http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

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

Information Technology Journal 10 (7): 1415-1420, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.1415.1420

An Excellent Image Data Hiding Algorithm Based on BTC

[1]Nur Mohammad, [1]Xingming Sun and [2]Hengfu Yang
[1]School of Computer Science and Communication, Hunan University, Changsha, 410082, China
[2]Department of Information Science and Engineering, Hunan First Normal University, Changsha, 410205, China

Abstract: The Development of modern communication technology, demand for digital image, audio, video and other contents transmission and storage are increasing rapidly. To protect digital product and ensure the secure transfer of the digital items become important issue in home and abroad. The researcher developed many algorithms; these are some specific fields. But can't grantee the whole safety of the contents. The Block Truncation Coding one of the effective and real time application for the hiding data compare with transform domain and other techniques. In a coding technique, a number of bits required to represent an image which needs less data store and less computation. Application of coding in the field of image processing generally concern image data compression for storage and transmission as well as feature extraction for pattern recognition. Most existing BTC-based data hiding algorithms do not fully exploit visual perception of the host images and cannot obtain high hiding capacity and visual quality. For fully exploit visual perception and high hiding capacity, an excellent data hiding scheme based on BTC is proposed. First, the BTC scheme uses a two level (one-bit) nonparametric quantizer that adapts to local properties of the image. Second we employed Human Visual System (HVS) masking characteristics which ensure high visual quality of stego image. At the last, we embedded the data into the modified bitmap of BTC. The experimental results show that the proposed algorithm has good transparency, high hiding capacity and the visual quality of stego-images is very good.

Key words: Block truncation coding, data hiding, human visual masking, transparency, quantization

INTRODUCTION

Nowadays, internet has become very popular to data transmission; such as digital context, image, video and audio (Swanson *et al*., 1998) but data transfer on internet has become unsecure. Through the internet, almost the digital content can be found and downloaded. So it is easy to be redistributed, copied and modified the digital content over the internet which renders copyright protection issues. The integrity and authenticity of digital media can be protected by using digital watermarking. The hiding data represents the ownership of the owner according to the hiding information into the original image or content. It can be applied to different applications including digital signatures, fingerprinting, broadcast and publication monitoring, authentication, copy control and secret communication (Cox *et al*., 2002). Usually, an effective data hiding scheme provides the three major properties (Hartung and Kutter, 1999): (1) Imperceptibility (2) Robustness and (3) Unambiguity. The data which is hided must be imperceptibility and invisible because of two primary concerns; firstly we should not lower the quality of the original image or it will break the aesthetic feeling and diminish the commercial value of the original image. Secondly, if the hiding data is detected by hacker, it will be easily broke or be removed. The BTC scheme, we embedded the hiding data in the modified bitmap. So it is not easy to break the imperceptibility against attacks. Hiding information should be unambiguous to prove the ownership of the owner (Hartung and Kutter, 1999). In order to improve the data hiding of the BTC (Luo *et al*., 2011) scheme, some has hided multiple data to enhance the robustness of the algorithm. It seems like that the original image has been interfered with much more noise. On the other hand, in order to keep the quality of the original image, we hide less information and high robust of the BTC scheme. Usually, there are two kinds of basic information hiding design scheme (Lu *et al*., 2000; Su *et al*., 2001), Spatial domain (Kutter *et al*., 1997; Xia *et al*., 1997; Cox *et al*., 1999) and Transform domain or frequency domain (DCT, DWT, DFT) (Hsu and Wu, 1998; Seo and Yoo, 2006). Many coefficient based image

