International Journal of Security and Its Applications
Vol.8, No.2 (2014), pp.301-314
http://dx.doi.org/10.14257/ijsia.2014.8.2.31

Reversible Data Hiding Scheme for BTC-compressed Images Based on Histogram Shifting

Chun-Chi Lo[1], Yu-Chen Hu[2], Wu-Lin Chen[2] and Chang-Ming Wu[3]

[1]*Department of Computer Science and Information Engineering, Providence University, Taiwan (Republic of China)*
[2]*Department of Computer Science and Information Management, Providence University, Taiwan (Republic of China)*
[3]*Department of Electronic Engineering, Chung Yuan Christian University, Taiwan (Republic of China)*
cclo@pu.edu.tw, ychu@pu.edu.tw, wlchen@pu.edu.tw, cmwu@cycu.edu.tw

Abstract

In this paper, we proposed a novel reversible data hiding scheme for the compressed images for block truncation coding (BTC). In this scheme, the secret data is embedded into the compressed codes of BTC. The histogram shifting technique is employed in the proposed scheme to embed the secret data into the quantization levels of the compressed codes. After the data embedding procedure is executed, the embedded compressed codes still follow the standard format of BTC. The experimental results reveal that the proposed scheme provides good image quality of the embedded image.

Keywords: *reversible data hiding, block truncation coding, image compression, histogram shifting*

1. Introduction

Digital data communication over the Internet has become more and more popular due to the rapid and continuous development of the networking technologies. The Internet is a public but insecure channel. The security problems such as interception, modification, and duplication become an important issue for digital data communication via the Internet. Data hiding techniques [1-9] can be used to endorse the security and secrecy of the transmitted information.

Basically, data hiding schemes can be classified in spatial domain schemes, frequency domain schemes, and compressed domain schemes. The spatial domain schemes and the frequency domain data hiding schemes embed the secret data into the pixels and the transformed coefficients of the digital images in raw format, respectively. The compressed domain data hiding schemes embed the secret data into the compressed codes of the original cover images. Typically, the hiding capacity of one compressed domain data hiding scheme is less those of the spatial domain and frequency domain data hiding schemes.

In addition, data hiding schemes can be classified into two categories: irreversible data hiding schemes [1-5] and reversible data hiding schemes [6-15]. In the irreversible data hiding schemes, secret data is first embedded into the original cover images to generate the stego-images. Then, secret data can be extracted when it is needed by executing the secret extraction procedure. However, the original cover images cannot be restored. On the contrary, the reversible data hiding schemes can extract the secret data, and recover the original cover images simultaneously. In general, the hiding capacity of the reversible data hiding scheme is less that of the irreversible data hiding scheme. But, the image

ISSN: 1738-9976 IJSIA

quality of the embedded image of reversible data hiding scheme is better than that of the irreversible data hiding scheme.

The reversible data hiding schemes are also called the lossless data hiding schemes. Two main approaches of the reversible data hiding schemes had been introduced. They are the histogram shifting approach [10-13] and the difference Expansion approach [14-15]. Some reversible data hiding schemes that use the mix of these two approaches had also been proposed.

In 2006, Ni *et al.*, proposed the reversible data hiding scheme based on histogram shifting [10]. In this scheme, the histograms of the pixels in the cover image are explored. The pairs of the peak points and the zero points are searched. The pixels between the peak and zero pair are modified in the embedding processing. Each pixel in the peak point is used to embed 1-bit secret data. The others are modified and no secret data are embedded. In this scheme, the number of pixels in the peak point is the maximal hiding capacity for the secret data to be embedded. More of the peak and zero pairs are selected to increase the hiding capacity. Tsai *et al.*, proposed an improved data hiding scheme based on histogram shifting [11] in 2009. In this scheme, the cover image is divided into non-overlapping image blocks. Each pixel in the block is processed by using the linear prediction technique to generate the predicted errors. The residual histogram of the cover image is employed to embed the secret data. This scheme provides much higher hiding capacity than that of the traditional histogram shifting data hiding scheme. In addition, Tsai proposed the reversible data hiding scheme [12] for the compressed images of the vector quantization technique in 2009. In this scheme, the histogram shifting technique is employed to embed the secret data into the histogram of the indices of the compressed image blocks.

In 2003, Tian proposed the difference expansion data hiding scheme [14]. In this scheme, the redundancy of the pixels was explored to achieve a high hiding capacity. Each pair of the two neighboring pixels is used to embed at most 1-bit secret data. The difference and average values of two neighboring pixels in each pair are calculated. The secret data to be embedded is appended to the difference value represented as a binary number. In other words, the difference value is first multiplied with 2. Then the addition of the difference value and 1-bit secret data is calculated. The calculated result is stored in the modified difference value. Two modified neighboring pixels are replaced with the summation and subtraction of the average value.

In this paper, we design a reversible data hiding scheme for the BTC-compressed images. The proposed scheme intends to embed the secret data into the quantization levels of the compressed image blocks. The embedded results will still satisfy the compressed format of the BTC scheme. In other words, it is hard to find out that the secret data is transmitted via the embedded image. The rest of this paper is organized as follows. We will review some block truncation coding schemes in Section 2. Section 3 will present the proposed scheme. The experimental results will be discussed in Section 4. Finally, some discussions and conclusions will be given in Section 5.

