Research Article

Data-Hiding Scheme Using Multidirectional Pixel-Value Differencing on Colour Images

Pyung-Han Kim,1 Eun-Jun Yoon,2 Kwan-Woo Ryu,1 and Ki-Hyun Jung2

1School of Computer Science and Engineering, Graduate School, Kyungpook National University, 1370 Sankyuk-Dong, Buk-Gu, Daegu 702-701, Republic of Korea
2Department of Cyber Security, Kyungil University, Gyungbuk 38428, Republic of Korea

Correspondence should be addressed to Ki-Hyun Jung; khanny.jung@gmail.com

Received 27 March 2019; Accepted 17 September 2019; Published 31 October 2019

Academic Editor: Debasis Giri

Copyright © 2019 Pyung-Han Kim et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Data hiding is a technique that hides the existence of secret data from malicious attackers. In this paper, we propose a new data-hiding scheme using multidirectional pixel-value differencing, which can embed secret data in two directions or three directions on colour images. The cover colour image is divided into nonoverlapping blocks, and the pixels of each block are decomposed into R, G, and B channels. The pixels of each block perform regrouping, and then the minimum pixel value within each block is selected. The secret data can be embedded into two directions or three directions based on the minimum pixel value by using the difference value for the block. The pixel pairs with the embedded secret data are put separately into two stego images for secret data extraction on receiver sides. In the extraction process, the secret data can be extracted using the difference value of the two stego images. Experimental results show that the proposed scheme has the highest embedding capacity when the secret data are embedded into three directions. Experimental results also show that the proposed scheme has a high embedding capacity while maintaining the degree of distortion that cannot be perceived by human vision system for two directions.