Corresponding Author: Xingming Sun, School of Computer and Communication, Hunan University, No. 252, Lushan South Road, Yuelu District, Changsha, 410082, China Tel: 86-731-88821341 Fax: 86-731-88821341

coding scheme have developed; Such as DCT, DFT, DWT ... But very few works has done in BTC based data hiding domain. Recently research has focused more attention on Block truncation Coding technique. Although BTC is designed to compress gray rather than color images, the same procedure can be applied to color images. Unfortunately, the compression ratio is not the same when BTC is used to compress a color image because a color image is composed of three planes, R, G and B and these three planes form three bitmaps when BTC is used (Chang *et al*., 2008). So, we choice the gray level image to enhance the research algorithm. If we can hide the secret information in the modified codes (Hong *et al*., 2009) of a host image, instead of that original host image then the efficiency for data transmission can be improved. But we need to insure that if the unauthorized receiver decodes the compression code according to the original rules of BTC compression decoding or the unauthorized receiver fails to decode through original BTC compression decoding rule, they may try to develop the suspicious possible BTC compression decoding to detecting the secret information. If secret information is detectable by the unauthorized then the solution of information hiding is damage. In this paper, a secret information hiding into the modified codes based on BTC compression of a host image is proposed. We used Human Visual System (HVS) model (Abdulfetah *et al*., 2010) ensure high quality of Stego image (Hong *et al*., 2010) and hiding adaptive values of secret data to enhance the security of illegal detection. The proposed method, a uniform block has the capacity embed sixteen bits into its bit matrix and increase the embedding capacity doesn't lose the image quality (Keissarian, 2010). Only the authorize receiver can decode the secret information using the modified BTC bitmap key. The experimental results, this part consist of transparency test, hiding capacity test and performance comparison.

BASIC PROCESS OF BLOCK TRUNCATION CODING

BTC is a block based lossy image compression technique for gray-level images, which is proposed in early 1979 (Delp and Mitchell, 1979). In BTC an image is segmented into n×n non overlapping blocks of pixels, and a two-level (one-bit) (Lv and Lu, 2011) quantizer is independently designed for each block. BTC is use real time application so it is more efficient than spatial domain and transform domain. The average value ($\bar{x}$) and the standard deviation (δ) are calculated for each block and setting up first two expressions which indicate the moment before and after quantization. The original image block is encoded into a bitmap (Fig. 1). The pixels which values are lees than mean value is set as "0" and the pixels which value are greater than or equal to mean values are set as "1". For "0" we use 'm' and for "1" we use "n". Let say, xth = ($\bar{x}$); if xi = xth , then set n (1) and if xi = xth then set m (0).

In BTC process; we can calculate the average value as below Eq:

$$\bar{x} = \frac{1}{n^2}\sum_{n} x_i \tag{1}$$

where, n is the total number of pixels and x_i is the total sum of the Pixel. I where, (i = 1, 2,3, ..., n). As the Eq. 1 the average value ($\bar{x}$) is calculated. And the standard deviation is:

$$\sigma = x^2 - \overline{x^2} \tag{2}$$

where, a bit plane of "0" and "1" is formed by assigning 1 to those greater than or equal to mean and 0 to those less than mean. For the selection of quantization level, we can use Eq. 3 and 4. First level quantization:

$$n^2\bar{x} = n^- x^- - n^+ x^+ \tag{3}$$

where, n^+ is the number of pixels above the mean value and is the number of pixel below mean value.

Second level quantization:

$$n^2\overline{x^2} = n^-(x^-)^2 - n^+(x^+)^2 \tag{4}$$

Calculate the value before and after quantization, using Eq. 5 and 6:

$$x^+ = \bar{x} + \sigma\sqrt{\frac{n^-}{n^+}} \tag{5}$$

$$x^- = \bar{x} - \sigma\sqrt{\frac{n^+}{n^-}} \tag{6}$$

According to Eq. 5 and 6, we can calculate x^- and x^+.