2. Review on Absolute Moment Block Truncation Coding

The block truncation coding (BTC) scheme [16-23] is a commonly used image coding method for digital images. In 1979, the block truncation coding scheme [16] was first proposed by Delp and Ritcell for grayscale image compression. It is also called the moment-preserving block truncation coding (MPBTC) scheme because it preserves the first and second moments of image blocks. In addition, the absolute moment block truncation coding (AMBTC) [17] had been proposed to preserve the sample mean and the sample first absolute central moment in 1984. AMBTC can be applied to the compression of the grayscale and color images. It is proved that AMBTC provides better reconstructed image quality than MPBTC when the squared Euclidean distance measurement is

employed. We shall describe the image encoding procedure and the image decoding procedure of the AMBTC scheme in the following.

The BTC scheme has very simple image encoding/decoding procedures and requires little computational complexity. It can be applied to the compression of monochrome images, moving imagery, color imagery [17], and graphics. The main problem of the BTC scheme is that its compression ratio is low. From the literature, some image coding methods [18-22] that aim to raise the compression ratio of BTC had been proposed. In this section, the AMBTC scheme will be introduced. In addition, the search of the optimal threshold for pixel group in BTC had also been proposed [23]. From the literature, some multimedia application based on BTC such as hybrid image coding, [24-25], progressive image transmission [26], data hiding [27-28], and image authentication [29-31] had been proposed.

2.1. The Image Encoding Procedure of AMBTC

Each grayscale image to be compressed is divided into a set of non-overlapping image blocks of $n \times n$ pixels. Each $n \times n$ image block can be viewed as an image vector of k dimensions, where $k = n \times n$. Each image block is sequentially processed in the order of left-to-right and top-to-down.

To compress each image block x, the mean value ($\bar{x}$) is calculated according to the following equation:

$$\bar{x} = \frac{1}{k}\sum_{i=1}^{k} x_i . \tag{1}$$

To generate the bit map (*BM*) of x, all the pixels in x are classified into two groups according to $\bar{x}$. If the intensity of one pixel is less than $\bar{x}$, it is classified as the first group and a corresponding bit with value 0 is stored in *BM*. Otherwise, it is classified as the second group and a corresponding bit with value 1 is stored in *BM*.

After the bit map of the image block is generated, these two quantization levels for these two groups are to be generated. Pixels in the same group will be encoded by the same quantization level. Let a and b denote the quantization levels in the first and the second groups, respectively. These two quantization levels can be computed according to the following equations:

$$a = \frac{1}{k-q} \times \sum_{x_i < \bar{x}} x_i \text{ , and} \tag{2}$$

$$b = \frac{1}{q} \times \sum_{x_i \geq \bar{x}} x_i \text{ .} \tag{3}$$

Here q stands for the number of pixels whose values are greater than or equal to $\bar{x}$.

Each compressed image block forms a trio (a, b, *BM*) where each quantization level is stored in 8 bits. A total of (8+8+k) bits are needed to store the compressed codes (a, b, *BM*) of each compressed block in the AMBTC scheme. The required bit rate of MPBTC equals (8+8+k)/k bpp. For example, the bit rate of the AMBTC scheme equals 2 bpp when the block size k is set to 16.

An example of the image encoding procedure is described in the following. Figure 1 shows the original image block of 4×4 pixels. The block mean value is first computed by using Eq. (1). In this example, the block mean value equals 122.125. The bit map generated by AMBTC is shown in Fig. 2. Then, the quantization levels for these two groups are then calculated by using Eqs. (2) and (3), respectively. These two quantization levels are 82 and 147, respectively. Finally, the compressed trio (94, 158, $(1000100011001110)_2$) is sent to the receiver.

132	97	70	60
152	124	92	75
170	144	130	99
183	168	145	125

Figure 1. Image Block of 4×4 Pixels

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

Figure 2. The Resultant Bit Map of the AMBTC Scheme

2.2. The Image Decoding Procedure of AMBTC

In the image decoding procedure, each image block is to be rebuilt by using the received trio (*a*, *b*, *BM*). One pixel is reconstructed by quantization level *a* if a corresponding bit valued 0 is found in the bit map *BM*. Otherwise, it is recovered by quantization level *b*. After each pixel is recovered by either the quantization level *a* or *b* according to its retrieved bit map, the image block is then reconstructed. When each image block is sequentially recovered by using the above-mentioned steps, the whole compressed image of the AMBTC scheme can be generated.

An example of the image decoding procedure is described in the following. The compressed trio (94, 158, $(1000100011001110)_2$) is received. To recover each pixel, each bit in of the bit map is sequentially checked to recover the compressed pixel and the reconstructed image block is shown in Figure 3. In this example, the mean squared error (MSE) between the original image block as shown in Figure 1 and the rebuilt image block as shown in Figure 3 equals 390.875.

