High Capacity Reversible Data Hiding in AMBTC-Compressed Images

Zhenfei Zhao (corresponding author), Lin-Lin Tang

School of Electronics and Information
Zhejiang University of Media and Communications
NO.998 Xueyuan Street, Xiasha Higher Education Zone, Hangzhou 310018, China
Email: tree1118220@126.com

Department of Computer Science and Technology
Harbin Institute of Technology Shenzhen Graduate School
Shenzhen, China
Email: linlintang2009@gmail.com

Abstract
This paper proposes a high capacity reversible data hiding scheme in images compressed by absolute moment block truncation coding (AMBTC). The quantization levels of compressed blocks are employed as cover media, and some extra confidential data are hidden in it based on a multilevel histogram shifting mechanism. The transmission system preserves the same complexity. Moreover, the reconstructed image quality is exactly the same as the original compressed version due to the reversibility. Extensive experimental results demonstrate the effectiveness of the proposed scheme.

Keywords: absolute moment block truncation coding, multilevel histogram shifting, data hiding

1. Introduction

Block truncation coding (BTC) [1] is a popular used lossy image compression prototype with low computation complexity, although its compression ratio is usually low. In [2], absolute moment block truncation coding (AMBTC) is developed to improve the performance of conventional BTC technique. It exploits the first absolute moments instead of variances as thresholds. Because of its better mean square error (MSE) performance, AMBTC has been extensively used in the field of image compression. In recent years, transmission security of image content has drawn much attention among researchers. As an effective technique to solve this problem, digital watermarking and data hiding [3, 4, 12, 13] plays an important role in multimedia security. More recently, many reversible data hiding schemes have been reported in literatures. The reversibility means not only the confidential data but also the cover image can be precisely recovered in decoder at the same time. Due to this advantage, the reversible data hiding technique is suitable for some special applications, e.g. hiding secret data in military maps, medical images, etc.

Nowadays, most reversible data hiding methods are derived from two principles, histogram shifting [5] and difference expansion [6]. In [7], Ni et al. first proposed the histogram shifting based reversible data hiding algorithm. Thereafter, Li et al. [8] presented the adjacent pixel difference (APD) scheme to improve the embedding capacity. In [9], Zhao et al. proposed an multilevel histogram shifting algorithm to further enhance the capacity.

It is necessary to note that, most data hiding algorithms [10] in BTC compressed image are irreversible. In our scheme, a reversible data hiding scheme is designed for AMBTC compressed images. In particular, each image block is compressed into two quantization levels and a bitmap. Our method is developed to hide data in these quantization levels with the reversibility preserved. It can be used in some specific application scenarios, e.g., covert communication during AMBTC compressed image transmission.

The rest of this paper is organized as follows. In section 2, the AMBTC and multilevel histogram shifting algorithm are briefly reviewed. In section 3, the proposed scheme is extensively described. In Section 4, experimental results are demonstrated. Finally, conclusions are given in Section 5.

2. Related Work
2.1. Absolute moment block truncation coding

AMBTC is a variant of BTC presented by Lema and Mitchell in 1984. It adopts the mean and the first absolute central moment of each block to guarantee low computational complexity. AMBTC has been shown as the best bi-level moment preserving quantizer [11], and its encoding and decoding procedures are described below.

Suppose the original image \( I \) is a gray-level image. In the encoding stage, firstly, \( I \) is divided into a set of \( m \times m \) non-overlapping blocks \( X_i \). In this way, the mean value \( x_m \) of each block is computed as

\[
x_m = \frac{1}{m^2} \sum_{j=1}^{m^2} x_j
\]

where \( x_i \) denotes the pixel value of the non-overlapping blocks \( X_i \).

Secondly, the two quantization levels \( a \) and \( b \) and each block is computed as

\[
a = \frac{1}{p} \sum_{x_i \leq x_m} x_i
\]

\[
b = \frac{1}{q} \sum_{x_i > x_m} x_i
\]

where \( p \) denotes the number of pixels smaller than or equal to the block mean value \( x_m \), \( q \) denotes the number of pixels higher than \( x_m \).

Finally, the \( m \times m \) bitmap \( C \) of the block pixels is written as

\[
C = \begin{cases} 
1 & \text{if } x_i \leq x_m \\
0 & \text{otherwise}
\end{cases}
\]

The two quantization levels and bitmap \( \{a, b, C\} \) are transmitted to the receiver. In the decoding stage, each block can be approximately recovered with \( a \), \( b \) and \( C \) as

\[
x'_i = \begin{cases} 
b & \text{if } C_i = 1 \\
a & \text{otherwise}
\end{cases}
\]

where \( x'_i \) is the recovered pixel value of the current decoded block. Thus, the decoded image can be reconstructed by all reconstructed blocks.