HUMAN VISUAL SYSTEM MODEL

Designing image adaptive data hiding schemes with human visual perception can obtain higher capacity and lower distortion. In this approach, we exploit the luminance masking and texture masking features of the high order image generated by extracting high order bits of the original BTC image and create HVS masking model

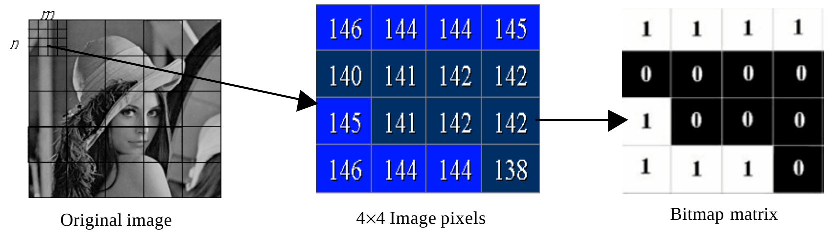

Fig. 1: An example of BTC process

in a better way and then use the visual masking model to develop an adaptive data hiding scheme. Human eyes usually have different sensitivity to different luminance. In fact, human eyes are more sensitive to changes in the areas with middle level luminance, while less sensitive to changes in those areas with high and low gray-scale values (Barni *et al*., 2001). So, the texture masking of each pixel can be estimated as:

$$\alpha = \frac{\left|X^{+} - X^{-}\right|}{255} \tag{7}$$

where, x^+ and x^- are the lowest and highest value of BTC pixel.

For the luminance masking, we can use the following formula:

$$\beta = \frac{\left|\frac{(X^{+} + X^{-})}{2} - 127.5\right|}{127.5} \tag{8}$$

Based on all the above considerations, the effect of HVS masking characteristics is expressed by the formula:

$$\lambda = \alpha \times \beta \tag{9}$$

IMAGE DATA HIDING ALGORITHM BASED ON BTC

To achieve good transparency, high hiding capacity and quality stego image the luminance masking and texture masking was utilized to develop a BTC domain HVS model. Then a gray level image divided into a blocks. After that every block divided into 4x4 bits map. Figure 1 shows the bits map of blocks. For each block, we transmit bit-level matrix and calculated the standard deviation and average value. The levels X^+ and X^- can be determined by setting up the expressions that indicate the moments before and after quantization. Details of data embedding are described as follows:

Step 1: The original bit matrix transmitted by two levels quantization and got the modified bit matrix which we plan to embed the hiding data

Step 2: We embed a binary image into the modified bitmap of the host image. Binary image modify binary sequence P

Step 3: Use key1 to generate a watermark sequence P

$$P = \{p(i) | p(i) \in (-1,1), i = 1, 2, \cdots n\} \tag{10}$$

Step 4: Utilize Eq.10 to modify as binary form of the sequence P and then a watermark sequence W is generated, where:

$$W = \{w(i) | w(i) \in \{0,1\}, i = 1, 2, \cdots n\} \tag{11}$$

And adopt Eq. 12:

$$w(i) = \begin{cases} 1, & p(i) \geq 0 \\ 0, & p(i) < 0 \end{cases} \tag{12}$$

Step 5: Calculate the HVS model's texture masking and luminance masking factor of each pixel of original cover image on the based on Eq. 9

Step 6: Define following rules of embedding message

$$\text{if } 0 \leq \lambda_i \leq \frac{1}{4} \tag{13}$$

Moderate activity detected and 4x4 blocks are used. All (two 8 bit) value is used in the bitmap:

$$\text{if } \frac{1}{4} \leq \lambda_i \leq \frac{1}{2} \tag{14}$$

A low activity region is detected and 4x4 blocks are used. Only half (one bit) value is used in the bitmap:

$$\text{if } \frac{1}{2} \leq \lambda_i \leq 1 \tag{15}$$

Two quantization level detected and 4x4 blocks are used. Embed watermark in to two quantization level.

EXPERIMENT RESULTS

We have tested the performance of the proposed BTC based data hiding scheme through a computer simulation on six gray level images (Fig. 2) . These images are 8 bits per pixel and 512 x 512 pixels in size. The simulation platform is Microsoft Windows XP, Pentium IV and the proposed scheme is implemented using Matlab. Three performance matrices are used to measure the performance of the proposed BTC based data hiding scheme; hiding capacity, image quality (PSNR) of BTC image and Stego BTC image. Resulting Table 1; BTC image (PSNR), Stego BTC image (PSNR) and Embedding capacity (Kbyte). It can be observed that big amount of the transmitted code is used to embed data, yet keeping a satisfactory image quality. To further investigate the performance of the proposed scheme, we compared the stego-image quality and the hiding capacity of the proposed scheme with Keissarian (2010) scheme. Table 2, for comparison of our results with Keissarian (2010) results. At the end Fig. 3 ; the visual quality of Original image, BTC Compress image and Stego BTC image. The visual quality of the test image is very good and hiding capacity is higher than previous proposed method. As mentioned previously, since a uniform block is reconstructed by replacing all the block pixels by the bitmap matrix mean ($\bar{x}$), the quality of reconstructed block will be the same in previous quality.

