A New Reversible Data Hiding Technique Combined with Interpolation and Pixel Value Differencing Method

Jayeeta Majumder*, Chittaranjan Pradhan*

*Department of CSE, Haldia Institute of Technology, West Bengal, India
2Department of CSE, KIIT University, Orissa, India

ABSTRACT

Steganography is the popular security method that provides complete security for communicating secret details. Image steganography is a very interesting field because of the imperceptible way of hiding data in images, since small distortion in the images cannot be identified by a human eye. This is the main idea to develop image steganography algorithms to improve visual quality. Pixel Value Differencing is able to provide a high quality stego image in spite of the high capacity of the concealed information. This paper proposes the first the interpolation techniques with the pixel block then applying then the Pixel Value Differencing method. Here in the first phase the original image is portioned into 2X2 block then applying the nearest neighbour interpolation technique after that in the second phase PVD is used to embed the secret data. Then the new pixel value of the neighbouring pixel also calculated. In this paper one variant are proposed by using single range table. We observed that for both the variant PSNR value and the hiding capacity are increased.

Keywords: Data Hiding, Nearest Neighbour Interpolation, PVD Scheme, Steganography.

1. INTRODUCTION

In modern days steganography is one of the most important data hiding techniques. When one can propose any steganographic scheme, the hiding capacity and the undetectability properties are to be considered. One of the most common steganographic scheme is LSB substitution method. The simplest technique is detected by RS analysis. Wu and Tsai [1] exposed the fact that the edge regions in an image can conceal more amounts of data as compared to the smooth regions. Based on this principle they proposed pixel value differencing (PVD) steganography. The PVD technique with block size 2 × 2 has been proposed to enhance the embedding capacity [2, 3]. In blocks of size 2 × 2, edges in three directions are considered. To calculate the pixel value differences, Chang and Tseng [4] considered the values of 2, 3, and 4 neighboring pixels. The data embedding locations can be randomized based on the messages [5]. Further, the capacity of data hiding is improved when 2X2 pixel blocks are taken and calculate the difference of pixel value directionally [7, 8]. Chen [9] proposed a PVD steganography using two reference tables to randomize the data embedding. Based on pixel value differences, adaptive LSB substitution has been performed in [10]. Khodaei and Faez [11] proposed a hybrid approach by combining LSB substitution and PVD in 1 × 3 pixel block. It is extended to 2 × 2 size block in [12] and 2 × 3 size block in [13] to improve the performance. Swain [15] proposed two adaptive PVD steganography techniques using vertical, horizontal, and diagonal edges, which does not suffer with step effect. The first technique uses pixel blocks of size 2 × 2, and the second technique uses pixel blocks of size 3 × 3. In general, adaptive image steganography
schemes possess lower embedding capacity. Anita et al. [16] optimized the performance of adaptive PVD by using 6 pixel blocks. The edges can be predicted by some prediction functions, and hiding capacity depends upon this prediction. If we hide bits of data in smooth regions, distortion will be more. Based on the level of complexity of the edge regions, adaptive embedding can be applied [17]. In this way capacity can be increased and chance of detection can be decreased. Balasubramanian et al. [18] proposed a PVD scheme with $3 \times 3$ size pixel blocks, to achieve higher hiding capacity. To prevent the detection from pixel difference histogram (PDH) analysis, multidirectional edges have been exploited in [19]. Darabkh et al. [20] also proposed PVD steganography using eight directional PVD which is an extension in principle from Wu and Tsai’s original PVD. Any PVD technique which is an extension of Wu and Tsai’s approach should qualify through PDH analysis. This paper proposes the steganographic scheme in a 2X2 pixel block along with interpolation and PVD technique. Here one type of range table are used for both PSNR and higher data bit capacity.

II. THE PROPOSED TECHNIQUE

The proposed technique in data embedding phase is divided into two part. First the original image is scaled up using interpolation scheme then applying the PVD techniques.

A. Interpolation Phase

Step1- divide the cover image into 2X2 non-overlapping pixel block by scanning the cover image in raster scan order. Then applying the nearest neighbour interpolation techniques and convert the pixel block into 3X3 pixel block.

<table>
<thead>
<tr>
<th>p_x(0,0)</th>
<th>p(0,1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>p(1,0)</td>
<td>p(1,1)</td>
</tr>
</tbody>
</table>

Let $p_x(0,0)$, $P(1,0)$, $P(0,1)$ and $P(1,1)$ are the pixel values of cover images

- First decide the Maximum pixel value among the above pixel, let it is $p_{max}$, then,
- Calculate $p_r$ as $(p_{max} + (p_x + p(0,1))/2)/2$
- Calculate $p_l$ as $(p_{max} + (p_{x} + p(1,0))/2)/2$
- Calculate $p_c$ as $(p_r + p_l)/2$

In this way also calculated $p(1,2)$ and $p(2,1)$ using the above formula.

The interpolated pixels are $p_r$, $p_l$, $p_c$, $p(1,2)$, and $p(2,1)$ and their location in the image is shown in above figure.

B. Data embedding phase with PVD Technique

Step1. Select the maximum and the minimum values among the four pixel values.

