Hindawi
Security and Communication Networks
Volume 2019, Article ID 9038650, 11 pages
https://doi.org/10.1155/2019/9038650

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 Jung**[2]

[1]*School of Computer Science and Engineering, Graduate School, Kyungpook National University, 1370 Sankyuk-Dong, Buk-Gu, Daegu 702-701, Republic of Korea*
[2]*Department 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

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 towing 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

R_1	R_2	R_3	R_4	R_5	R_6
Lower: 0 Upper: 7	Lower: 8 Upper: 15	Lower: 16 Upper: 31	Lower: 32 Upper: 63	Lower: 64 Upper: 127	Lower: 128 Upper: 255

Figure 1: Range table.

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:

$$d_i = g_{i+1} - g_i. \tag{1}$$

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:

$$n = \log_2(u_i - l_i + 1). \tag{2}$$

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.

$$d' = \begin{cases} l_i + b, & \text{for } d \geq 0, \\ -(l_i + b), & \text{for } d < 0. \end{cases} \tag{3}$$

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:

$$(g_i', g_{i+1}') = \begin{cases} \left(g_i + \left\lceil \frac{m}{2} \right\rceil, g_{i+1} - \left\lfloor \frac{m}{2} \right\rfloor\right), & \text{if } g_i \geq g_{i+1} \text{ and } d_i' > d_i, \\ \left(g_i - \left\lfloor \frac{m}{2} \right\rfloor, g_{i+1} + \left\lceil \frac{m}{2} \right\rceil\right), & \text{if } g_i < g_{i+1} \text{ and } d_i' > d_i, \\ \left(g_i - \left\lceil \frac{m}{2} \right\rceil, g_{i+1} + \left\lfloor \frac{m}{2} \right\rfloor\right), & \text{if } g_i \geq g_{i+1} \text{ and } d_i' \leq d_i, \\ \left(g_i + \left\lceil \frac{m}{2} \right\rceil, g_{i+1} - \left\lfloor \frac{m}{2} \right\rfloor\right), & \text{if } g_i < g_{i+1} \text{ and } d_i' \leq d_i. \end{cases} \tag{4}$$

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:

$$\text{PSNR} = 10 \times \log_{10} \frac{255^2}{\text{MSE}}. \tag{5}$$

The mean square error is calculated using the following equation:

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 $\mathbf{c_i}$ to the stego image pixel value $\mathbf{s_i}$ according to the following conditions.

Case 1: $\mathbf{f} = \mathbf{d}$, then not modified
Case 2: $\mathbf{f} \neq \mathbf{d}$ and $\mathbf{f} < \mathbf{d}$, then $\mathbf{s_i} = \mathbf{c_i} + 1$
Case 3: $\mathbf{f} \neq \mathbf{d}$ and $\mathbf{f} > \mathbf{d}$, then $\mathbf{s_i} = \mathbf{c_i} - 1$

Step 5: Merge R, G, and B to generate a stego image.

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 channel
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.
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: $G_s = G_1 + G_2/2$
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

Algorithm 2: Embedding algorithm.

The embedding algorithm is as follows.
Step 1: Divide the colour image C into 2×2 size blocks. If the i-th block is C^i, then the pixels in C^i are defined as: $C^i_{j,k}\ (0 \le j,k \le 1)$.
Step 2: Decompose the colour pixels in each block into R, G, and B. $C^i_{j,k}$ is decomposed into $R^i_{j,k}$, $G^i_{j,k}$, and $B^i_{j,k}\ (0 \le j,k \le 1)$ by the following equation: $C^i_{0,0} = (R^i_{0,0}, G^i_{0,0}, B^i_{0,0})$, $C^i_{0,1} = (R^i_{0,1}, G^i_{0,1}, B^i_{0,1})$, $C^i_{0,2} = (R^i_{0,2}, G^i_{0,2}, B^i_{0,2})$, $C^i_{0,3} = (R^i_{0,3}, G^i_{0,3}, B^i_{0,3})$
Step 3: Regroup the $R^i_{j,k}$, $G^i_{j,k}$, and $B^i_{j,k}$ pixel values in the block C^i to generate $NR^i_{j,k}$, $NG^i_{j,k}$, and $NB^i_{j,k}\ (0 \le j,k \le 1)$. $NR^i_{j,k} = (NR^i_{0,0} = R^i_{0,0}, NR^i_{0,1} = R^i_{0,1}, NR^i_{1,0} = R^i_{0,2}, NR^i_{1,1} = R^i_{0,3})$, $NG^i_{j,k} = (NG^i_{0,0} = G^i_{0,0}, NG^i_{0,1} = G^i_{0,1}, NG^i_{1,0} = G^i_{0,2}, NG^i_{1,1} = G^i_{0,3})$, $NB^i_{j,k} = (NB^i_{0,0} = B^i_{0,0}, NB^i_{0,1} = B^i_{0,1}, NB^i_{1,0} = B^i_{0,2}, NB^i_{1,1} = B^i_{0,3})$
Step 4: Find the minimum pixel value of $NR^i_{j,k}$, $NG^i_{j,k}$ and $NB^i_{j,k}$, respectively. The min function returns the minimum value. $\min NR^i_{j,k} = \min(NR^i_{0,0}, NR^i_{0,1}, NR^i_{1,0}, NR^i_{1,1})$, $\min NG^i_{j,k} = \min(NG^i_{0,0}, NG^i_{0,1}, NG^i_{1,0}, NG^i_{1,1})$, $\min NB^i_{j,k} = \min(NB^i_{0,0}, NB^i_{0,1}, NB^i_{1,0}, NB^i_{1,1})$.
Step 5: Generate pairs in two directions or three directions.