158	94	94	94
158	94	94	94
158	158	94	94
158	158	158	94

Figure 3. The Reconstructed Image Block of the AMBTC Scheme

3. The Proposed Scheme

The goal of the proposed scheme is to losslessly embed the secret data into the compressed codes of BTC. The proposed scheme is based on the histogram shifting technique. The embedded results should still in the standard compressed format of BTC so that the illegal user cannot easily find out the existence of the secret data. The proposed scheme consists of the secret data generation procedure, the data embedding procedure, and the data extraction procedure.

3.1. The Secret Data Generation Procedure

To generate the secret data, the pseudo random number generator (PRNG) with a predefined seed is used. Each random value *rv* induced by the random seed is converted to the 1-bit secret data using the following equation:

$$sd = rv \bmod 2. \quad (4)$$

By using Eq. (4) mentioned above, we can generate the required number of secret data that will be embedded into the compressed codes of the BTC-compressed image with the specific random seed.

An example of secret data generation is described in the following. Suppose we want to generate 25 authentication codes. We need to choose the random seed that is used to induce the random number sequence. Suppose the random seed is set to 2013. The first 25 random values induced by the random seed are listed in Figure 4(a). The corresponding 1-bit secret data is listed in Figure 4(b).

6612	17381	2551	10783	29949
19216	15041	5153	21529	8088
3030	18462	2219	15747	30576
19578	24669	22884	18219	20081
30020	32651	1638	23282	21348

(a) Random values

$(0)_2$	$(1)_2$	$(1)_2$	$(1)_2$	$(1)_2$
$(1)_2$	$(1)_2$	$(1)_2$	$(1)_2$	$(0)_2$
$(0)_2$	$(0)_2$	$(1)_2$	$(1)_2$	$(0)_2$
$(0)_2$	$(1)_2$	$(0)_2$	$(1)_2$	$(1)_2$
$(1)_2$	$(1)_2$	$(1)_2$	$(1)_2$	$(1)_2$

(b) 1-bit secret data

Figure 4. Example of Secret Data Generation

3.2. The Data Embedding Procedure

Suppose the grayscale image of $W \times H$ pixels had been already compressed by the BTC scheme with the block size is set to $n \times n$. A total of $w \times h$ compressed image blocks of BTC are generated where $w = W/n$ and $h = H/n$. In other words, the compressed codes of the images are these $w \times h$ trios of (a, b, BM).

Let (a_i, b_i, BM_i) denote the compressed trio of i-th image block where a_i and b_i are these two quantization levels and BM_i is the bit map. All the smaller quantization level of each compressed block are collected to form the set QLA where $QLA=\{a_1, a_2, \ldots, a_{w \times h}\}$. Similarly, all the other quantization level of each compressed are collected to generate the set QLB where $QLB=\{b_1, b_2, \ldots, b_{w \times h}\}$. In addition, the difference value dv_i between the two quantization levels a_i and b_i is first computed:

$$dv_i = b_i - a_i. \tag{5}$$

All the difference value of each compressed block are collected to form the set DV where $DV=\{dv_1, dv_2, \ldots, dv_{w \times h}\}$.

There are three choices to embed the secret data in the above three sets by using the histogram shifting technique.

Choice 1: Embed the secret data into QLA and QLB.
Choice 2: Embed the secret data into QLA and DV.
Choice 3: Embed the secret data into DV and QLB.

The flowchart to embed the secret data into the selected data set by using the histogram shifting technique is listed in Figure 5. Let DS_1 and DS_2 denote the two data sets that are selected to embed the secret data. To process each data set by using the histogram shifting technique with PNO pair of peak and zero points, these PNO pair of peak and zero points should be determined first. If PNO pair of peak and zero points can be found, the maximum hiding capacity (mhc) of the histogram shifting technique with the use of PNO pair is then determined. Otherwise, the data embedding process is terminated because we cannot find enough pair of peak and zero points. The histogram of the data set is shifted and the secret data of mhc bits is extracted. The secret data is then embedded to generate the embedded data set.