1. Introduction

In recent years, the use of the Internet has become more increased owing to the development of computer performance and communication technology. Therefore, digital contents such as image, video, movie, and audio files are generally used to transmit and receive each other on the Internet. Digital contents have many advantages such as convenience of transmission and ease of use. Therefore, information exchange using digital contents is becoming common. However, digital contents are easy to change and can be duplicated on the Internet that has the characteristics of an open space. Thus, there are many problems that can infringe on the copyright of an individual or an organization. To solve these problems, cryptographic techniques and data-hiding techniques are used to prevent illegal use of information. Cryptography encrypts data with embedded secret data [1, 2]. Cryptography can prevent the transmitted data from being manipulated or leaked. On the other hand, data-hiding techniques hide the existence of secret data [3, 4]. Therefore, malicious attackers cannot know the existence of secret data in digital contents. Data hiding or digital watermarking techniques are used steadily for complete digital information and copyright protection. Watermarking embeds a watermark on digital contents to prevent copyright problems [5, 6]. Data-hiding techniques can be divided into various categories according to classification criteria. Data-hiding methods can be classified into hidden channel technique, steganography technique, anonymity technique, and technique for hiding copyright information. The covert channel technique reduces the signal-to-noise ratio in order to reduce the bandwidth of the base channel, so that the secret data are not exposed to others [7, 8]. Therefore, only authorized senders and receivers can know whether the secret data exist or not. In other words, it is a technique to transmit secret data through a secret path.
Steganography is a technique that hides the existence of secret data [9–11]. Steganography can hide the secret data in common digital contents such as image, audio, and video file, so that the secret data to be transmitted cannot be detected by human senses. Conventional cryptography technique sends the encrypted data together with secret data to conceal confidential information, while steganography is related to hide the existence of secret data. Anonymity is a technique that hides the subject of communication and conceals the identity of the sender and the receiver that transmit and receive secret data, where the secret channel between the sender and the receiver is not exposed [12]. Information hiding techniques for hiding copyright information can be categorized into robustness and ductility. Watermarking and fingerprinting are robustness methods. The watermarking technique records copyright information in a video, audio file, or image file for copyright protection. If attackers attempt to modify the digital watermarking information in an illegal manner, the original video or audio files cannot be used. Fingerprinting is a technique that inserts buyer information into contents to track which purchaser has started illegal distribution of contents when illegal distribution of contents occurs [13]. In particular, data-hiding techniques can be classified into data-hiding method and reversible data-hiding method. The data-hiding methods using digital images embed the secret data after changing the pixels of the original cover image. Therefore, the stego image having the embedded secret data is distorted. In order to solve distortion problems, various techniques have been suggested, but such distortions have been acted sensitively in the fields of military, medical, and artwork. As a result, reversible data-hiding methods are being actively researched not only to recover the original cover image but also to extract the secret data [14, 15]. LSB (Least Significant Bit) and PVD (Pixel-Value Differencing) are typical examples of data-hiding techniques. The LSB is a technique to hide secret data into the least significant bits so that it cannot be easily recognized by the human eye [3]. Generally, when secret data are hidden by using up to 3 least significant bits, distortion of the image cannot be perceived by human eyes. However, image distortion can be perceived by human eyes when the least significant bits are used more than 4. In order to overcome the distortion problem, the optimal LSB replacement algorithm has been proposed [16], and Wang et al. proposed an improved scheme using the genetic algorithm [17]. The PVD scheme proposed by Wu and Tsai uses difference values of two consecutive pixels in a block to determine the size of the secret data [18]. Also, an improved PVD scheme using the LSB replacement method for the smooth area of the cover image has been proposed by Wu et al. [19]. Wang et al.'s scheme was proposed to improve the image quality by applying the coefficient function to the PVD scheme [20]. In 2009, Chang et al. proposed a dual image-based data-hiding scheme that could embed secret data into two images [21]. Chang et al.'s scheme improved the function of EMD (Exploiting Modification Direction) scheme which used secret data based on pentadecimal number [22]. However, the embedding capacity of secret data was low in EMD scheme, so Chang et al.'s scheme solved the low embedding capacity problem by using dual image. Lee et al.'s scheme embedded secret data into two images using four directions [23]. Qin et al.'s scheme performed different embedding processes on the two images [24]. The EMD scheme is used for the first image, and three rules are applied to the second image based on the first image to embed the secret data. Lu et al.'s scheme reduced image distortion using CFS (Center Folding Strategy) method, where two stego images using the up and down functions were produced [25]. In 2017, Yao et al. proposed a dual image-based data-hiding scheme using selection strategy of shiftable pixel's coordinates to improve the scheme proposed by Lu et al. [26]. The technique using PVD on colour image was proposed by Nagaraj et al.'s scheme uses modulus three function with PVD to embed the secret message bits into the colour image [27]. Prema and Manimegalai proposed a technique using three pairs of {(R, G), (G, B), (B, R)} and modified PVD scheme [28]. Swain et al. proposed an adaptive PVD-based colour image-hiding scheme [29]. In 2017, Shiv and Arup proposed a technique to apply PVD scheme to overlapping blocks on colour image. In Shiv and Arup’s scheme, colour image is grouped into two pairs (R, G) and (G, B). The PVD scheme is applied to each pixel pair and performs a reconditioning step to obtain a modified stego image. The concept of redundant blocks is considered to increase embedding capacity. Although there are many techniques to use the PVD on colour image, it still have to improve the image quality and the embedding capacity. In this paper, a novel steganography scheme using the PVD to multidirections on colour images is proposed. We divide a colour image into nonoverlapping blocks and decompose the colour pixels in each block into R, G, and B. The decomposed pixels perform regrouping and find the minimum value to apply the PVD scheme in two directions or three directions. The pairs of pixels on which the PVD scheme was performed are stored in two images and generate two stego images. The remainder of this paper is organized as follows. The pixel-value differencing, data hiding in dual images, and the pixel-value differencing on colour images are explained in Section 2. The proposed scheme is described in Section 3, and the experimental results are analysed in Section 4. Finally, the conclusions are described in Section 5.

2. Related Works

In this section, the Wu and Tsai’s PVD scheme and Chang et al.’s dual image-based data-hiding scheme are explained [18, 21]. In addition, we describe the PVD based on the colour image proposed by Shiv and Arup [30].

2.1. PVD Scheme. PVD technique determines the size of the secret data that can be hidden by using the difference value of two consecutive pixels in a block. There exists a smooth area and an edge area in images. The edge region is relatively more complicated than the smooth region. When the image is distorted, the change of the smooth area in the human eye can be well distinguished, but the change of the edge area is not well
distinguished. Therefore, we can hide more secret data in the edge area than in the smooth area when hiding the secret data in an image. In the PVD scheme, the cover image is separated into blocks, and two consecutive pixels in an each block are used which are defined as $p_i$ and $p_{i+1}$. The pixel values of $p_i$ and $p_{i+1}$ are defined as $g_i$ and $g_{i+1}$, and the difference value $d_i$ of two pixels is calculated using the following equation:

$$d_i = g_{i+1} - g_i,$$  

(1)

The difference value $d_i$ ranges from $-255$ to $255$. If $d_i$ has a value close to 0, it is located in the smooth region, whereas if $d_i$ has a value close to $-255$ and $255$, it is located in the edge region. When the defined range is $R_i$ and $i$ has a range from 1 to $n$, $l_i$ is defined as the lowest value, and $u_i$ is defined as the highest value. The range table is defined in Figure 1.

