A New Difference Expansion Transform in Triplets for Reversible Data Hiding

E. Chrysochos, V. Fotopoulos and A. N. Skodras
Digital Systems & Media Computing Laboratory
School of Science and Technology, Hellenic Open University
13-15 Tsamadou st., GR-26222, Patras, Greece
phone: (+30) 2610367535, fax: (+30) 2610367520, email: {e.chrysochos, vfotop1, skodras}@eap.gr
web: dsmc2.eap.gr

Abstract

Difference expansion (DE) has been widely used for reversible data hiding. In this paper a novel transform which embeds two bits of information in a triplet of coefficients is presented. This transform can be applied in spatial or frequency domain and induces minimum distortion to the initial data or coefficients. The proposed method outperforms all similar DE methods using triplets in terms of computational cost, visual quality and bitrate.

Keywords: 3C2B; Difference Expansion; Lossless Data Hiding; Triplets; DCT.

1. Introduction

Digital watermarking and data hiding are two close but distinct research areas which are characterized by data embedding in digital media. The main difference between them is the scope of the application. In data hiding the medium-carrier is of no importance, and its purpose is restricted in transmitting a secret message through a communication channel without being noticed. In digital watermarking the medium is of crucial importance as well as the message hidden within.

In both research areas there are applications that require the embedding process to be reversible, i.e. with no overall loss of information. In this case the embedding process is characterized as reversible watermarking [14], [15] and lossless data hiding, respectively [11], [9], [7]. Reversible watermarking and lossless data hiding are appropriate for military and medical applications where all information is considered critical and no loss is tolerated.

A reversible data embedding technique based on difference expansion was introduced by J. Tian in
The specific data embedding technique was not robust to any attacks, but provided high capacity, low image distortion and low computational cost. Based on Tian’s algorithm many algorithms were proposed in order to improve its robustness [4], [14], [5] or its capacity [13], [15]. In order to further improve its embedding capacity transforms on triplets [2], [8] and quads [1] were used.

In the present work triplets are selected over quads because for each triplet only two out of three coefficients need to be altered, as opposed to quads where all coefficients need to be altered. In this way, and for the same payload, triplets are expected to induce less image degradation than quads.

The rest of the paper is organized as follows. In section 2 the major difference expansion methods and the proposed transform are described. Analysis and comparisons are discussed in section 3. Experimental results are presented in section 4, while conclusions are drawn in section 5.

2. Difference Expansion Transforms

Difference expansion, introduced by Tian in 2003, is a reversible transform [10]. According to this algorithm one bit of information is embedded reversibly in each pair of data as shown below. These data can be in spatial or frequency domain, while the capacity of the method approaches 0.5 bpp. (In the following coefficients will refer to data, independently of whether they represent pixel values or transform coefficients).

An extension of Tian’s algorithm is to implement difference expansion on triplets of coefficients [2], [8]. In that way the capacity of the algorithm is increased by 33%, as two bits of information are embedded in each triplet of coefficients. Shen-Hsu’s, Alattar’s and the proposed transform are all based on triplets and achieve a capacity of up to 0.67 bpp.

2.1 Tian’s Difference Expansion Transform

In Tian’s difference expansion one bit of information $b$ is embedded in each pair of coefficients $C_1$, $C_2$, resulting in a new pair $C_{1n}$, $C_{2n}$ as in (1) and (2).

$$C_{1n} = \left[ \frac{C_1 + C_2}{2} \right] + C_1 - C_2 + b \quad (1)$$

$$C_{2n} = \left[ \frac{C_1 + C_2}{2} \right] - C_1 + C_2 \quad (2)$$
where \( \lfloor . \rfloor \) denotes the integer floor operator. Provided the resulting coefficients \( C_{1n}, C_{2n} \) are available, the transform is reversible and \( C_1, C_2, b \) can be retrieved by means of (3), (4) and (5) respectively.

\[
C_1 = \left\lfloor \frac{C_{1n} + C_{2n}}{2} \right\rfloor + \left\lfloor \frac{d + 1}{2} \right\rfloor \tag{3}
\]

\[
C_2 = \left\lfloor \frac{C_{1n} + C_{2n}}{2} \right\rfloor - \left\lfloor \frac{d}{2} \right\rfloor \tag{4}
\]

\[
b = (C_{1n} - C_{2n}) \mod 2 \tag{5}
\]

where \( d = \left\lfloor \frac{C_{1n} - C_{2n}}{2} \right\rfloor \).