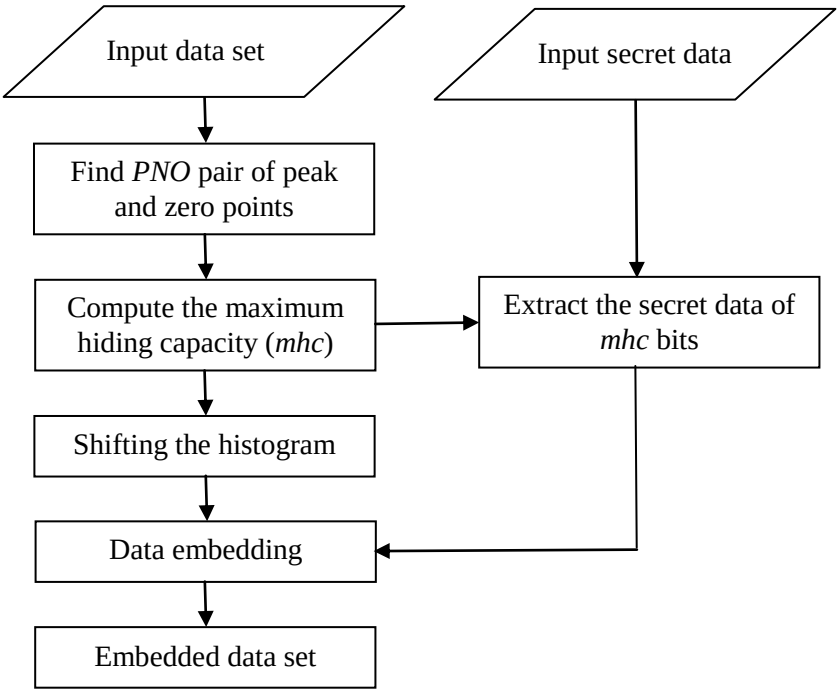


Figure 5. Flowchart of the Data Embedding Process for the Selected Data Set

When the first choice is employed in selecting the two data sets, no change should be made for these two modified data sets. When the second or third choices is employed in selecting the data sets, additional data converting process should be executed to genera the modified quantization levels. The modified quantization level b_i' of the *i*-th image block for the second choice can be computed as follows.

$$b_i' = a_i' + dv_i'. \quad (6)$$

Here, a_i' and dv_i' denotes the modified quantization level and the modified difference value of the *i*-th image block, respectively.

Similarly, the modified quantization level a_i' of the *i*-th image block for the third choice can be computed as follows.

$$a_i' = b_i' - dv_i'. \quad (7)$$

When the two data sets DS_1 and DS_2 are sequentially processed by the above mentioned process, the modified data sets are generated. The modified data sets can then be converted back to the two sets of quantization levels. Therefore, the embedded results of the proposed scheme follow the standard compressed format of AMBTC.

The hiding capacity of the proposed scheme equals mhc_1+mhc_2 where mhc_1 and mhc_2 are the maximum hiding capacity of DS_1 and DS_2, respectively. The choice of the selection of the two data sets should be privately transmitted to the receiver. Also, these *PNO* pair of peak and zero points should be transmitted to the receiver by using a secure channel.

3.3. The Data Extraction Procedure

The goal of the data extraction procedure is to extract the secret data, and recover the original compressed codes simultaneously. Some system parameters, such as *W*, *H*, *n*, *PNO*, and the pair of peak and zero points for these two data sets should be available. In addition, the choice used in generating the two data sets should be known and the BTC

compressed codes of the image are required. The compressed image consists of $w \times h$ trios of (a, b, BM) where w and h equal W/n and H/n, respectively.

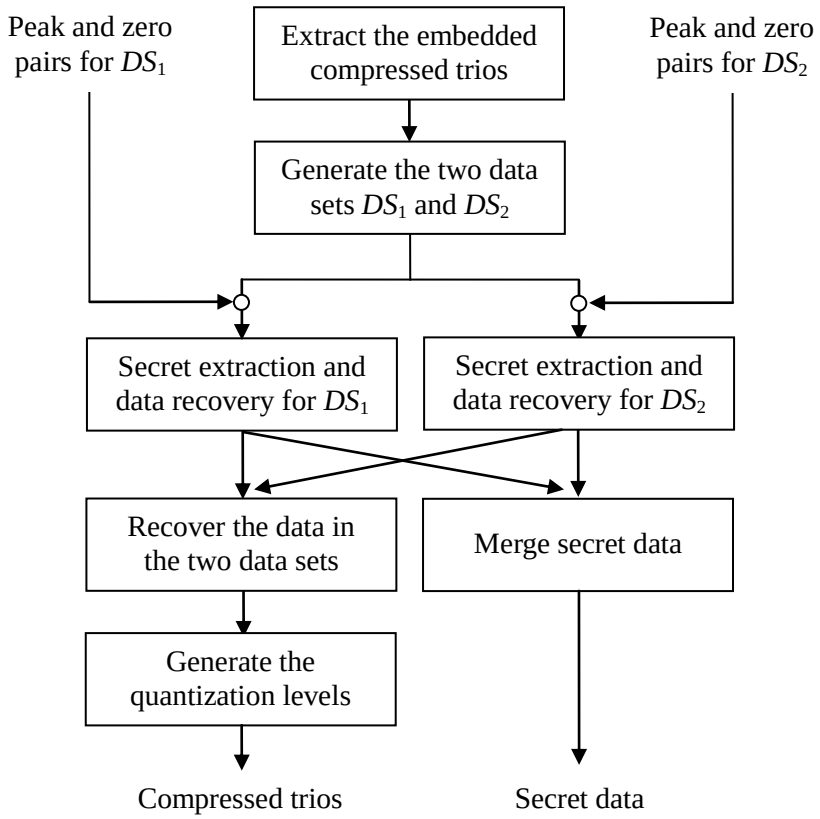


Figure 6. Flowchart of the Data Extraction Procedure

The flowchart of the data extraction procedure is shown in Figure 6. To extract the secret data, the embedded compressed codes are extracted. According to the choice that was used in the data embedding procedure, the two embedded data sets EDS_1 and EDS_2 are generated. By using PNO pair of peak and zero points, the secret data of mhc_1 bits that was embedded into EDS_1 can be extracted and the original data set DS_1 is then recovered. Similarly, the secret data of of mhc_2 bits that was embedded into EDS_2 can be extracted by using PNO pair of peak and zero points, and the original data set DS_2 is then recovered.