Step 5-1: Construct two pairs in two directions based on the minimum value as shown Figure 2. The same algorithm is performed on $NR^i_{j,k}$, $NG^i_{j,k}$ and $NB^i_{j,k}$. Therefore, we will explain only $NR^i_{j,k}$. If the minimum pixel value in $NR^i_{j,k}$ is $\min NR^i_{0,1}$, then the two pairs are $(\min NR^i_{0,1}, NR^i_{0,0})$ and $(\min NR^i_{0,1}, NR^i_{1,1})$.
Step 5-2: Construct three pairs in three directions based on the minimum value as shown Figure 3. The same algorithm is performed on $NR^i_{j,k}$, $NG^i_{j,k}$, and $NB^i_{j,k}$. Therefore, we will explain only $NR^i_{j,k}$. If the minimum pixel value in $NR^i_{j,k}$ is $\min NR^i_{0,1}$, then the three pairs are $(\min NR^i_{0,1}, NR^i_{0,0})$, $(\min NR^i_{0,1}, NR^i_{1,0})$, and $(\min NR^i_{0,1}, NR^i_{1,1})$.

Step 6: Apply PVD scheme in two directions or three directions.

Step 6-1: Perform the PVD scheme to two pairs for embeds the secret data. The two pairs after the PVD scheme is performed which are defined as $(S_1 NR^i_{0,1}, SNR^i_{0,0})$ and $(S_2 NR^i_{0,1}, SNR^i_{1,1})$.
Step 6-2: Perform the PVD scheme to three pairs for embeds the secret data. The three pairs after the PVD scheme is performed which are defined as $(S_1 NR^i_{0,1}, SNR^i_{0,0})$, $(S_2 NR^i_{0,1}, SNR^i_{1,0})$, and $(S_3 NR^i_{0,1}, SNR^i_{1,1})$.

Step 7: Distribute pixels in two pairs or three pairs to two images

Step 7-1: Distribute pixels in two pairs to two images RI_1 and RI_2 as shown Figure 4.
Step 7-2: Distribute pixels in three pairs to two images RI_1 and RI_2 as shown Figure 5.

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 colour images S_1C and S_2C by using the following equation. The merge function combines R, G, and B to produce a colour image. $S_tC = \text{merge}(RI_i, GI_i, BI_i)$, for $1 \le t \le 2$.
Step 9: Repeat the above steps for all blocks.

Algorithm 3: The proposed embedding algorithm.

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_1C and S_2C into 2×2 size blocks. If the i-th block is $S_tC^i\,(0 \le t \le 1)$, then the pixels in S_tC^i are defined as $S_tC^i_{j,k}\,(0 \le j,k \le 1)$.
Step 2: Decompose two stego colour images S_1C and S_2C into R, G, and B. S_tC is decomposed into RI_t, GI_t, and BI_t.
Step 3: Extract the secret data by using the following equation. pvd_{EA} means extraction algorithm of PVD scheme. secret data $= \text{pvd}_{\text{EA}}(RI_1, RI_2) \| \text{pvd}_{\text{EA}}(GI_1, GI_2) \| \text{pvd}_{\text{EA}}(BI_1, BI_2)$.
Step 4: Repeat the above Steps for all blocks.

Algorithm 4: The proposed extraction algorithm.