### 2.2 Shen and Hsu’s 3C2B Transform on triplets [8]

According to Shen-Hsu’s method [8], designated as method A and denoted by the subscript A below, two bits \( b_1, b_2 \) are embedded in three coefficients \( C_1, C_2, C_3 \) as follows:

\[
D_{1A} = |C_1| - |C_2| \tag{6}
\]

\[
D_{2A} = |C_3| - |C_2| \tag{7}
\]

\[
b_3 = \text{sign}(C_1) \tag{8}
\]

\[
b_4 = \text{sign}(C_3) \tag{9}
\]

\[
b_5 = \text{sign}(D_{1A}) \tag{10}
\]

\[
b_6 = \text{sign}(D_{2A}) \tag{11}
\]

(The sign function has an output of 0 or 1)

The expanded difference results to:

\[
\tilde{D}_{1A} = 8|D_{1A}| + 4b_3 + 2b_4 + b_5 \tag{12}
\]

\[
\tilde{D}_{2A} = 8|D_{2A}| + 4b_6 + 2b_1 + b_2 \tag{13}
\]

The transformed coefficients are:

\[
C_{1A} = C_2 - \tilde{D}_{1A} \tag{14}
\]

\[
C_{3A} = C_2 - \tilde{D}_{2A} \tag{15}
\]
\[ C_{2,A} = C_2 \text{ (remains the same)} \quad (16) \]

### 2.3 Alattar’s Transform on triplets [2]

In accordance with Alattar’s approach, designated as method B and denoted by the subscript B below, the two bits \( b_1, b_2 \) are embedded in the three coefficients \( C_1, C_2, C_3 \) by means of (17), (18) and (19) below:

\[
\begin{align*}
C_{1B} &= \left[ \frac{C_1 + C_2 + C_3}{3} \right] \\
C_{2B} &= 2(C_3 - C_2) + b_1 \\
C_{3B} &= 2(C_1 - C_2) + b_2
\end{align*}
\]

### 2.4 The Proposed Transform

According to the proposed method, designated as method C and denoted by the subscript C below, the two bits \( b_1, b_2 \) are embedded (forward transform) in three coefficients \( C_1, C_2, C_3 \) as given below:

\[
\begin{align*}
D_{1C} &= C_1 - C_2 \\
D_{2C} &= C_2 - C_3 \\
C_{1C} &= C_2 + 2D_{1C} + b_1 \\
C_{2C} &= C_2 \text{ (remains the same)} \\
C_{3C} &= C_2 - 2D_{2C} + b_2
\end{align*}
\]

The extraction (inverse transform) is given by:

\[
\begin{align*}
b_1 &= (C_{1C} - C_{2C}) \mod 2 \\
b_2 &= (C_{2C} - C_{3C}) \mod 2 \\
C_1 &= C_{2C} + \frac{C_{1C} - C_{2C} - b_1}{2} \\
C_2 &= C_{2C} \text{ (remains the same)} \\
C_3 &= C_{2C} + \frac{C_{2C} - C_{3C} - b_2}{2}
\end{align*}
\]
3. **Analysis and Comparisons**

As mentioned above, all transforms can be used in spatial domain [2] or frequency domain [8]. These transforms are evaluated in terms of computational cost, and performance with regard to overall coefficient alteration.

### 3.1 Computational Cost Analysis

In all three transforms two bits of information are embedded using three coefficients (either in spatial or in frequency domain). For the embedding process Shen-Hsu’s algorithm performs 10 sign and absolute value function calls, 6 shift operations (multiplications) and 10 additions. Alattar’s algorithm performs 1 lower bound function call, 2 shift operations (multiplications), 1 division and 6 additions. The proposed algorithm for the same embedding process performs only 2 shift operations (multiplications) and 6 additions. For the extraction process, i.e. in order to extract two bits of information and restore the coefficients to their initial values, Shen-Hsu’s algorithm performs 6 absolute value function calls, 8 shift operations, 4 multiplications and 4 additions. Alattar’s algorithm performs 1 lower bound function call, 5 shift operations, 1 division and 8 additions, while the proposed algorithm performs 4 shift operations and 4 additions.

The computational cost of the proposed method is significantly lower than that of the other methods, achieving higher performance (in terms of execution time). The proposed transform is also more appropriate for application in embedded systems where computational cost is of crucial importance.

