. Conf. Image Processing (ICIP), pp. 2137–2141, Sept. 2016.

[2] Y. Hu, K. Choo, and W. Chen, "Tamper detection and image recovery for BTC-compressed images," Multimedia Tools Appl., vol. 76, pp. 15435–15463, July 2017.

[3] N. Huynh, K. Bharanitharan, C. Chang, and Y. Liu, "Minima-maxima preserving data hiding algorithm for absolute moment block truncation coding compressed images," Multimedia Tools Appl., vol. 77, pp. 5767–5783, March 2018.

[4] S. Parah, J. Sheikh, N. Loan, and G. Bhat, "Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing," Digital Signal Processing, vol. 53, pp. 11–24, June 2016.

 ISBN: 978-1-61208-674-3

[5] Md. A. Wahed and H. Nyeem, "Efficient LSB substitution for interpolation based reversible data hiding scheme," 20th Int. Conf. Computer and Information Technology, pp. 1–6, Dec. 2017.

[6] D. Lieberman and J. Allebach, "A dual interpretation for direct binary search and its implications for tone reproduction and texture quality," IEEE Trans. Image Processing, vol. 9, pp. 1950–1963, Nov. 2000.

[7] Online available (the last access date: July 2018). http://www.osirix-viewer.com/