When the $i$-th block $B$ has the difference value $d_i$, the bits can be embedded in the block $B$ are calculated by the following equation:

$$n = \log_2(u_i - l_i + 1).$$  

(2)

The parameter $n$ denotes the number of embeddable secret bits. The $n$ binary secret bits are converted into secret data $b$ in decimal. The new difference value $d'_i$ is calculated by equation (3) after inserting the secret data.

$$d'_i = \begin{cases} l_i + b_i, & \text{for } d'_i \geq 0, \\ -(l_i + b_i), & \text{for } d'_i < 0. \end{cases}$$  

(3)

The value of $b$ has a range from 0 to $u_i - l_i$, so $d'_i$ has a range from $l_i$ to $u_i$. When the value of $d'_i$ is calculated, a new pixel value $(g'_i, g'_{i+1})$ is calculated from the following equation:

$$(g'_i, g'_{i+1}) = \begin{cases} \left( g_i + \frac{m}{2}, g_{i+1} - \frac{m}{2} \right), & \text{if } g_i \geq g_{i+1} \text{ and } d'_i \geq d_i, \\ \left( g_i - \frac{m}{2}, g_{i+1} + \frac{m}{2} \right), & \text{if } g_i < g_{i+1} \text{ and } d'_i > d_i, \\ \left( g_i - \frac{m}{2}, g_{i+1} + \frac{m}{2} \right), & \text{if } g_i \geq g_{i+1} \text{ and } d'_i \leq d_i, \\ \left( g_i + \frac{m}{2}, g_{i+1} - \frac{m}{2} \right), & \text{if } g_i < g_{i+1} \text{ and } d'_i \leq d_i. \end{cases}$$  

(4)

2.2. PVM Scheme. In 2013, Nagaraj et al. proposed a PVM (Pixel-Value Modification) scheme using a modulus 3 function. The colour cover image is decomposed into R, G, and B, and the modulus 3 operation is performed. The result of the modulus 3 operation is compared with the ternary secret data, and the cover image pixel value is changed according to the compared result. The embedding algorithm is given in Algorithm 1.

In the extraction process, the stego image is separated into R, G, and B. And the modulus 3 operation is performed on all the pixels to extract the ternary secret data. Finally, the ternary secret data are transformed into the original secret data.

2.3. Shiv and Arup's Scheme. In 2017, Shiv and Arup proposed a PVD scheme based on RGB colour image. RGB colour image is separated into R, G and B grayscale images, and two pairs (R, G) and (G, B) are created for all pixel values for each R, G, and B grayscale images. Then the PVD scheme is applied to generate $R_1$, $G_1$, $G_2$, and $B_1$ for the two pairs. A stego RGB image is generated using the average values of $G_1$ and $G_2$ and the adjusted values of $R_1$ and $B_1$. The embedding algorithm is given in Algorithm 2.

In the extraction process, the stego RGB image is separated into $R_s$, $G_s$, and $B_s$. And two pairs $(R_s, G_s)$ and $(G_s, B_s)$ are created. Then, the extraction algorithm of PVD scheme is applied to $(R_s, G_s)$ and $(G_s, B_s)$ to extract secret data.

3. The Proposed Scheme

In this paper, we divide colour image into nonoverlapping blocks, and pixel values in each block decompose into R, G, and B. In the embedding process, the R, G, and B pixel values of each block are regrouped to apply the PVD scheme in two directions or three directions. In order to embed the secret data, we find the minimum value in the regrouped blocks. The secret data are embedded in two directions or three directions based on the minimum value. We split two pixels of each pair into two images for the perfect extraction of the secret data. In the extraction process, we extract the secret data by applying extraction algorithm of PVD scheme in two stego images (Algorithms 3 and 4).