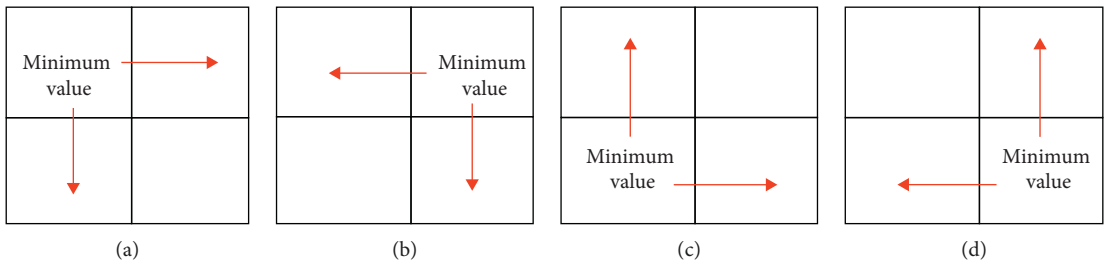


Figure 2: Two pairs in two directions. (a) Case 1: minimum value position (0, 0). (b) Case 2: minimum value position (0, 1). (c) Case 3: minimum value position (1, 0). (d) Case 1: minimum value position (1, 1).

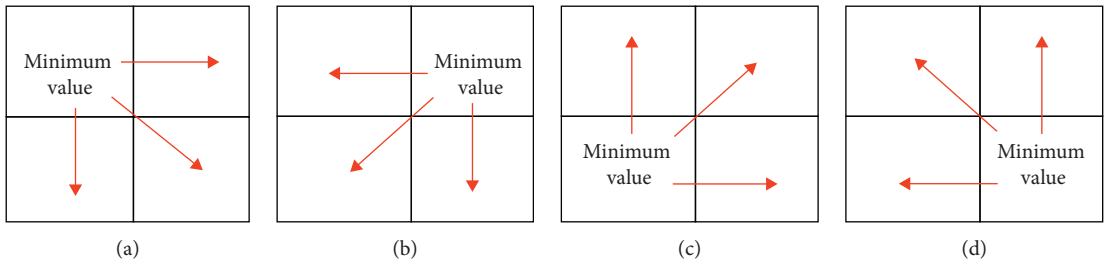


Figure 3: Three pairs in three directions. (a) Case 1: minimum value position (0, 0). (b) Case 2: minimum value position (0, 1). (c) Case 3: minimum value position (1, 0). (d) Case 1: minimum value position (1, 1).

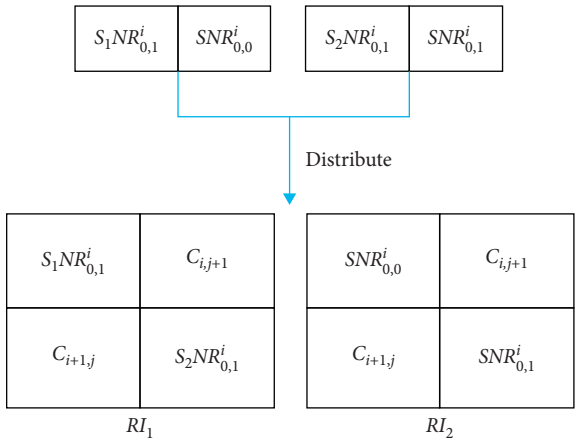


Figure 4: Distributed pixels in two pairs.