By merging the secret data extracted from EDS_1 and EDS_2, secret data of mhc_1+mhc_2 bits are now generated. In addition, the data sets DS_1 and DS_2 are now recovered. The two data sets are now used to generate the two sets QLA and QLB of quantization levels.

When the first choice was used in generating the DS_1 and DS_2, QLA and QLB are set to DS_1 and DS_2, respectively. When the second or third choices is employed to generate the DS_1 and DS_2, additional data converting process that is similar to that of the data embedded procedure will be executed to generate the quantization levels of each compressed image block. The quantization level b_i of the i-th image block for the second choice can be computed as follows.

$$b_i = a_i + dv_i. \tag{8}$$

Similarly, the quantization level a_i of the i-th image block for the third choice can be computed as follows.

$$a_i = b_i - dv_i. \tag{9}$$

After the quantization levels of each image block are generated, the compressed codes of the image block by using BTC is now recovered.

4. Experimental Results

To verify the efficiency of the proposed scheme, several simulations are performed on windows 7 PC with an Intel Core™ i5 2.80GHz CPU and the 2GB RAM. The program language used to do the simulation is Bloodshed Dev C++ Version 4.9.9.2. In the simulation, the AMBTC scheme instead of the MPBTC scheme is employed because the AMBTC scheme is proved to be the optimal scheme under the squared Euclidean distance measurement. In the simulations, eight grayscale images of 512×512 pixels "Airplane", "Boat", "Girl", "Goldhill", "Lenna", "Pepper", "Sailboat" and "Toys", as shown in Figure 7.

Table 1. Reconstructed Image Qualities of the AMBTC Scheme

Block size / Images	2×2 (5 bpp)	4×4 (2 bpp)	8×8 (1.25 bpp)
Airplane	40.747	33.266	30.141
Boat	39.450	31.961	28.975
Girl	41.921	34.763	31.057
Goldhill	41.316	33.694	30.293
Lenna	40.657	33.692	30.247
Pepper	41.456	34.069	30.247
Sailboat	38.078	31.176	28.125
Toys	41.152	33.235	30.098
Average	**40.597**	**33.232**	**29.898**

Table 1 lists the experimental results of the reconstructed image qualities of the AMBTC scheme with different block sizes. It is shown that the reconstructed image quality decreases with the increase of the block size. Average image qualities of 40.597 dB, 33.232 dB, and 29.898 dB are achieved by the AMBTC scheme when the block sizes are set to 2×2, 4×4, and 8×8, respectively. The bit rates of the AMBTC scheme equal 5 bpp, 2 bpp, and 1.25 bpp when the block sizes are set to 2×2, 4×4, and 8×8, respectively. According to the results, the AMBTC scheme with the block size of 4×4 pixels is selected to evaluate the performance of the proposed scheme. By doing so, the image quality embedded results of the proposed can be approximately close to 30 dB.

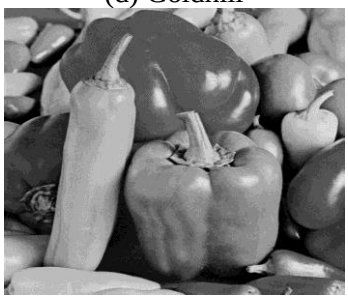
(a) Airplane

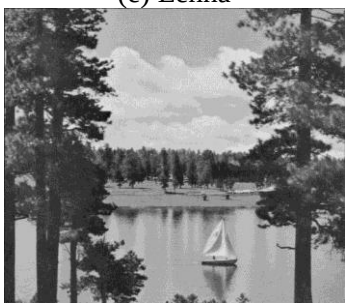

(b) Boat


(c) Girl


(d) Goldhill


(e) Lenna


(f) Pepper


(g) Sailboat

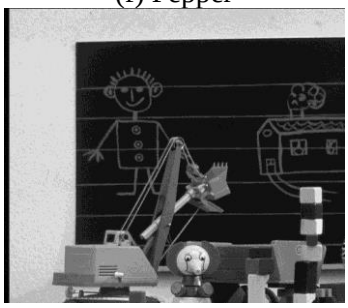

(h) Toys

Figure 7. Grayscale Testing Images of 512×512 Pixels

Table 2 lists the number of the zero points of the AMBTC scheme when the block size set to 4×4. There are 16384 compressed trios of (*a*, *b*, *BM*) for each 512×512 grayscale image that is compressed by the AMBTC scheme with the block size of 4×4 pixels is used. In other words, the size of each data size is of 16384 elements. The possible values in each data set are 0, 1, 2, …, 255. Average numbers of 53.625, 52.875, and 126.875 zero points are found in *QLA*, *QLB*, and *DV*, respectively.

Table 2. Total Number of the Zero Points of the AMBTC Compressed Data

Data Set / Images	*QLA*	*QLB*	*DV*
Airplane	79	79	136
Boat	52	50	138
Girl	61	56	118
Goldhill	38	42	154
Lenna	58	55	132
Pepper	42	40	118
Sailboat	61	69	128
Toys	38	32	91
Average	**53.625**	**52.875**	**126.875**

The accumulated hiding capacities of *QLA* by using the histogram shifting technique are listed in Table 3. The accumulated hiding capacity increases as the increase of the *PNO* value. Average accumulated hiding capacity of 367.625 and 689.75 bits are obtained when the *PNO* values are set to 1 and 2, respectively. Severn out of eight images can find 3 pair of peak and zero points. However, difference value of the accumulated hiding capacity between 2 pair and 3 pair are quite small.