4. Experimental Results

In this section, we analyse PSNR, quality index, and embedding capacity for performance evaluation in the proposed scheme. In the data hiding scheme, PSNR is measuring the degree of distortion between the cover image and the stego image by using the following equation:

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

(5)

The mean square error is calculated using the following equation:

<table>
<thead>
<tr>
<th>$R_1$</th>
<th>$R_2$</th>
<th>$R_3$</th>
<th>$R_4$</th>
<th>$R_5$</th>
<th>$R_6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower: 0</td>
<td>Lower: 8</td>
<td>Lower: 16</td>
<td>Lower: 32</td>
<td>Lower: 64</td>
<td>Lower: 128</td>
</tr>
</tbody>
</table>

Figure 1: Range table.
The embedding algorithm of PVM scheme is as follows.
Step 1: Separate RGB colour image into R, G, and B channels
Step 2: Convert decimal secret data to generate ternary secret data \( d \)
Step 3: Perform modulus 3 operation on the all pixel values of the R, G, and B grayscale images to generate \( f \)
Step 4: Convert the cover image pixel value \( c_i \) to the stego image pixel value \( s_i \) according to the following conditions.

\[
\text{Case 1:} \quad f = d, \text{ then not modified} \\
\text{Case 2:} \quad f \neq d \text{ and } f < d, \text{ then } s_i = c_i + 1 \\
\text{Case 3:} \quad f \neq d \text{ and } f > d, \text{ then } s_i = c_i - 1
\]
Step 5: Merge R, G, and B to generate a stego image.

\textbf{Algorithm 1: Embedding algorithm.}

The embedding algorithm of Shiv and Arup’s scheme is as follows.
Step 1: Separate RGB colour image into R, G, B channels
Step 2: Create two pairs (R, G) and (G, B)
Step 3: Compute \( t_1 \) and \( t_2 \) for the threshold: \( t_1 = |R - G| \), \( t_2 = |G - B| \)
Step 4: Perform Steps 5 through 7. If the threshold is less than the sum of \( t_1 \) and \( t_2 \), then the pixels in \( C \) will be embedded.
Step 5: Apply the PVD scheme to generate \((R_1, G_1)\) and \((G_2, B_1)\) on two pairs
Step 6: Calculate the average value of \( G_1 \) and \( G_2 \) to generate \( G_s \): \( G_s = \frac{G_1 + G_2}{2} \)
Step 7: Calculate \( R_s, B_s \) using \( R_s = R_1 - (G_1 - G_s) \), \( B_s = B_1 - (G_2 - G_s) \)
Step 8: Repeat Steps 1 through 7 for all pixels

\textbf{Algorithm 2: Embedding algorithm.}

The embedding algorithm is as follows.
Step 1: Decompose the colour image \( C \) into 2 \( \times \) 2 size blocks. If the \( i \)-th block is \( C_i \), then the pixels in \( C_i \) are defined as \( C_{i,j} (0 \leq j, k \leq 1) \).
Step 2: In this step, \( G_{i,j} \) and \( B_{i,j} \) are defined as \( G_{i,j} = \min(G_{i,0}, G_{i,1}) \) and \( B_{i,j} = \min(B_{i,0}, B_{i,1}) \) for the following equation: \( G_{i,j} = (R_{i,j}, G_{i,j}, B_{i,j}) \), \( G_{i,0} = (R_{i,0}, G_{i,0}, B_{i,0}) \), \( R_{i,0} = (R_{i,0}, 0, 0) \), \( G_{i,0} = (G_{i,0}, 0, 0) \), \( B_{i,0} = (B_{i,0}, 0, 0) \), \( G_{i,1} = (G_{i,1}, 0, 0) \), and \( B_{i,1} = (B_{i,1}, 0, 0) \).
Step 3: Regroup the \( R_{i,j}, G_{i,j} \), and \( B_{i,j} \) pixel values in the block \( C_i \) to generate \( NR_{i,j}, NG_{i,j} \), and \( NB_{i,j} \) for the following equation: \( NR_{i,j} = (NR_{i,0}, NR_{i,1}), NG_{i,j} = (NG_{i,0}, NG_{i,1}), NB_{i,j} = (NB_{i,0}, NB_{i,1}) \).
Step 4: Find the minimum pixel value of \( NR_{i,j}, NG_{i,j} \), and \( NB_{i,j} \), respectively. The min function returns the minimum value: \( \min NR_{i,j} = \min(R_{i,0}, R_{i,1}), \min NG_{i,j} = \min(G_{i,0}, G_{i,1}), \min NB_{i,j} = \min(B_{i,0}, B_{i,1}) \).
Step 5: Generate pairs in two directions or three directions.