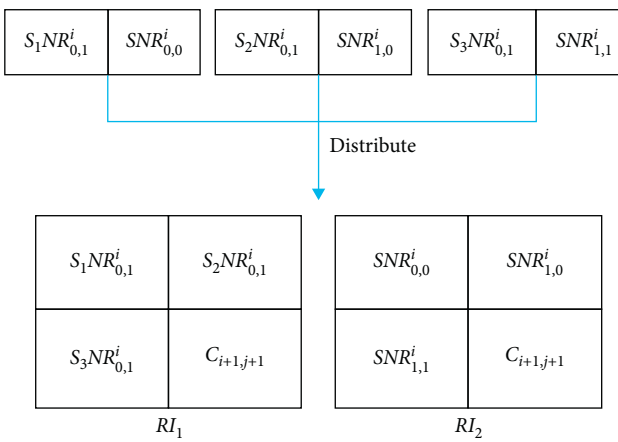
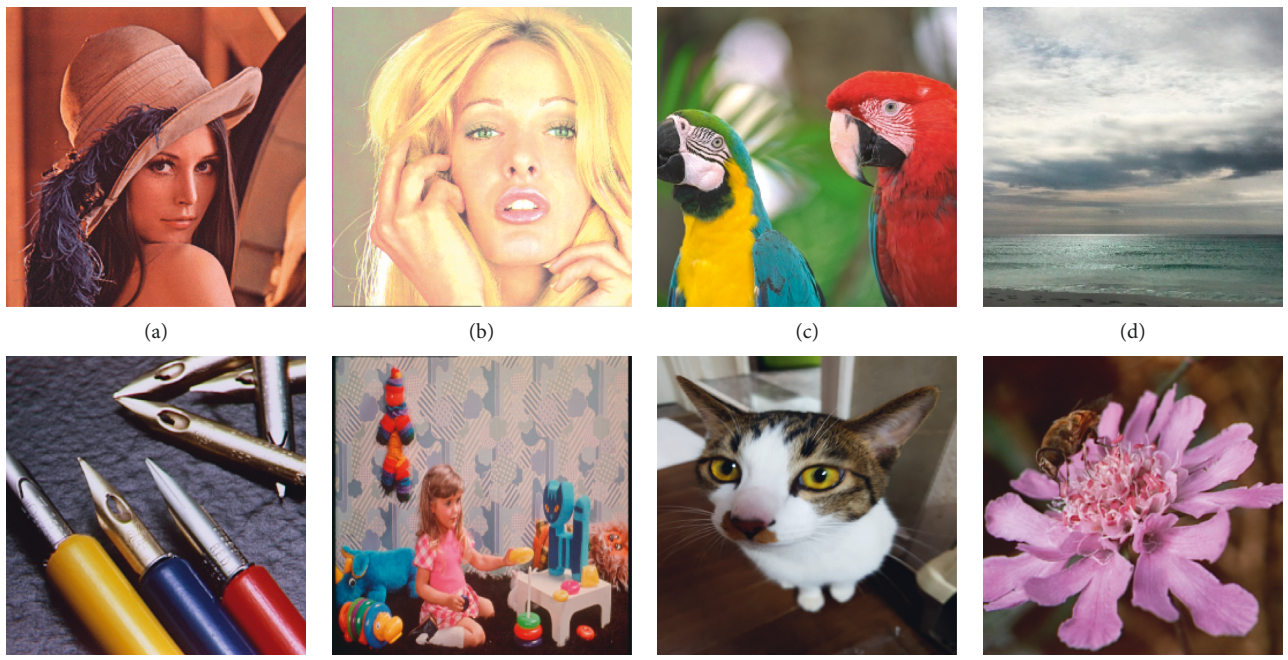


Figure 5: Distributed pixels in three pairs.



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 6: Cover images. (a) Lena. (b) Tiffany. (c) Macaw. (d) Beach. (e) Pens. (f) Girl. (g) Cat. (h) Flower.

$$\text{MSE} = \sum_{i=1}^{W\times H} \frac{(p_i - p_i')^2}{W \times H}. \tag{6}$$

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:

$$Q = \frac{4\delta_{xy}\overline{p_x^2}\overline{p_x^2}}{\left(\delta_x^2 + \delta_y^2\right)\left(\overline{p_x^2} + \overline{p_y^2}\right)}. \tag{7}$$

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

$$\begin{aligned}
\overline{p_x} &= \frac{1}{wh}\sum_{i=0}^{wh-1} p_i,\\
\overline{p_y} &= \frac{1}{wh}\sum_{i=0}^{wh-1} p_i',\\
\delta_x^2 &= \frac{1}{wh-1}\sum_{i=0}^{wh-1} (p_i - \overline{p_x})^2,\\
\delta_y^2 &= \frac{1}{wh-1}\sum_{i=0}^{wh-1} (p_i' - \overline{p_y})^2,\\
\delta_{xy} &= \frac{1}{wh-1}\sum_{i=0}^{wh-1} (p_i - \overline{p_x}) - (p_i' - \overline{p_y}).
\end{aligned} \tag{8}$$

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

$$Q = \frac{\delta_{xy}}{\delta_x\delta_y} \cdot \frac{2\overline{p_x^2}\,\overline{p_y^2}}{\overline{p_x^2} + \overline{p_y^2}} \cdot \frac{2\delta_x\delta_y}{\delta_x^2 + \delta_y^2}. \tag{9}$$

The correlation coefficient between the two images is $\delta_{xy}/\delta_x\delta_y$. The luminance between the two images measures by using $2\overline{p_x^2}\,\overline{p_y^2}/\overline{p_x^2} + \overline{p_y^2}$, and the similarity of the two images measures by using $2\delta_x\delta_y/\delta_x^2 + \delta_y^2$. 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 performing the PVD scheme in two directions. RI_1 and RI_2 are related to R channel, GI_1 and GI_2 are related to G channel, and BI_1 and BI_2 are related to B channel. The first stego image is S_1C and the second stego image is S_2C. Figure 8 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.