Table 3. Accumulated Hiding Capacities (unit: bits) of *QLA* by using the Histogram Shifting Technique

PNO / Images	*PNO* = 1	*PNO* = 2	*PNO* = 3	*PNO* = 4	*PNO* = 5
Airplane	569	1005	N/A	N/A	N/A
Boat	358	701	703	704	705
Girl	313	596	697	N/A	N/A
Goldhill	218	406	407	N/A	N/A
Lenna	196	386	387	N/A	N/A
Pepper	212	417	419	N/A	N/A
Sailboat	325	613	616	618	619
Toys	750	1394	1396	1397	N/A
Average	**367.625**	**689.75**	**N/A**	**N/A**	**N/A**

Table 4 lists the accumulated hiding capacities of *QLB* by using the histogram shifting technique. Similarly, the accumulated hiding capacity increases as the increase of the *PNO* value. Average accumulated hiding capacity of 377.5 and 720 bits are obtained when the *PNO* values are set to 1 and 2, respectively. Four out of eight images can find 3 pair of peak and zero points. However, difference value of the accumulated hiding capacity between 2 pair and 3 pair are quite small.

Table 4. Accumulated Hiding Capacity (unit: bits) of *QLB* by using the Histogram Shifting Technique

PNO / Images	*PNO* = 1	*PNO* = 2	*PNO* = 3	*PNO* = 4	*PNO* = 5
Airplane	701	1371	N/A	N/A	N/A
Boat	421	806	N/A	N/A	N/A
Girl	298	560	562	563	N/A
Goldhill	212	403	N/A	N/A	N/A
Lenna	221	420	421	422	N/A
Pepper	192	377	N/A	N/A	N/A
Sailboat	365	691	692	N/A	N/A
Toys	610	1132	1246	1260	1261
Average	**377.5**	**720**	**N/A**	**N/A**	**N/A**

The accumulated hiding capacities of *DV* by using the histogram shifting technique are listed in Table 5. Average accumulated hiding capacity of 2318.5 and 3850.75 bits are obtained when the *PNO* values are set to 1 and 2, respectively. Four out of eight images

can find 3 pair of peak and zero points. Compared to the results shown in Tables 4 and 5, the accumulated hiding capacities of *DV* are greater than those of *QLA* and *QLB*.

Table 5. Accumulated Hiding Capacity (unit: bits) of *DV* by Using the Histogram Shifting Technique

PNO / Images	*PNO* = 1	*PNO* = 2	*PNO* = 3	*PNO* = 4	*PNO* = 5
Airplane	**3364**	5702	N/A	N/A	N/A
Boat	2658	4581	N/A	N/A	N/A
Girl	1703	2958	2964	2969	N/A
Goldhill	1039	2007	N/A	N/A	N/A
Lenna	2189	3605	3608	3610	N/A
Pepper	2611	4505	N/A	N/A	N/A
Sailboat	1219	2391	2394	N/A	N/A
Toys	3465	5057	5075	5093	5098
Average	**2318.5**	**3850.75**	**N/A**	**N/A**	**N/A**

Accumulated hiding capacities of the proposed scheme when the *PNO* values are set to 1 and 2 are listed in Table 6. In the first choice, *QLA* and *QLB* are used to embed the secret data. In the second choice, secret data is embedded into *QLA* and *DV*. In the third choice, *DV* and *QLB* are used to embed the secret data. According to the results, the proposed with the second choice achieves the highest capacity when *PNO* is set to 1. The proposed with the third choice achieves the highest capacity when *PNO* is set to 2. However, the accumulated hiding capacities between the second choice and the third choice are quite close.

Table 6. Accumulated Hiding Capacity (unit: bits) of the Proposed Scheme

PNO / Images	Choice 1		Choice 2		Choice 3	
	PNO = 1	*PNO* = 2	*PNO* = 1	*PNO* = 2	*PNO* = 1	*PNO* = 2
Airplane	1270	2376	4233	6707	4365	7073
Boat	779	1507	3016	5282	3079	5387
Girl	611	1156	2016	3554	1720	3518
Goldhill	430	809	1257	2413	1251	2410
Lenna	417	806	2385	3991	2410	4025
Pepper	404	794	2823	4922	2803	4882
Sailboat	690	1304	1544	3004	1584	3082
Toys	1360	2526	4215	6451	4075	6189
Average	**745.125**	**1409.75**	**2686.125**	**4540.5**	**2660.875**	**4570.75**

Table 7 lists the reconstructed image qualities of the proposed scheme. From Table 1 it is shown that average image quality of 33.232 dB is achieved by using the AMBTC scheme when the block size is set to 4×4. Average image qualities of 33.209 dB, 33.229 dB, and 33.202 dB are achieved by using the proposed scheme with these three choices when *PNO* is set to 1, respectively. When *PNO* is set to 2, average image qualities of 33.090 dB, 33.140 dB, and 32.973 dB are obtained by using the proposed scheme with these three choices, respectively. The average image quality degradation of the proposed scheme when *PNO* is set to 2 is less than 0.3 dB compared to the AMBTC scheme.