**Algorithm 3: The proposed embedding algorithm.**

In this step, generated \( RI_1 \) and \( RI_2 \) associated with R channel. \( GI_1 \) and \( GI_2 \) are generated in the G channel, and \( BI_1 \) and \( BI_2 \) are generated in the B channel.
Step 8: Generates two stego images \( S_C \) and \( S_B \) by using the following equation. The merge function combines R, G, and B to produce a colour image: \( S_C = \max (RI_1, GI_1, BI_1) \) for \( 1 \leq t \leq 2 \).
Step 9: Repeat the above steps for all blocks.
In the extraction process, we split the two stego colour images into nonoverlapping blocks and decompose each colour image into R, G, and B. Then, the PVD extraction algorithm is applied to R, G, and B to extract secret data. The extraction algorithm is as follows. Step 1: Divide the two stego colour images $S_C$ and $S_C$ into $2 \times 2$ size blocks. If the $i$-th block is $S_C^i (0 \leq t \leq 1)$, then the pixels in $S_C^i$ are defined as $S_C^i_{j,k} (0 \leq j, k \leq 1)$. Step 2: Decompose two stego colour images $S_C$ and $S_C$ into R, G, and B. $S_C$ is decomposed into $R_I$, $G_I$, and $B_I$. Step 3: Extract the secret data by using the following equation. $pvd_{EA}$ means extraction algorithm of PVD scheme. $\text{secret data} = pvd_{EA} (R_I, R_I) \parallel pvd_{EA} (G_I, G_I) \parallel pvd_{EA} (B_I, B_I)$. Step 4: Repeat the above Steps for all blocks.

**Algorithm 4:** The proposed extraction algorithm.

**Figure 2:** Two pairs in two directions. (a) Case 1: minimum value position (0, 0). (b) Case 2: minimum value position (0, 1). (c) Case 3: minimum value position (1, 0). (d) Case 1: minimum value position (1, 1).

**Figure 3:** Three pairs in three directions. (a) Case 1: minimum value position (0, 0). (b) Case 2: minimum value position (0, 1). (c) Case 3: minimum value position (1, 0). (d) Case 1: minimum value position (1, 1).

**Figure 4:** Distributed pixels in two pairs.

**Figure 5:** Distributed pixels in three pairs.
\[ \text{MSE} = \sum_{i=1}^{W \times H} \frac{(p_i - \bar{p}_i)^2}{W \times H}. \]  

When the size of the image is given as \( M \times N \), the cover image is \( I \) and the stego image is \( I' \). If the PSNR value is more than 30 dB, the image distortion cannot be detected by human eyes. The quality index is an indicator of the correlation between two images. If quality index is 1, the two images are the same. Conversely, if the quality index is \(-1\), the two images are different images. The quality index is shown in the following equation:

\[ Q = \frac{4 \delta_{xy} \delta_{x} \delta_{y}}{\delta_{x}^2 + \delta_{y}^2} \left( \frac{\delta_{x}^2}{\delta_{x}^2 + \delta_{y}^2} \right). \]

The equations for each element of equation (8) are as follows:

\[ \bar{p}_x = \frac{1}{wh} \sum_{i=0}^{wh-1} p_i, \]

\[ \bar{p}_y = \frac{1}{wh} \sum_{i=0}^{wh-1} p'_i, \]

\[ \delta_x^2 = \frac{1}{wh-1} \sum_{i=0}^{wh-1} (p_i - \bar{p}_x)^2, \]

\[ \delta_y^2 = \frac{1}{wh-1} \sum_{i=0}^{wh-1} (p'_i - \bar{p}_y)^2, \]

\[ \delta_{xy} = \frac{1}{wh-1} \sum_{i=0}^{wh-1} (p_i - \bar{p}_x)(p'_i - \bar{p}_y). \]

The quality index is defined as the combination of loss of correlation, luminance distortion, and contrast distortion which is redefined as the following equation:

\[ Q = \frac{2 \delta_{xy} \delta_x \delta_y}{\delta_x^2 + \delta_y^2} \left( \frac{2 \delta_{xy} \delta_x \delta_y}{\delta_x^2 + \delta_y^2} \right). \]