### 3.2 Performance Analysis with regard to coefficient alteration

During the embedding process two bits of information are embedded in each triplet of coefficients causing the alteration of these coefficients. Provided the coefficients are in spatial domain, the effect of the embedding algorithm in an image (visual degradation) is proportional to the alteration of its coefficients. In frequency domain the alteration of the coefficients results not only in lower peak-signal-to-noise-ratio (PSNR) values but in higher bitrates as well, since the coefficient’s values are more scattered, resulting in higher entropy and less efficient compression. The analysis presented below relates to frequency domain where coefficients may have positive or negative values.

i) In Shen-Hsu’s 3C2B transform the alteration of the coefficient $C_I$ according to (12), (14) is:
\[ a_{1A} = C_1 - C_{1A} = C_1 - C_2 + \bar{D}_{1A} = C_1 - C_2 + 8|D_{1A}| + 4b_4 + 2b_4 + b_5 \]  

(30)

And since the absolute alteration of the coefficient is of interest:

\[ |a_{1A}| \leq |C_1| + |C_2| + 8|D_{1A}| + 7 \]  

(31)

Therefore the upper bound of the alteration of coefficient \( C_1 \) is given by (31), where \( D_{1A} \) is the difference between the absolute values of \( C_1 \) and \( C_2 \). The same applies to the alteration of coefficient \( C_3 \):

\[ |a_{3A}| \leq |C_3| + |C_2| + 8|D_{2A}| + 7 \]  

(32)

where \( D_{2A} \) is the difference between the absolute values of \( C_3 \) and \( C_2 \). The coefficient \( C_2 \) is not altered during the embedding process.

ii) In Alattar’s transform the alteration of the coefficient \( C_2 \) according to (18) is:

\[ a_{2B} = C_2 - C_{2B} = C_2 - 2(C_3 - C_2) - b_1 = 3C_2 - 2C_3 - b_1 \]  

(33)

And since the absolute alteration of the coefficient is of our interest:

\[ |a_{2B}| \leq 3|C_2| + 2|C_3| + 1 \]  

(34)

Likewise from (19), (17):

\[ a_{3B} = C_3 - C_{3B} = C_3 - 2(C_1 + C_2) - b_2 \]  

(35)

\[ |a_{3B}| \leq |C_3| + 2|C_1| + 2|C_2| + 1 \]  

(36)

\[ a_{1B} = C_1 - C_{1B} = C_1 - \left| \frac{C_1 + C_2 + C_3}{3} \right| \]  

(37)

\[ |a_{1B}| \leq \left| \frac{|C_1| + |C_2| + |C_3|}{3} \right| + |C_1| \]  

(38)

In Alattar’s method all three coefficients are altered in contrary to the other methods where only two coefficients of each triplet are altered.

iii) In the proposed method the alteration of the coefficient \( C_1 \) according to (22) is:

\[ a_{1C} = C_1 - C_{1C} = C_2 - C_1 - b_1 \]  

(39)

Therefore:

\[ |a_{1C}| \leq |C_1| + |C_2| + 1 \]  

(40)

Likewise from (24):
\[ a_{3C} = C_3 - C_{3C} = C_2 - C_3 - b_2 \]  \hspace{1cm} (41)

\[ |a_{3C}| \leq |C_2| + |C_3| + 1 \]  \hspace{1cm} (42)

The coefficient \( C_2 \) remains unaltered during the embedding process.

From (31), (32), (34), (36), (38), (40), (42) it is derived that the proposed transform induces significantly lower alterations, than Shen-Hsu’s and Alattar’s transform in the coefficients during the phase of embedding, justifying the higher PSNR and weighted-PSNR (wPSNR) as well as lower entropy results of the proposed method.

4. Experimental Results

Shen and Hsu’s 3C2B, Alattar’s and the proposed algorithm are compared in terms of PSNR (Table1), weighted PSNR (Table2) and entropy (Table3).

Peak-signal-to-noise-ratio is the most common metric used to evaluate the distortion of an image during a watermarking process. This objective quality measure is defined in dB as:

\[ \text{PSNR} = 10 \cdot \log \left( \frac{255^2}{\text{MSE}} \right) \]  \hspace{1cm} (43)

where MSE is the mean square error between the original image \( I_{\text{orig}} \) and the watermarked one \( I_w \). The MSE is defined as:

\[ \text{MSE} = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (I_{\text{orig}}(i,j) - I_w(i,j))^2 \]  \hspace{1cm} (44)

where \( M \) and \( N \) are the image dimensions.

Weighted PSNR (wPSNR) was selected because PSNR metric does not take into account whether a region is flat or textured and all regions are treated equally. wPSNR emulates the Human Visual System (HVS) by introducing different weights for the perceptually different regions of an image. wPSNR is given by:

\[ \text{wPSNR} = 10 \cdot \log \left( \frac{\text{max}(I_{\text{orig}})^2}{\text{MSE} \cdot \text{NVF}} \right) \]  \hspace{1cm} (45)

where NVF is the Noise Visibility Function which is a texture masking function and is used as a penalization factor. For flat regions, the NVF is close to 1 while for edge or textured regions NVF is more close to 0. The NVF is given by:

\[ \text{NVF}(i,j) = \frac{1}{1 + \theta \sigma_x^2(i,j)} \]  \hspace{1cm} (46)