(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 7: Two directions embedding (Lena image). (a) RI_1. (b) RI_2. (c) GI_1. (d) GI_2. (e) BI_1. (f) BI_2. (g) SI_1. (h) SI_2.

(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 8: Three directions embedding (Lena image). (a) RI_1. (b) RI_2. (c) GI_1. (d) GI_2. (e) BI_1. (f) BI_2. (g) SI_1. (h) SI_2.

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 el 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.

	Wu and Tsai's scheme [18]	Nagaraj et al.'s scheme [27]	Prema and Manimegalai's scheme [28]	Shiv and Arup's scheme [30]	Proposed scheme (two directions)		
	Colour image	Colour image	Colour image	Colour image	S_1C	S_2C	
	PSNR (dB)	PSNR (dB)	PSNR (dB)	PSNR (dB)	PSNR-1 (dB)	PSNR-2 (dB)	Average
Lena	40.0379	49.8948	43.7599	30.7933	30.9791	32.2565	30.9791
Tiffany	41.6758	49.9241	43.8679	31.2709	30.2070	30.4749	30.3409
Macaw	41.4435	50.0031	43.8326	30.4724	30.5083	32.7829	31.6456
Beach	43.1482	49.9013	42.1780	41.0727	35.1747	36.2268	35.7007
Pens	41.8196	49.8866	43.1339	32.6592	29.8021	32.4704	31.1362
Girl	41.7187	49.8949	43.0240	32.8201	30.2782	32.9632	31.6207
Cat	42.5678	49.8925	43.7878	37.4366	34.0405	36.0262	35.0333
Flower	42.0581	49.8871	43.2004	31.2419	30.3256	32.8820	31.6038
Average	41.8087	49.9105	43.3480	33.4708	31.4144	33.2603	32.3373

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

	Wu and Tsai's scheme [18]	Nagaraj el al.'s scheme [27]	Prema and Manimegalai's scheme [28]	Shiv and Arup's scheme [30]	Proposed scheme (two directions)
	Capacity (bits)	Capacity (bits)	Capacity (bits)	Capacity (bits)	Capacity (bits)
Lena	1,248,890	524,457	2,305,342	2,516,141	3,739,287
Tiffany	1,225,240	523,641	2,306,394	2,330,381	3,678,830
Macaw	1,211,869	524,261	2,328,347	2,185,173	3,643,723
Beach	1,188,477	523,896	2,305,296	1,588,798	3,597,199
Pens	1,208,497	524,380	2,307,066	1,878,029	3,643,788
Girl	1,234,315	524,351	2,307,919	1,919,833	3,670,028
Cat	1,193,828	524,330	2,305,296	1,700,834	3,591,096
Flower	1,206,025	524,733	2,305,305	2,255,479	3,621,236
Average	1,214,643	524,256	2,308,871	2,046,834	3,648,148

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

	Shiv and Arup's scheme [30]	Proposed scheme			
	Quality index	Two directions		Three directions	
		Quality index-1	Quality index-2	Quality index-1	Quality index-2
Lena	0.6870	0.7653	0.7325	0.7735	0.7148
Tiffany	0.4686	0.4181	0.4563	0.3767	0.4863
Macaw	0.4486	0.4456	0.4401	0.4477	0.4348
Beach	0.3297	0.3346	0.3284	0.3451	0.3190
Pens	0.2370	0.2248	0.2354	0.2221	0.2362
Girl	0.0712	0.0719	0.0693	0.0733	0.0677
Cat	0.3792	0.3804	0.3755	0.3802	0.3756
Flower	0.3294	0.3415	0.3344	0.3456	0.3300
Average	0.3688	0.3727	0.3714	0.3705	0.3705

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

Images	Proposed scheme					
	Two directions			Three directions		
	PSNR-1 (dB)	PSNR-2 (dB)	Capacity (bits)	PSNR-1 (dB)	PSNR-2 (dB)	Capacity (bits)
Lena	30.9791	32.2565	3,739,287	26.9258	29.5024	5,671,307
Tiffany	30.2070	30.4749	3,678,830	27.6425	30.8193	5,557,627
Macaw	30.5083	32.7829	3,643,723	28.0548	30.2345	5,507,035
Beach	35.1747	36.2268	3,597,199	32.1241	35.2979	5,420,140
Pens	29.8021	32.4704	3,643,788	28.2435	30.0250	5,563,465
Girl	30.2782	32.9632	3,670,028	28.7210	30.4778	5,601,851
Cat	34.0405	36.0262	3,591,096	33.2151	35.9475	5,429,264
Flower	30.3256	32.8820	3,621,236	29.1141	31.1358	5,494,673
Average	31.4144	33.2603	3,648,148	29.2551	31.6800	5,530,670