CONCLUSION

In this study, we proposed a new data hiding technique, which can be applied to hide not only one bit secret data but also several bit secret data. To reduce the number of bits needed for a data hiding a host image, the secret images are compressed using BTC with HVS model. Then the encrypted message is hided into the host image modified bitmap. From the experimental results of Section 4, we find that when we apply our scheme to 'a gray level image for hiding another gray level image', the average PSNR value of secret images is 31.60dB. Compared to the [10] image compression is 31.25 dB, which is quite acceptable for viewing the messages with the naked eye. In addition, when we apply our scheme to a gray level image hiding secret data, we find the average hiding capacity 40.00 kbyte. The scheme can maintain the high quality of embedding capacity into the host image in summary, our scheme increases the number of embedded secret data and also ensures the quality of the host image and the retrieved secret image. In addition, the hidden images can be safely protected in this scheme because the HVS model is employed. Therefore, our scheme not only increases the data transmission performance but also is very suitable for protecting valuable content in the current on-line trading environment.

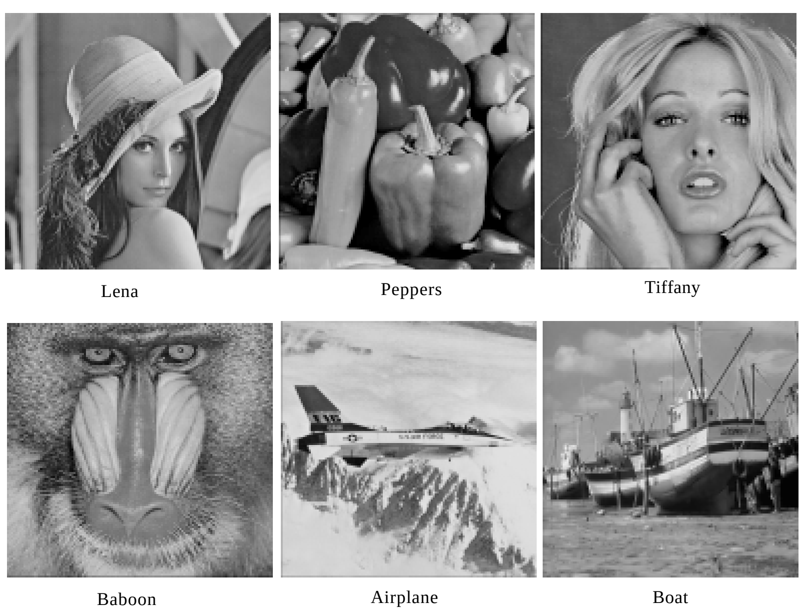

Fig. 2: Test Images; Lena, Peppers, Tiffany, Baboon, Airplane and Boat

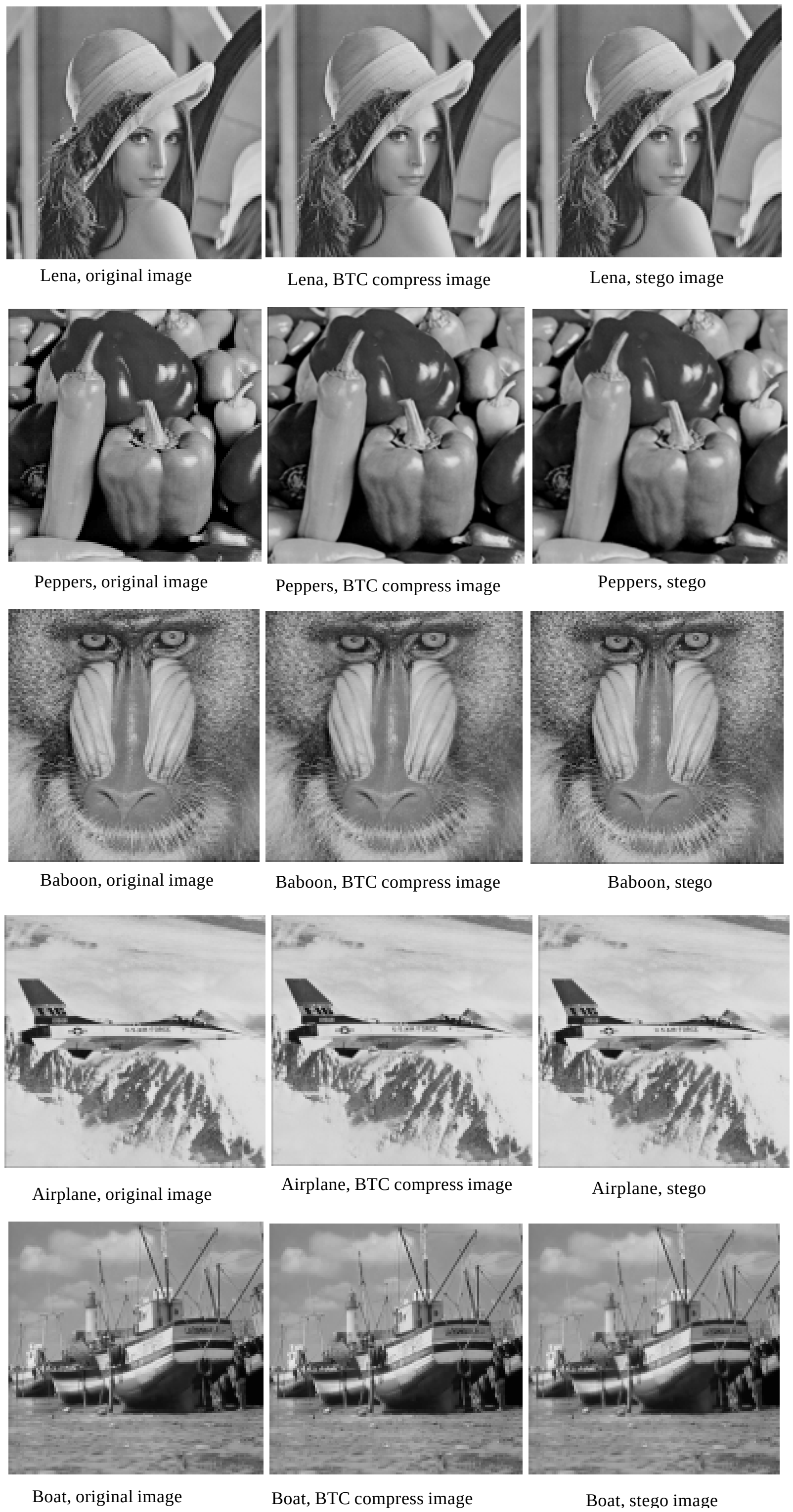

Fig. 3: Original Image, BTC Compress Image and Stego Iamge of Lena, Peppers, Tiffany, Baboon, Airplane and Boat

Table 1: PSNR values (dB) of BTC compressed image and Stego images and Embedding capacity of hiding data

Image	BTC compressed image (PSNR)db	Stego BTC image (PSNR)db	Embedding capacity (kbyte)
Lena	33.23	32.02	29.67
Peppers	33.20	31.12	32.66
Tiffany	32.49	30.27	26.99
Baboon	27.01	26.09	52.09
Plane	31.98	30.01	29.57
Boat	31.27	29.51	39.62

Table 2: Compare present method with Keissaerian (2010) methods (10)

Image	Present method	Keissarian (2010) method	Difference
Lena			
Hiding capacity (kbyte)	29.67	26.76	2.91
BCT image (PSNR)dB	33.23	nil	nil
Stego image (PSNR)dB	32.21	31.28	0.93
Peppers			
Hiding capacity (Kbyte)	32.66	28.16	4.50
BCT compression (PSNR)	33.20	nil	nil
Stego image (PSNR)	31.12	31.34	-0.22

ACKNOWLEDGMENTS

This study is supported by the National Natural Science Foundation of China (61073191, 61070196, 60973128, 60973113, 60873198, 60736016), National Basic Research Program 973 (2009CB326202, 2010CB334706), Hunan Provincial Natural Science Foundation of China (10JJ6090).