2.2. Multilevel histogram shifting

Zhao et al. proposed reversible data hiding scheme based on multilevel histogram shifting. The histogram is constructed by neighbor pixels difference values because of the similarity of two adjacent pixels’ values. Multilevel histogram shifting mechanism is employed to hide confidential data. In data extraction stage, the confidential data is extracted from the marked sequences of pixels’ differences. Meanwhile, the host image can be accurately recovered with an inverse multi-level histogram shifting mechanism strategy employed after removing the secret data from the marked image.

This scheme demonstrates that the embedding capacity is determined by the embedding level \( f \) and the peak bins around bin zero. Suppose no overflow or underflow occurs, the capacity \( \text{Cap} \) (bit) can be estimated as

\[
\text{Cap} = \begin{cases} 
b_0 & \text{if } f = 0 \\
\sum_{k} b_k & \text{if } f > 0
\end{cases}
\]

where \( b_0 \) refers to the number of samples falling into the histogram bin at zero. In addition, \( f \) indicates the embedding round. More details of multilevel histogram shifting can be referred to [9].

3. Proposed Scheme
In this section, a high capacity reversible data hiding scheme in AMBTC-compressed images is introduced. In our scheme, the multilevel histogram shifting mechanism is used in the data embedding stage. The motivation of multilevel histogram shifting utilization lies in that it can provide a relatively high embedding capacity and generate acceptable quality stego-images. An integer parameter \( f (f \geq 0) \) denotes the level of the data hiding. It is used to control the data hiding capacity. A higher \( f \) indicates more confidential data could be embedded. A set of experiments demonstrate that \( f \) should be no larger than 10 for natural gray level images. The confidential data and host media can be recovered with distortion in data extraction and image recovery stage by using the inverse procedures of multilevel histogram shifting.

The encoding operations are described below.

Suppose the original image \( I \) is a gray-level image. The reconstructed AMBTC compressed image is denoted by \( I_r \). The confidential data is represented by \( w \).

Step1. Perform AMBTC encoding on \( I \). Hence \( a \), \( b \) and \( C \) are generated.

Step2. Rearrange \( a \) and \( b \) of all blocks into a one-dimensional array \( M \). Suppose \( m_1, m_2, \ldots, m_{M \times N} \) denote the elements of \( M \). Then compute the difference \( d_i \) of two adjacent neighboring pixels one by one. In this way, a difference sequence is obtained as

\[
d_i = \begin{cases} 
  m_i & i = 1 \\
  m_{i+1} - m_i & 2 \leq i \leq M \times N
\end{cases}
\]  

(7)

Next, construct a histogram \( H \) based on the differences \( d_i \). The scan order of the values of \( a \) and \( b \) is illustrated in Figure 1, where a 3×3 image block is used to illustrate this principle. The scan direction is marked as the blue line, from left to right and from top to bottom.

![Figure 1. Scan order of a 3×3 image block](image)

Step3. Select an appropriate parameter \( f \) according to the amount of data to be embedded, and then compute the shifting difference \( d_i' \) based on Eq. (8) one by one.

\[
d_i' = \begin{cases} 
  m_i & i = 1 \\
  d_i & -f \leq d_i \leq f, 2 \leq i \leq M \times N \\
  d_i + 1 & d_i > f, 2 \leq i \leq M \times N \\
  d_i - f & d_i < -f, 2 \leq i \leq M \times N
\end{cases}
\]  

(8)

Step4. Embed the confidential data \( w \) by multilevel histogram shifting according to Eq. (9). Next, compute the marked pixels difference sequence \( d_i'' \).

\[
d_i'' = \begin{cases} 
  m_i & i = 1 \\
  d_i' & -f < d_i' < f, 2 \leq i \leq M \times N \\
  2 \times f + w & d_i' = f, 2 \leq i \leq M \times N \\
  -2 \times f - w + 1 & d_i' = -f, 2 \leq i \leq M \times N
\end{cases}
\]  

(9)

Step5. Generate the marked pixels sequence \( m_i' \) as

\[
m_i' = \begin{cases} 
  m_i & i = 1 \\
  m_i - d_i'' & 2 \leq i \leq M \times N
\end{cases}
\]  

(10)
The corresponding operations in the decoding stage are described as follows.

Step 1. Obtain the $f$ parameter from the sender.

Step 2. The secret data $w$ is extracted and the sequence $m_i$ is recovered.

$$m_i = \begin{cases} p'_i & \text{if } i = 1 \\ p'_i + f + 1 & \text{if } m_i = m_i + f + 1, 2 \leq i \leq M \times N \\ m'_i - f & \text{if } m_i - m'_i \leq -2 f, 2 \leq i \leq M \times N \\ m'_i - 1 & \text{if } -2 f < m_i - m'_i < 0 \\ m'_i + 1 & \text{if } 0 < m_i - m'_i < 2 f + 1 \end{cases}$$

(11)

$$w_k = \begin{cases} 0 & \text{if } m_{i-1} - m'_i = 2 \times f, 2 \leq i \leq M \times N \\ 0 & \text{if } m_{i-1} - m'_i = -2 \times f + 1, 2 \leq i \leq M \times N \\ 1 & \text{if } m_{i-1} - m'_i = 2 \times f + 1, 2 \leq i \leq M \times N \\ 1 & \text{if } m_{i-1} - m'_i = -2 \times f, 2 \leq i \leq M \times N \end{cases}$$

(12)

Step 3. Reconstruct the AMBTC-compressed block based on the quantization levels $a$, $b$ and the bitmap $C$ according to Eq. (5).