Step2. Calculate the difference value $d$ between the maximum pixel value and the minimum pixel value using the following formula,

$$d = v_{max} - v_{min},$$

Where,

$v_{max} = \max(v(x+1,y), v(x,y+1), v(x+1,y+1))$ and $v_{min} = \min(v(x+1,y), v(x,y+1), v(x+1,y+1))$

Step3. Using the above equations, the target pixel is either included in an edge area or in a smooth area. using the range Table determine the lower boundary of the pixel difference.
Suppose the lower boundary is \( l \)

**Table 1. Quantization ranges for Type 1**

<table>
<thead>
<tr>
<th>Range</th>
<th>No. of bits to be hidden</th>
</tr>
</thead>
<tbody>
<tr>
<td>R=[0,7)</td>
<td>3</td>
</tr>
<tr>
<td>R=[8,15]</td>
<td>3</td>
</tr>
<tr>
<td>R=[16,31]</td>
<td>4</td>
</tr>
<tr>
<td>R=[32,63]</td>
<td>4</td>
</tr>
<tr>
<td>R=[64,127]</td>
<td>4</td>
</tr>
<tr>
<td>R=[128,255]</td>
<td>4</td>
</tr>
</tbody>
</table>

Step 4. Calculate \( n = \log_2 (lb) \); if \( d > 3 \).

\( n = 1; \) otherwise.

Step 5. Calculate a temporary value \( t(x, y) = (v(x, y) \mod 2^n) \), where \( b \) is the data to be hidden.

Step 6. Calculate

\[
T_1 = t(x, y) \quad \text{if} \quad (-2^n - 1)/2 \leq T(x, y) < (2^n - 1)/2
\]

\[
T_1 = t(x, y) + 2^n \quad \text{if} \quad (-2^n + 1) \leq T(x, y) < (-2^n - 1)/2
\]

\[
T_1 = t(x, y) \quad \text{if} \quad (2^n - 1)/2 < T(x, y) < 2^n
\]

Step 7. \( v_1(x, y) = v(x, y) + T_1(x, y) \).

Where \( v_1(x, y) \) is the new pixel value.

### 2.3 Data Extracting Process

Step 1. Calculate ‘\( n \)’ in the same way as in data embedding method.

Step 2. The target pixel value presents in \( v(x, y) \).

Step 3. The data hidden is \( b = v_1(x, y) \mod 2^n \)

**III. MATHEMATICAL EXPLANATIONS**

Take the pixel block in 2X2 manner using Raster Scan method.

This is the Cover image pixel block

<table>
<thead>
<tr>
<th>100</th>
<th>150</th>
</tr>
</thead>
<tbody>
<tr>
<td>120</td>
<td>90</td>
</tr>
</tbody>
</table>

Now, Applying Nearest neighbour Interpolation method.

Here, \( p_x = 100 \), and \( P_{\text{max}} = 150 \)

Now, \( p_r = (150+(100+150)/2)/2 = 138 \)

Similarly,

\( p_l = (150+(100+120)/2)/2 = 130 \)

\( p_{(1,2)} = (150+(150+90)/2)/2 = 135 \)

\( p_c = (138 + 130)/2 = 134 \)

\( p_{(2,1)} = (150+(120+90)/2)/2 = 128 \)

After that moving towards data embedding.

Take 2X2 Pixel block, i.e,

Consider the secret data bit stream is 111001110011

Now, \( V_{\text{max}} = 138 \), and \( V_{\text{min}} = 130 \).

\( d = |138-130| = 8 \)

so, \( d \) value is in the range \([8-15]\). So, the \( lb=8 \), then calculate, \( n = \log_2 (8) = 3 \).

According to the range table the no. of hidden bite is 3, so, the first 3 bit is \((111)_2 = (7)_{10} = b \)

\( t(x, y) = 7 - (100 \mod 2^3) = 3 \)

so, new pixel value is \( = 100+3 = 103 \)
The new stego pixel block after data embedding is:

<table>
<thead>
<tr>
<th>103</th>
<th>138</th>
</tr>
</thead>
<tbody>
<tr>
<td>130</td>
<td>134</td>
</tr>
</tbody>
</table>

Moving towards data extraction, pixel value = 103

Now, $V_{\text{max}} = 138$, and $V_{\text{min}} = 130$.

$$d = |138-130| = 8$$

so, d value is in the range [8-15]. So, the lb = 8, then calculate, $n = \log_2(8) = 3$.

$$103 \mod 2^3 = 7 = (111)_2$$

**IV. RESULTS & DISCUSSIONS**

The proposed method is verified by MATLAB. Here we take three Sample Cover image as shown below. After hiding 756035 bits of data the following stego image is observed.

![Fig 1. Cover Image](image1.png)

![Fig 2. Stego Image (using Type 1)](image2.png)

**Table 2. PSNR and the hiding capacity of the proposed image**

<table>
<thead>
<tr>
<th>Image</th>
<th>PSNR</th>
<th>Hiding capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>42.86</td>
<td>2365795</td>
</tr>
<tr>
<td>Boat</td>
<td>38.39</td>
<td>2370158</td>
</tr>
<tr>
<td>Baboon</td>
<td>35.56</td>
<td>2427365</td>
</tr>
</tbody>
</table>

**V. CONCLUSION**

Steganography techniques along with the principles of PVD and interpolation measures by three issues: (i) fall of boundary problem (FOBP), (ii) pixel difference histogram (PDH) analysis, and (iii) RS analysis. This paper proposes a steganography technique in onre variants using PVD with interpolation techniques. The
first type operates on $2 \times 2$ pixel blocks and after interpolation it is $3 \times 3$ pixel block and the second type operates on same manner. Based on the new value of this pixel after nearest neighbour interpolation, difference values with other neighboring pixels are calculated. Using these differences, PVD approach is applied. The experimental results such as data hiding capacity and PSNR are satisfactory.

VI. REFERENCES


[23]. G. Swain, "Digital image steganography using eight directional PVD against RS analysis and PDH analysis," Advances in Multimedia.


**Cite this article as:**


Journal URL : http://ijsrst.com/IJSRST207111