REFERENCES

Abdulfetah, A.A., X. Sun, H. Yang and N. Mohammad, 2010. Robust adaptive image watermarking using visual models in DWT and DCT domain. Inform. Technol. J., 9: 460-466.

Barni, M., F. Bartolini and A. Piva, 2001. Improved wavelet-based watermarking through pixel-wise masking. IEEE Trans. Image Process., 10: 783-791.

Chang, C.C., C.C. Lin, C.H. Lin and Y.H. Chen, 2008. A novel secret image sharing scheme in color images using small shadow images. Inform. Sci., 178: 2433-2447.

Cox, I.J., M.L. Miller and A.L. McKellips, 1999. Watermarking as communications with side information. IEEE Proce., 87: 1127-1141.

Cox, I.J., M.L. Miller and J.A. Bloom, 2002. Digital Watermarking. Morgan Kaufmann Publishers, San Francisco, USA.

Delp, E. and O. Mitchell, 1979. Image compression using block truncation coding. IEEE Trans. Commun., 27: 1335-1342.

Hartung, F. and M. Kutter, 1999. Multimedia watermarking techniques. Proc. IEEE, 87: 1079-1107.

Hong, W., J. Chen and T.S. Chen, 2009. Blockwise reversible data hiding by contrast mapping. Inform. Technol. J., 8: 1287-1291.

Hong, W., T.S. Chen, K. Y. Lin and W.C. Chiang, 2010. A modified histogram shifting based reversible data hiding scheme for high quality images. Inform. Technol. J., 9: 179-183.

Hsu, C.T. and J.L. Wu, 1998. Multiresolution watermarking for digital images. IEEE Trans. Circuits Syst. II: Analog Digital Signal Process., 45: 1097-1101.

Keissarian, F., 2010. Hiding secrete data in compressed images using histogram analysis. Proceedings of the 2nd International Conference on Computer and Automation Engineering, Feb. 26-28, Singapore, pp: 492-496.

Kutter, M., F. Jordan and F. Bossen, 1997. Digital signature of color images using amplitude modulation. Proceedings of the SPIE Electronic Imaging, Storage and Retrieval for Image and Video Databases, Feb. 13, San Jose, CA, USA., pp: 518-526.

Lu, C.S., S.K. Huang, C.J. Sze and H.Y. Liao, 2000. Cocktail watermarking for digital image protection. IEEE Trans. Multimedia, 2: 209-224.

Luo, H., Z. Zhao and Z.M. Lu, 2011. Joint secret sharing and data hiding for block truncation coding compressed image transmission. Inform. Technol. J., 10: 681-685.

Lv, M.L. and Z.M. Lu, 2011. Multipurpose perceptual image hashing based on block truncation coding. Inform. Technol. J., 10: 207-212.

Seo, J.S. and C.D. Yoo, 2006. Image watermarking based on invariant regions of scale-space representation. IEEE Trans. Signal Process., 54: 1537-1549.

Su, P.C., H.Y.M. Wang and C.C.J. Kuo, 2001. An integrated approach to image watermarking and JPEG-2000 compression. J. VLSI Signal Process, 27: 35-53.

Swanson, M.D., M. Kobayashi and A. H. Tewfik, 1998. Multimedia data-embedding and watermarking technologies. Proc. IEEE, 86: 1064-1087.

Xia, X.G., C.G. Boncelet and G.R. Arce, 1997. A multiresolution watermark for digital images. Proc. IEEE Int. Conf. Image Process., 1: 548-551.