Table 7. Results of the Reconstructed Image Quality of the Proposed Scheme

PNO / Images	Choice 1		Choice 2		Choice 3	
	PNO = 1	*PNO* = 2	*PNO* = 1	*PNO* = 2	*PNO* = 1	*PNO* = 2
Airplane	33.259	33.079	33.264	33.179	33.245	32.914
Boat	31.957	31.838	31.957	31.898	31.948	31.751
Girl	34.759	34.507	34.762	34.602	34.758	34.339
Goldhill	33.685	33.545	33.691	33.595	33.659	33.435
Lenna	33.687	33.572	33.687	33.601	33.663	33.364
Pepper	33.954	33.941	34.064	33.968	33.971	33.873
Sailboat	31.173	31.055	31.175	31.114	31.163	30.943
Toys	33.196	33.180	33.228	33.165	33.211	33.168
Average	**33.209**	**33.090**	**33.229**	**33.140**	**33.202**	**32.973**

5. Conclusions

A novel reversible data hiding scheme based on the histogram shifting technique is proposed in the apepr. In the propsed scheme, the secret data is embeded into the quantization levels of the compressed codes of the block truncation coding scheme. Three different choices to organize the two data sets for data embedding had been designed.

From the experiemntal results, it is suggested that the second choice should be used to organize the data sets. Average accumulated hiding capacity of 2686.125 and 4540.5 bits are obtained by using the proposed scheme when the *PNO* values are set to 1 and 2, respectively. Only 0.003 dB 0.092 dB image degradation are incurred by using the proposed scheme when the *PNO* values are set to 1 and 2, respectively.

Acknowledgements

This research was supported by Providence University, Taichung, Taiwan under contract the National Science Council, Taipei, R.O.C. under contract NSC 101-2221-E-126-014 and NSC 102-2221-E-126-010.

References

[1] W. Bender, D. Gruhl, N. Morimoto and A. Lu, “Techniques for data hiding”, IBM Systems Journal, vol. 35, no. 3-4, **(1996)**, pp. 313-336.
[2] C. C. Chang, Y. H. Yu and Y. C. Hu, “Hiding secret data in images via predictive coding”, Pattern Recognition, vol. 38, no. 5, **(2005)**, pp. 691-705.
[3] Y. C. Hu, “High capacity image hiding scheme based on vector quantization”, Pattern Recognition, vol. 39, no. 9, **(2006)**, pp. 1715-1724.
[4] C. C. Chang, W. C. Wu and Y. C. Hu, “Lossless recovery of a VQ index table with embedded secret data”, Journal of Visual Communication and Image Representation, vol. 18, no. 3, **(2007)**, pp. 207-216.
[5] Y. C. Hu, C. C. Tsou and B. H. Su, “Grayscale image hiding based on modulus function and greedy method”, Fundamenta Informaticae, vol. 86, no. 1-2, **(2008)**, pp. 113-126.
[6] C. C. Chang, C. Y. Lin and F. H. Fan, “Lossless data hiding for color images based on block Truncation Coding”, Pattern Recognition, vol. 41, no. 7, **(2008)**, pp. 2347-2357.
[7] C. C. Chang, C. C., C. Y. Lin and Y. H. Fan, “Reversible steganography for BTC-compressed images”, Fundamenta Informaticae, vol. 109, no. 2, **(2011)**, pp. 121-134.
[8] C. H. Yang and Y. C. Lin, “Reversible data hiding of a VQ index table based on referred counts”, Journal of Visual Communication and Image Representation, vol. 20, no. 6, **(2009)**, pp. 399-407.
[9] C. C. Chang, S. N. Thai and C. C. Lin, “A reversible data hiding scheme for VQ indices using locally adaptive coding”, Journal of Visual Communication and Image Representation, vol. 22, no. 7, **(2011)**, pp. 664-672.
[10] Z. Ni, Y. Q. Shi, N. Ansari and W. Su, “Reversible data hiding”, IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, **(2006)**, pp. 354-362.