where \( \theta \sigma_x^2(i,j) \) denotes the local variance of the image in a window centered on the pixel with coordinates \( (i,j) \) and \( \theta \) is a tuning parameter corresponding to the particular image. Local variance is given by:
\[ \sigma_x^2(i, j) = \frac{1}{(2L+1)^2} \sum_{k=-L}^{L} \sum_{l=-L}^{L} \left( x(i + k, j + l) - \bar{x}(i, j) \right)^2 \]  \hspace{1cm} (47)

and

\[ \bar{x}(i, j) = \frac{1}{(2L+1)^2} \sum_{k=-L}^{L} \sum_{l=-L}^{L} x(i + k, j + l) \]  \hspace{1cm} (48)

where a window of size \((2L+1) \times (2L+1)\) is considered. The image-depend tuning parameter is given as:

\[ \theta = \frac{D}{\sigma_x^{2(\text{max})}} \]  \hspace{1cm} (49)

where \(\sigma_x^{2(\text{max})}\) is the maximum local variance for a given image and \(D\) is an experimental value, ranging from 50 to 100.

Entropy of discrete cosine transform (DCT) coefficients is an indicator of the resulting bit rate after compression of an image and is given by the formula:

\[ H = - \sum_{k=0}^{L-1} P_r(k) \log_2 P_r(k) \]  \hspace{1cm} (50)

where \(L\) is the number of intensity values and \(P_r(k)\) is the probability occurrence of \(k\) intensity and is given by:

\[ P_r(k) = \frac{n_k}{M \cdot N} \]  \hspace{1cm} (51)

where \(n_k\) is the number of times that the \(k_{th}\) intensity appears in the \(M \times N\) image.

Shen-Hsu’s, Alattar’s and the proposed transform are all based on triplets and have a theoretical upper bound for capacity of up to 0.67 bpp. All three methods were implemented in frequency domain using Matlab (v7.0). Discrete Cosine Transform was applied on non-overlapping 8x8 blocks for all images and 24 coefficients of each block (8 triplets) were used for the embedding procedure. The number of coefficients used per block is arbitrary and coefficients 41 to 64 were selected in order to have comparable results with [8]. Therefore 16 bits of information were embedded in each block of the image and the capacity of all methods is the same. The least significant coefficients, in raster scan order, of each block were selected for embedding in order to have minimum distortion. Since the embedding process takes place in the frequency domain there are no overflow/underflow issues and no need for location map [8]. The only side information needed for the embedding and extracting procedure is the starting coefficient of each block (i.e. the coefficient from which the embedding/extracting process begins). If the algorithm was implemented in spatial domain, a location map would be necessary [10]. The same applies for Shen and
Hsu’s 3C2B and Alattar’s transform. In this case the payload in figure1 and tables 1 and 2 represents the mixed capacity for all three methods.

As shown in Tables 1, 2 and 3, the proposed transform outperforms Shen-Hsu’s and Alattar’s transform. In all cases the proposed algorithm introduces less visual degradation measured in PSNR and wPSNR. The entropy of the DCT coefficients is kept at lower levels allowing for more efficient compression and lower bitrates.

The number of coefficients used for embedding per block affects the capacity of the scheme. By altering more coefficients per block the capacity increases, while visual quality (PSNR) decreases. In Fig.1 the output of each algorithm with regard to payload is outlined for Lena image. The capacity in Fig.1 remains lower than 0.67bpp because not all the coefficients of each block are used. By using 54 out of 64 coefficients for Lena image, the PSNR of Shen-Hsu is 18.08 dB, Alattar’s is 23.62 dB and the proposed method’s 30.1 dB, respectively.

As shown in Fig.1, the proposed transform outperforms Shen-Hsu’s and Alattar’s transforms in all cases resulting in higher PSNR values for a certain payload. Consequently for a given PSNR threshold the proposed algorithm provides higher capacity.

5. Conclusions

A novel algorithm for reversible data hiding is presented based on the well known difference expansion family of techniques. A transform which embeds two bits of information in a triplet of coefficients in spatial or frequency domain is proposed. The method outperforms all other difference expansion methods using triplets in terms of payload and visual quality measured in PSNR and wPSNR. The transform has lower computational cost than all other transforms, while inducing smaller alteration in the coefficients used for embedding. This is measured by lower entropy of the watermarked images allowing more efficient compression and lower bitrates.
Acknowledgments

This work was funded by the European Union - European Social Fund (75%), the Greek Government - Ministry of Development - General Secretariat of Research and Technology (25%) and the Private Sector in the frames of the European Competitiveness Programme (Third Community Support Framework - Measure 8.3 - programme ΠΕΝΕΔ - contract no.03ΕΔ832).

References