The correlation coefficient between the two images is \( \delta_{xy}/\delta_x \delta_y \). The luminance between the two images measures by using \( 2 \frac{\delta_x^2 \delta_y^2}{\delta_x^2 + \delta_y^2} \), and the similarity of the two images measures by using \( 2 \frac{\delta_x \delta_y \delta_{xy}}{\delta_x^2 + \delta_y^2} \). The embedding capacity means the size of the secret data that can be embedded into the cover image. Figure 6 shows the 512×512 sized colour images used in the experiment.

Figure 7 shows \( RI_1, RI_2, GI_1, GI_2, BI_1, BI_2, S_1C, \) and \( S_2C \) for Lena image after to perform the PVD scheme in three directions. Table 1 compares the PSNR of the proposed scheme with other schemes. The proposed scheme generates two stego images. The PSNR value of the first stego image is PSNR-1 and the PSNR value of the second stego image is PSNR-2. In the case of embedding secret data in two directions, the each PSNR value of the proposed scheme is similar to Shiv and Arup’s scheme or about 1.5 dB lower. And the PSNR value of the proposed scheme is about 10 dB lower than Wu and Tsai’s scheme and about 8 dB lower than Nagaraj et al.’s scheme. However, the proposed scheme keeps the PSNR value above 30 dB on average, so it cannot detect image distortion by human eyes.
Table 2 compares the embedding capacity of the proposed scheme and other schemes. The embedding capacity of the proposed scheme is about 2,400,000 bits higher than Wu and Tsai’s scheme and about 1,500,000 bits higher than Nagaraj et al.’s scheme. Also, the embedding capacity of the proposed scheme is about 1,350,000 bits higher than Shiv and Arup’s scheme and about 1,330,000 bits higher than Prema and Manimegalai’s scheme. As a result, the proposed scheme maintains the PSNR of 30 dB or more while the embedding capacity of the secret data is much higher than other
Table 1: Comparison of PSNR for the proposed scheme and other schemes.

<table>
<thead>
<tr>
<th>Images</th>
<th>Wu and Tsai’s scheme [18]</th>
<th>Nagaraj el al.’s scheme [27]</th>
<th>Prema and Manimegalai’s scheme [28]</th>
<th>Shiv and Arup’s scheme [30]</th>
<th>Proposed scheme (two directions)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Colour image PSNR (dB)</td>
<td>Colour image PSNR (dB)</td>
<td>Colour image PSNR (dB)</td>
<td>Colour image PSNR (dB)</td>
<td>S_C PSNR-1 (dB) S_C PSNR-2 (dB)</td>
</tr>
<tr>
<td>Lena</td>
<td>40.0379</td>
<td>49.8948</td>
<td>43.7399</td>
<td>30.9793</td>
<td>30.9791 32.2565 30.9791</td>
</tr>
<tr>
<td>Tiffany</td>
<td>41.6758</td>
<td>49.9241</td>
<td>43.8679</td>
<td>31.2709</td>
<td>30.2070 30.4749 30.3409</td>
</tr>
<tr>
<td>Macaw</td>
<td>41.4435</td>
<td>50.0031</td>
<td>43.8326</td>
<td>30.4724</td>
<td>30.5083 32.7829 31.6456</td>
</tr>
<tr>
<td>Beach</td>
<td>43.1482</td>
<td>49.9013</td>
<td>42.1780</td>
<td>41.0727</td>
<td>35.1747 36.2268 35.7007</td>
</tr>
<tr>
<td>Pens</td>
<td>41.8196</td>
<td>49.8866</td>
<td>43.1339</td>
<td>32.6592</td>
<td>29.8021 32.4704 31.1362</td>
</tr>
<tr>
<td>Girl</td>
<td>41.7187</td>
<td>49.8949</td>
<td>43.0240</td>
<td>32.8201</td>
<td>30.2782 32.9632 31.6207</td>
</tr>
<tr>
<td>Cat</td>
<td>42.5678</td>
<td>49.8925</td>
<td>43.7878</td>
<td>37.4366</td>
<td>34.0405 36.0262 35.0333</td>
</tr>
<tr>
<td>Flower</td>
<td>42.0581</td>
<td>49.8871</td>
<td>43.2004</td>
<td>31.2419</td>
<td>30.3256 38.8220 31.6038</td>
</tr>
<tr>
<td>Average</td>
<td>41.8087</td>
<td>49.9105</td>
<td>43.3480</td>
<td>33.4708</td>
<td>31.4144 33.2603 32.3373</td>
</tr>
</tbody>
</table>