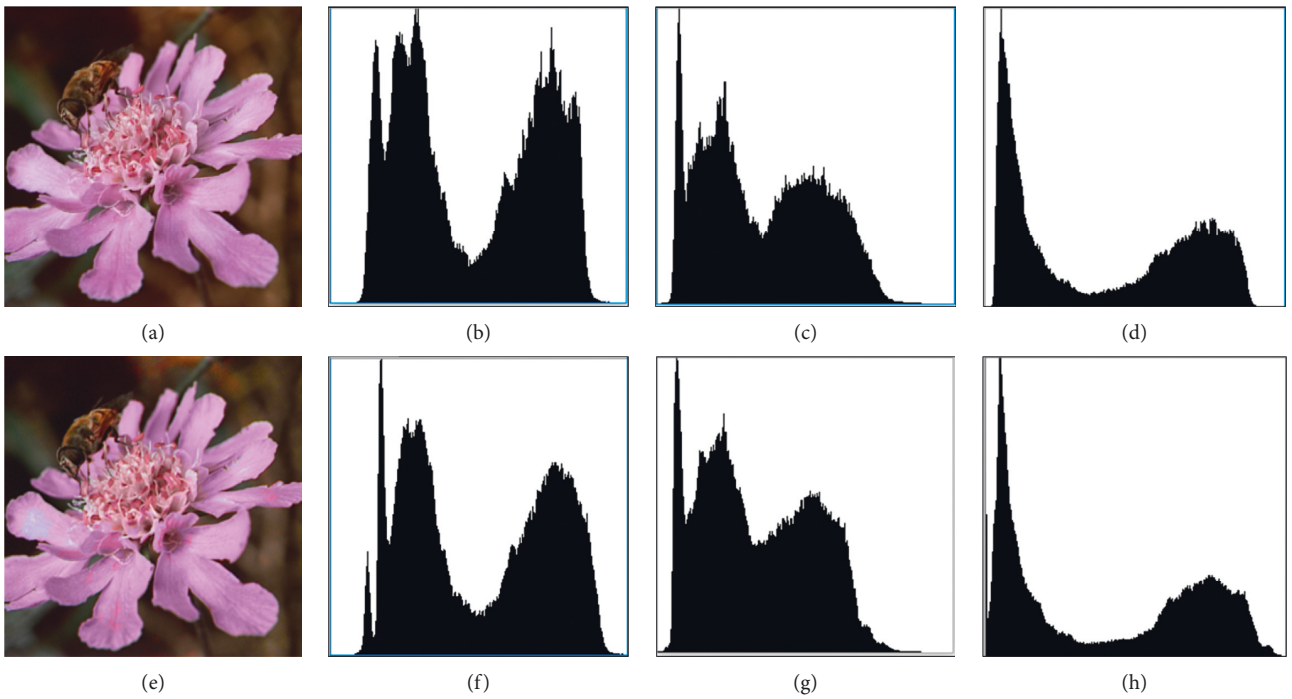


Figure 9: (a) Flower cover image (b–d) R, G, B histograms of cover image (e) Flower stego image (f–h) R, G, and B histograms of Shiv and Arup's scheme.