[11] P. Y. Tsai, Y. C. Hu and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting", Signal Processing, vol. 89, no. 6, **(2009)**, pp. 1129-1143.
[12] P. Y. Tsai, "Histogram-based reversible data hiding for vector quantization compressed images", IET Image Processing, vol. 3, no. 2, **(2009)**, pp. 100-114.
[13] Y. C. Chou, C. Y. Huang and Y. C. Hu, "Information hiding scheme with reversibility using difference segmentation and histogram adjustment", International Journal of Security and Its Applications, vol. 6, no. 2, **(2012)**, pp. 631-636.
[14] J. Tian, "Reversible data embedding using a difference expansion", IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 8, **(2003)**, pp. 890-896.
[15] H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam and H. G. Choo, "A novel difference expansion transform for reversible data embedding", IEEE Transactions on Information Forensics and Security, vol. 3, no. 3, **(2008)**, pp. 356-465.
[16] E. J. Delp and O. R. Mitchell, "Image compression using block truncation coding", IEEE Transactions on Communications, vol. 27, no. 9, **(1979)**, pp. 1335-1342.
[17] M. D. Lema and O. R. Mitchell, "Absolute moment block truncation coding and its application to color image", IEEE Transactions on Communications, vol. 32, no. 10, **(1984)**, pp. 1148-1157.
[18] P. Franti, P. Nevalainen and T. Kaudoranta, "Compression of digital image by block truncation coding: a survey", Computer Journal, vol. 37, no. 4, **(1994)**, pp. 308-332.
[19] Y. C. Hu, "Low-complexity and low-bit-rate image compression scheme based on AMBTC", Optical Engineering, vol. 42, no. 7, **(2003)**, pp. 1964-1975.
[20] Y. C. Hu, "Improved block truncation coding for image compression", Electronics Letters, vol. 39, no. 19, **(2003)**, pp. 1377-1379.
[21] Y. C. Hu, "Predictive moment preserving block truncation coding for gray-level image compression", Journal of Electronic Imaging, vol. 13, no. 10, **(2004)**, pp. 871-877.
[22] Y. C. Hu, B. H. Su and P. Y. Tsai, "Coluor image coding scheme using absolute moment block truncation coding and block prediction technique", Imaging Science Journal, vol. 56, no. 5, **(2008)**, pp. 254-270.
[23] C. C. Tsou, Y. C. Hu and C. C. Chang, "Efficient optimal pixel grouping schemes for AMBTC", Imaging Science Journal, vol. 56, no. 4, **(2008)**, pp. 217-231.
[24] Y. C. Hu and C. C. Chang, "Quadtree-segmented image coding schemes using vector quantization and block truncation coding", Optical Engineering, vol. 39, no. 2, **(2000)**, pp. 464-471.
[25] Y. C. Hu, "Predictive grayscale image coding scheme using VQ and BTC", Fundamenta Informaticae, vol. 78, no. 2, **(2007)**, pp. 239-255.
[26] Y. C. Hu and S. H. Wu, "Image progressive transmission by quadtree and BTC", Imaging Science Journal, vol. 56, no. 3, **(2008)**, pp. 153-162.
[27] Y. C. Hu, M. H. Lin and J. H. Jiang, "A novel color image hiding using block truncation coding", Fundamenta Informaticae, vol. 70, no. 4, **(2005)**, pp. 317-331.
[28] Y. C. Hu, "Multiple images embedding scheme based on moment preserving block truncation coding", Fundamenta Informaticae, vol. 73, no. 3, **(2006)**, pp. 373-387.
[29] Y. C. Hu, C. C. Lo, W. L. Chen and C. H. Wen, "Joint image coding and image authentication based on AMBTC", Journal of Electronic Imaging, vol. 22, no. 1, **(2013)**, 013012 (1-12).
[30] Y. C. Hu, W. L. Chen, C. C. Lo and C. M. Wu, "A novel tamper detection scheme for BTC compressed images," Opto-Electronics Review, vol. 21, no. 1, **(2013)**, pp. 137-146.
[31] Y. C. Hu, C. C. Lo, C. M. Wu, W. L. Chen and C. H. Wen, "Probability-based tamper detection scheme for BTC-compressed images based on quantization levels modification", International Journal of Security and Its Applications, vol. 7, no. 3, **(2013)**, pp. 11-32.

Authors

Yu-Chen Hu received his PhD. degree in computer science and information engineering from the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan in 1999. Currently, Dr. Hu is a professor in the Department of Computer Science and Information Management, Providence University, Sha-Lu, Taiwan. He is a member of ACM and IEEE. Dr. Hu Servers as the Editor-in-Chief of International Journal of Image Processing since 2009. He joints the editorial boards of several other journals. His research interests include image and signal processing, data compression, information hiding, and data engineering.

Chun-Chi Lo received the B.S., M.S., and Ph.D. degrees in computer science and information engineering from the National Taiwan University, Taipei, Taiwan, R.O.C., in 1989, 1991, and 1996, respectively. In 2004, he joined the faculty of the Department of Computer Science and Information Engineering, Providence University, Taiwan. Currently, he is an Assistant Professor. His research interests include wireless sensor networks, mean-field annealing, and combinatorial optimizations.

Wu-Lin Chen is currently an associate professor in the department of Computer Science and Information Management at Providence University. He received his M.S. and Ph.D. degrees in the School of Industrial Engineering at Purdue University in 1995, and 1999, respectively. His research interests include operations research, production management, and stochastic models.

Chang-Ming Wu received the B.S. and Ph.D. degrees, all in control and electrical engineering from the National Chiao-Tung University, Taiwan, in 1991 and 2000, respectively. From 2000 to 2007, he worked at Industrial Technology Research Institute, where he was R&D engineer for DSL and DVB-T transceiver and receiver chips. From 2007 to 2010, he was on the faculty of the Department of Computer Science and Information Engineering at the Providence University, Taiwan. Since 2010, he has been with the Department of Electronic Engineering, Chung Yuan Christian University at Taiwan, where he is an assistant professor. His current research interests are in the embedded system, vehicle control network, signal processing, and multivariable control system.