Step 4. Repeat Step 1 and Step 3 to all blocks. In this way, the original AMBTC-compressed image $I_r$ is reconstructed.

4. Experimental Results and Discussions

To evaluate the performance of the proposed scheme, three 512×512 gray level images (Lena, Barbara, Goldhill) are selected as test images as shown in Figure 2. The block size partitioned for AMBTC compression is 4×4. The confidential data for embedding is a binary sequence produced by a pseudo random number generator.

![Figure 2. Test images, Lena, Barbara, Goldhill (from left to right)](image)

The peak signal-to-noise rate (PSNR) is used to measure the image quality. The computation of PSNR is defined as

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}}$$

(13)

where MSE is defined as:

$$\text{MSE} = \frac{1}{m \times n} \sum_{x=1}^{m} \sum_{y=1}^{n} (I(x,y) - I'(x,y))^2$$

(14)

where $I(x,y)$ and $I'(x,y)$ indicate the pixel values of the cover image and stego image.
To evaluate the proposed scheme, Table 1 lists the capacity and PSNR values of with $f=0, 1, \ldots, 9$. The larger $f$ corresponds to a higher embedding capacity. The PSNR are computed between the recovered AMBTC-compressed image and the raw version. It can be seen the PSNR are still acceptable in most application scenarios. In particular, the PSNR values are independent to the embedding capacity.

<table>
<thead>
<tr>
<th>Method</th>
<th>Lena</th>
<th>Barbara</th>
<th>Goldhill</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Capacity</td>
<td>PSNR</td>
<td>Capacity</td>
</tr>
<tr>
<td>$f=0$</td>
<td>4064</td>
<td>34.00</td>
<td>2648</td>
</tr>
<tr>
<td>$f=1$</td>
<td>11136</td>
<td>34.00</td>
<td>7334</td>
</tr>
<tr>
<td>$f=2$</td>
<td>16115</td>
<td>34.00</td>
<td>10970</td>
</tr>
<tr>
<td>$f=3$</td>
<td>19245</td>
<td>34.00</td>
<td>13912</td>
</tr>
<tr>
<td>$f=4$</td>
<td>21362</td>
<td>34.00</td>
<td>16335</td>
</tr>
<tr>
<td>$f=5$</td>
<td>22787</td>
<td>34.00</td>
<td>18298</td>
</tr>
<tr>
<td>$f=6$</td>
<td>23924</td>
<td>34.00</td>
<td>19985</td>
</tr>
<tr>
<td>$f=7$</td>
<td>24890</td>
<td>34.00</td>
<td>21420</td>
</tr>
<tr>
<td>$f=8$</td>
<td>25608</td>
<td>34.00</td>
<td>22541</td>
</tr>
<tr>
<td>$f=9$</td>
<td>26246</td>
<td>34.00</td>
<td>23573</td>
</tr>
</tbody>
</table>

Figure 3. Experimental results on Lena image, (a) the original image, (b) the reconstructed image with the proposed scheme, PSNR=34.00dB, (c) the reconstructed image with AMBTC scheme, PSNR=34.00dB

Figure 4. Experimental results on Barbara image, (a) the original image, (b) the reconstructed image with the proposed scheme, PSNR=29.87dB, (c) the reconstructed image with AMBTC scheme, PSNR=29.87dB
Figure 5. Experimental results on Goldhill image, (a) the original image, (b) the reconstructed image with the proposed scheme, PSNR=32.86dB, (c) the reconstructed image with AMBTC scheme, PSNR=32.86dB

Experimental results show that the confidential data is embedded into the AMBTC compressed file, and can be extracted without distortion, results demonstrate that the proposed scheme not only can embed confidential data while maintains the same image quality as the original AMBTC compressed version from Figure 3 to Figure 5. In general, the parameters selection such as embedding level can be determined according to the quantity of confidential data.

5. Conclusions

In this paper, a high capacity reversible data hiding scheme for AMBTC compressed image has been proposed. Our method uses multilevel histogram shifting to obtain high embedding capacity, the confidential data is embedded directly into the compressed file of AMBTC compressed image, and while the secret data can recovered without distortion. Experimental results show that our scheme can embed secret data while maintains the same image quality as the original AMBTC compressed version.

6. Acknowledgement

This work is financially supported by the Post-doctoral Funds in China named Watermarking Techniques Based on the Multiple Description Coding under the granted number of BD24406001.

7. References