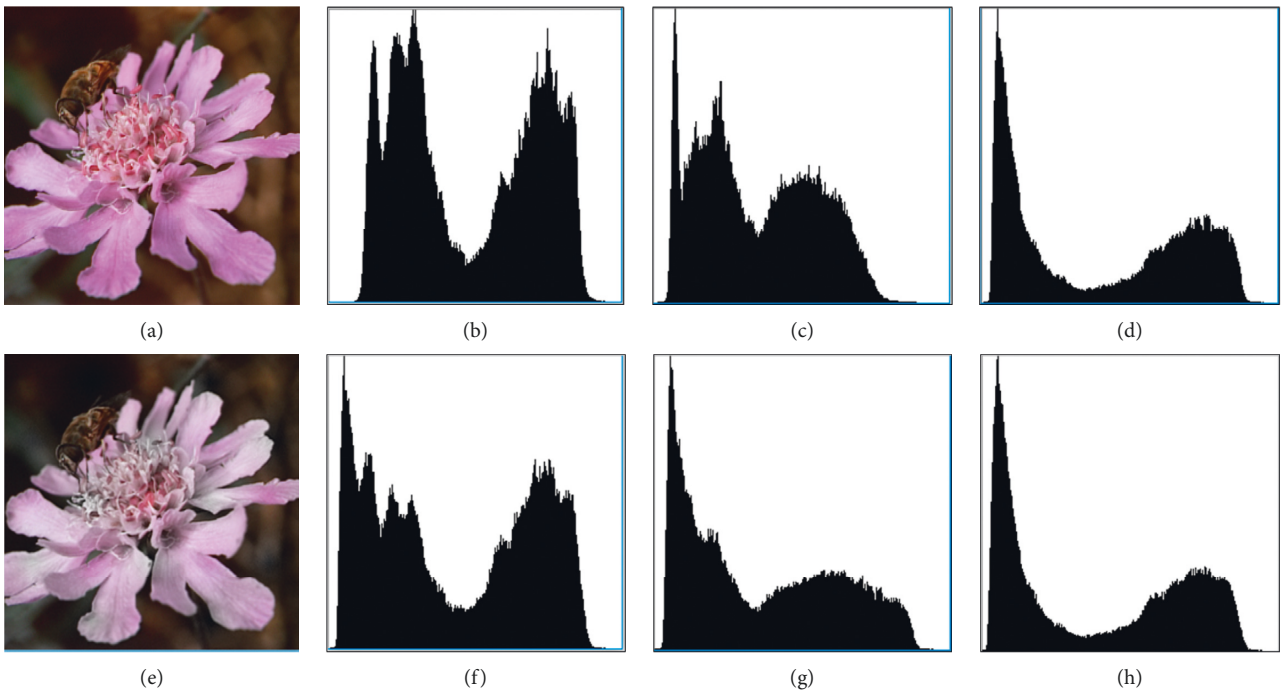
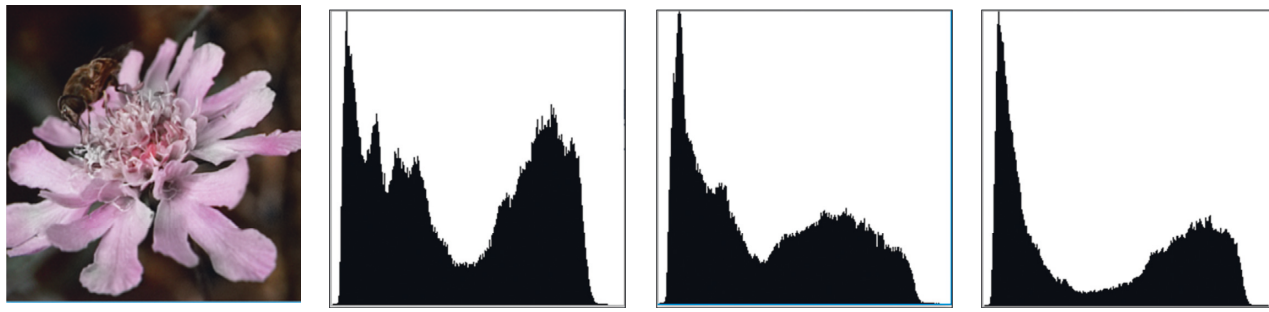


Figure 10: Continued.



(i) (j) (k) (l)

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.

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 colour stego images were separated into R, G, and B channels, and 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

[1] S. Wang, Z. Cao, M. A. Strangio, and L. Wang, "Cryptanalysis and improvement of an elliptic curve Diffie-Hellman key agreement protocol," *IEEE Communications Letters*, vol. 12, no. 2, pp. 149–151, 2008.

[2] D. R. Stinson, *Cryptography Theory and Practice*, Chapman & Hall/CRC Press, Boca Raton, FL, USA, 3rd edition, 2006.

[3] R.-Z. Wang, C.-F. Lin, and J.-C. Lin, "Hiding data in images by optimal moderately-significant-bit replacement," *Electronics Letters*, vol. 36, no. 25, pp. 2069-2070, 2000.

[4] M. Hussain, A. W. Abdul Wahab, A. T. S. Ho, N. Javed, and K.-H. Jung, "A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement," *Signal Processing: Image Communication*, vol. 50, pp. 44–57, 2017.

[5] M. H. Kang, I. S. Moskowitz, and S. Chincheck, "The pump: a decade of covert fun," in *Proceedings of the 21st Annual Computer Security Applications Conference*, pp. 352–358, Tucson, AZ, USA, December 2005.

[6] S. Zander, *Performance of Selected Noisy Covert Channels and Their Countermesures in IP Network*, Centre for Advanced Inter Net Architectures, Faculty of Information and Communication Technologies, Melbourne, Australia, 2010.