Table 2: Comparison of embedding capacity of the proposed scheme and other schemes.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>1,248,890</td>
<td>524,457</td>
<td>2,305,342</td>
<td>2,516,141</td>
<td>3,739,287</td>
</tr>
<tr>
<td>Tiffany</td>
<td>1,225,240</td>
<td>523,641</td>
<td>2,306,347</td>
<td>2,508,341</td>
<td>3,739,287</td>
</tr>
<tr>
<td>Macaw</td>
<td>1,211,869</td>
<td>524,261</td>
<td>2,328,347</td>
<td>2,330,341</td>
<td>3,643,723</td>
</tr>
<tr>
<td>Beach</td>
<td>1,188,477</td>
<td>523,896</td>
<td>2,305,296</td>
<td>1,588,798</td>
<td>3,643,723</td>
</tr>
<tr>
<td>Pens</td>
<td>1,208,497</td>
<td>524,351</td>
<td>2,307,066</td>
<td>1,918,829</td>
<td>3,643,723</td>
</tr>
<tr>
<td>Girl</td>
<td>1,234,315</td>
<td>524,351</td>
<td>2,307,919</td>
<td>1,919,833</td>
<td>3,670,028</td>
</tr>
<tr>
<td>Cat</td>
<td>1,193,828</td>
<td>524,330</td>
<td>2,305,296</td>
<td>1,700,834</td>
<td>3,591,096</td>
</tr>
<tr>
<td>Flower</td>
<td>1,206,025</td>
<td>524,733</td>
<td>2,305,305</td>
<td>2,255,479</td>
<td>3,621,236</td>
</tr>
<tr>
<td>Average</td>
<td>1,214,643</td>
<td>524,256</td>
<td>2,308,871</td>
<td>2,046,834</td>
<td>3,648,148</td>
</tr>
</tbody>
</table>

Table 3: Comparison of Quality index values of the proposed scheme and Shiv and Arup’s scheme.

<table>
<thead>
<tr>
<th>Images</th>
<th>Shiv and Arup’s scheme [30] Quality index</th>
<th>Proposed scheme Quality index Two directions</th>
<th>Three directions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>0.6870</td>
<td>0.7653 0.7325</td>
<td>0.7735 0.7148</td>
</tr>
<tr>
<td>Tiffany</td>
<td>0.4686</td>
<td>0.4181 0.4563</td>
<td>0.3767 0.4863</td>
</tr>
<tr>
<td>Macaw</td>
<td>0.4486</td>
<td>0.4456 0.4401</td>
<td>0.4477 0.4348</td>
</tr>
<tr>
<td>Beach</td>
<td>0.3297</td>
<td>0.3346 0.3284</td>
<td>0.3451 0.3190</td>
</tr>
<tr>
<td>Pens</td>
<td>0.2370</td>
<td>0.2248 0.2354</td>
<td>0.2221 0.2362</td>
</tr>
<tr>
<td>Girl</td>
<td>0.0712</td>
<td>0.0719 0.0693</td>
<td>0.0733 0.0677</td>
</tr>
<tr>
<td>Cat</td>
<td>0.3792</td>
<td>0.3804 0.3755</td>
<td>0.3802 0.3756</td>
</tr>
<tr>
<td>Flower</td>
<td>0.3294</td>
<td>0.3415 0.3344</td>
<td>0.3456 0.3300</td>
</tr>
<tr>
<td>Average</td>
<td>0.3688</td>
<td>0.3727 0.3714</td>
<td>0.3705 0.3705</td>
</tr>
</tbody>
</table>

Table 4: Comparison of experimental results of two-way embedding and three-way embedding.