[7] H. S. Majunatha Reddy and K. B. Raja, "High capacity and security steganography using discrete wavelet transform," *International Journal of Computer Science and Security*, vol. 4, no. 3, pp. 462–472, 2009.

[8] B. Ahuja, M. Kaur, and M. Rachna, "High capacity filter based steganography," *International Journal of Recent Trends in Engineering*, vol. 1, no. 1, pp. 672–674, 2009.

[9] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.

[10] A. Pfitzmann, M. Kohntopp, and A. Shostack, "Anonymity, unobservability, and pseudonymity—A proposal for terminology," in *Designing Privacy Enhancing Technologies*, pp. 1–9, Springer, Berlin, Germany, 2001.

[11] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, Elsevier, Amsterdam, Netherlands, 2008.

[12] Y. Yan, H. Rong, and X. Mintao, "A novel audio watermarking algorithm for copyright protection based on DCT domain," in *Proceedings of the Second International Symposium on Electronic Commerce and Security*, pp. 184–188, Nanchang, China, May 2009.

[13] M. Vatsa, R. Singh, A. Noore, M. M. Houck, and K. Morris, "Robust biometric image watermarking for fingerprint and face template protection," *IEICE Electronics Express*, vol. 3, no. 2, pp. 23–28, 2006.

[14] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," in *Proceedings of the International Symposium on Circuits and Systems*, vol. 2, pp. 912–915, Bangkok, Thailand, May2003.

[15] L.-C. Huang, L.-Y. Tseng, and M.-S. Hwang, "A reversible data hiding method by histogram shifting in high quality medical images," *Journal of Systems and Software*, vol. 86, no. 3, pp. 716–727, 2013.

[16] C. C. Chang, J. Y. Hsiao, and C. S. Chan, "Finding optimal least significant-bit substitution in image hiding by dynamic programming strategy," *Pattern Recognition*, vol. 36, no. 7, pp. 1583–1595, 2003.

[17] R.-Z. Wang, C.-F. Lin, and J.-C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recognition*, vol. 34, no. 3, pp. 671–683, 2001.

[18] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9-10, pp. 1613–1626, 2003.

[19] H.-C. Wu, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *IEEE Proceedings, Visual Image Signal Processing*, vol. 152, no. 5, pp. 6 11–615, 2005.

[20] C.-M. Wang, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, "A high quality steganographic method with pixel-value differencing and modulus function," *Journal of Systems and Software*, vol. 81, no. 1, pp. 150–158, 2008.

[21] C.-C. Chang, T. Kieu, and Y.-C. Chou, "Reversible data hiding scheme using two steganographic images," in *Proceeding of IEEE Region 10 International Conference*, pp. 1–4, Taipei, Taiwan, November 2007.

[22] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Communications Letters*, vol. 10, no. 11, pp. 781–783, 2006.

[23] C.-F. Lee, K.-H. Wang, C.-C. Chang, and Y.-L. Huang, "A reversible data hiding scheme based on dual steganograp hic images," in *Proceedings of the Third International Conference on Ubiquitous Information Management and Communication*, pp. 228–237, Suwon, South Korea, January 2009.

[24] C. Qin, C.-C. Chang, and T.-J. Hsu, "Reversible data hiding scheme based on exploiting modification direction with two steganographic images," *Multimedia Tools and Application*, vol. 74, no. 15, pp. 5861–5872, 2015.

[25] T.-C. Lu, J.-H. Wu, and C.-C. Huang, "Dual-Image-based reversible data hiding method using center folding strategy," *Signal Processing*, vol. 115, pp. 195–213, 2015.

[26] H. Yao, C. Qin, Z. Tang, and Y. Tian, "Improved dual-image reversible data hiding method using the selection strategy of shiftable pixels' coordinates with minimum distortion," *Signal Processing*, vol. 135, pp. 26–35, 2017.

[27] V. Nagaraj, V. Vijayalakshmi, and G. Zayaraz, "Color image steganography based on pixel value modification method using modulus function," *IERI Procedia*, vol. 4, pp. 17–24, 2013.

[28] C. Prema and D. Manimegalai, "Adaptive color image steganography using intra color pixel value differencing," *Australian Journal of Basic & Applied Sciences*, vol. 8, no. 3, pp. 161–167, 2014.

[29] G. Swain, "Adaptive pixel value differencing steganography using both vertical and horizontal edges," *Multimedia Tools Application*, vol. 75, no. 21, pp. 13541–13556, 2016.

[30] P. Shiv and K. P. Arup, "An RGB colour image steganography scheme using overlapping block-based pixel-value differencing," *Royal Society Open Science*, vol. 4, no. 4, 2017.