<table>
<thead>
<tr>
<th>Images</th>
<th>PSNR-1 (dB)</th>
<th>PSNR-2 (dB)</th>
<th>Capacity (bits)</th>
<th>PSNR-1 (dB)</th>
<th>PSNR-2 (dB)</th>
<th>Capacity (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>30.9791</td>
<td>32.2565</td>
<td>3,739,287</td>
<td>26.9258</td>
<td>29.5024</td>
<td>5,671,307</td>
</tr>
<tr>
<td>Tiffany</td>
<td>30.2070</td>
<td>30.4749</td>
<td>3,678,830</td>
<td>27.6425</td>
<td>30.8193</td>
<td>5,557,627</td>
</tr>
<tr>
<td>Macaw</td>
<td>30.5083</td>
<td>32.7829</td>
<td>3,643,723</td>
<td>28.0548</td>
<td>30.2345</td>
<td>5,507,035</td>
</tr>
<tr>
<td>Beach</td>
<td>35.1747</td>
<td>36.2268</td>
<td>3,597,199</td>
<td>32.1241</td>
<td>35.2979</td>
<td>5,420,140</td>
</tr>
<tr>
<td>Pens</td>
<td>29.8021</td>
<td>32.4704</td>
<td>3,643,788</td>
<td>28.2435</td>
<td>30.0250</td>
<td>5,563,465</td>
</tr>
<tr>
<td>Cat</td>
<td>34.0405</td>
<td>36.0262</td>
<td>3,591,096</td>
<td>33.2151</td>
<td>35.9475</td>
<td>5,429,264</td>
</tr>
<tr>
<td>Flower</td>
<td>30.3256</td>
<td>32.8820</td>
<td>3,621,236</td>
<td>29.1141</td>
<td>31.1358</td>
<td>5,494,673</td>
</tr>
<tr>
<td>Average</td>
<td>31.4144</td>
<td>33.2603</td>
<td>3,648,148</td>
<td>29.2551</td>
<td>31.6800</td>
<td>5,530,670</td>
</tr>
</tbody>
</table>
Figure 9: (a) Flower cover image (b–d) R, G, B histograms of cover image  (e) Flower stego image (f–h) R, G, and B histograms of Shiv and Arup’s scheme.

Figure 10: Continued.
schemes. Table 3 compares the quality index of the proposed scheme and Shiv and Arup’s scheme. The quality index of the proposed scheme is similar with Shiv and Arup’s scheme. Table 4 shows the experimental results for each case where secret data are embedded in two directions and three directions in the proposed scheme. When embedding secret data in three directions, the PSNR value is about 2 dB lower in both stego images, but the embedding capacity is approximately 1,800,000 bits higher.

Figures 9 and 10 show histograms about frequency of image pixel values. In the histogram, the leftmost value means 0 and the rightmost value is 255. Pixels with a high frequency in the image have a high shape. As shown in Figures 9 and 10, the shape of the histogram changes when the secret data is embedded.

5. Conclusion
In this paper, a data-hiding scheme using multidirectional pixel-value differencing based on colour image has been proposed. The colour image was divided into non-overlapping sub-blocks and then decomposed with three channels. The minimum value was determined in the each block, and the pixel-value differencing scheme was applied in two or three directions based on the minimum value. Two or three pairs with the secret data were stored separately in two grayscale images. The proposed embedding method was performed on R, G, and B channels and combined the grayscale images into two colour stego images. The secret data were extracted using the pixel-value differencing on two or three directions. The experimental results demonstrated that the proposed scheme had a high embedding capacity and acceptable imperceptibility in the visual image quality. The proposed method could hide 1,601,314 bits more than previous method. In the future, new data-hiding schemes will be worked to increase the embedding capacity by combining the pixel-value differencing scheme and secret sharing scheme.

Data Availability
The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest
The authors declare that they have no conflicts of interest.

Acknowledgments
The authors thank the anonymous reviewers for their valuable suggestions that improved the clarity of this article. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1D1A1A09081842 and NRF-2018R1A2A2A05023180). This research project was supported by Ministry of Culture, Sports and Tourism (MCST) and from Korea Copyright Commission in 2018 (2018-f_drm-9500) and 2017 (2017-watermark-9500).

References

Figure 10: (a) Flower cover image. (b–d) R, G, and B histograms of cover image. (e) Flower stego image $S_{1C}$. (f–h) R, G, and B histograms of the proposed scheme on $S_{1C}$. (i) Flower stego image $S_{2C}$. (j–l) R, G, and B histograms of the proposed scheme on $S_{2C}$. 


Submit your manuscripts at
www.hindawi.com