Reversible data hiding scheme based on pixel-value differencing in dual images

Pyung-Han Kim¹, Kwan-Woo Ryu¹ and Ki-Hyun Jung²

Abstract
In this article, a new reversible data hiding scheme using pixel-value differencing in dual images is proposed. The proposed pixel-value differencing method can embed more secret data as the difference value of adjacent pixels is increased. In the proposed scheme, the cover image is divided into non-overlapping blocks and the maximum difference value is calculated to hide secret bits. On the sender side, the length of embeddable secret data is calculated by using the maximum difference value and the log function, and the decimal secret data are embedded into the two stego-images after applying the ceil function and floor function. On the receiver side, the secret data extraction and the cover image restoration can be performed by using the correlation between two stego-images. After recovering the cover image from two stego-images, the secret data can be extracted using the maximum difference value and the log function. The experimental results show that the proposed scheme has a higher embedding capacity and the proposed scheme differs in embedding the secret data depending on the characteristics of the cover image with less distortion. Also, the proposed scheme maintains the degree of image distortion that cannot be perceived by the human visual system.

Keywords
Reversible data hiding, dual images, PVD, steganography

Date received: 10 November 2019; accepted: 5 February 2020

Handling Editor: Ru Zhang

Introduction
Recently, most of important information is transmitted over the Internet using advanced computer performance and Internet technology. Internet is convenient for information exchange because of easy access and various conveniences. However, the Internet is an open space, so important information can be deceived and altered by malicious attackers. Therefore, many data hiding schemes that can transmit information securely over the Internet have been proposed. In general, a data hiding scheme generates the stego-image by embedding the secret data into a cover image. Many data hiding schemes have been proposed based on least significant bits (LSB) replacement and pixel-value differencing (PVD) in irreversible data hiding methods.¹⁻⁵ The LSB scheme embeds or extracts the secret data in the lower bit region in each pixel or pixel group that is based on the fact that it is very difficult to be detected by the human visual system even if the lower bits of a pixel change. The LSB-based schemes uniformly embed the secret data as same quantity into all pixels of a cover image. However, there are edge and smooth areas in an image and it means that different amount of secret bits can be embedded on edge and smooth areas.

¹Department of Computer Science and Engineering, Kyungpook National University, Daegu, South Korea
²Department of Cyber Security, Kyungil University, Gyeongsan, Korea

Corresponding author:
Ki-Hyun Jung, Department of Cyber Security, Kyungil University, Gyeongsan 38428, Gyeongbuk, Korea.
Email: khanny.jung@gmail.com

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).
It is based on the fact that the alteration of edge areas cannot be distinguished well, but the alteration of smooth areas can be distinguished easily in human visual system. In other words, an edge area can be hidden more secret data than a smooth area. The PVD was first proposed by Wu and Tsai to distinguish edge and smooth areas. In the PVD method, two pixels are located in an edge area if the difference value between the two consecutive pixels is large, then more secret data can be hidden depending on the range table. On the other hand, if the difference value between the two consecutive pixels is small, less secret data can be hidden since the two pixels are located in a smooth area. Data hiding schemes using PVD method are proposed continuously.\(^6\) Although the PVD method can embed more secret data and guarantee high imperceptibility, the cover image cannot be restored because the original image is damaged after extracting the secret data from the stego-image. It could cause serious problems in the military and medical fields that are sensitive to the distortion of the original image, so reversible data hiding schemes have been proposed to overcome restoring the cover image.\(^9\)–\(^12\) The reversible data hiding scheme can extract the secret data from the stego-image and restore the original cover image perfectly without loss of cover image. In general, reversible data hiding schemes generate a single stego-image by embedding secret data into a single cover image, but recently, dual image–based reversible data hiding schemes have been proposed that generate two stego-images after embedding secret data into a cover image. Dual image–based reversible data hiding scheme was first proposed by Chang et al.\(^13\) in 2007. This scheme embeds and extracts secret data based on the quinary notation and improves the extraction function of exploiting modification direction (EMD) scheme\(^14\) to increase the embedding capacity. A modulus function is designed, and two stego-pixel values are defined according to the value of the quinary secret data. In 2009, Lee et al. proposed a dual image–based reversible data hiding scheme using four directions based on the central point.\(^15\) This scheme uses the relationship between two images to determine if secret data can be embedded in the second image. In the embedding process, two stego-pixel values are determined according to the combination of two binary secret bits. Qin et al. proposed a scheme for performing different embedding processes on two images,\(^16\) where the EMD scheme was applied to the first image and three rules based on the first image to embed the secret data was used to the second image. In this scheme, the distortion of the second stego-image is larger than the first stego-image. In 2015, Lu et al. proposed a dual image–based reversible data hiding scheme to reduce loss of original image by applying center folding strategy (CFS) method.\(^17\) The CFS method reduces the distortion of the image by adjusting the range of secret data. In this scheme, secret data are embedded by using the ceil function and the floor function to generate two stego-images. In 2017, Yao et al.\(^18\) proposed a dual image–based reversible data hiding scheme using the selection strategy of shiftable pixels’ coordinates to improve the Lu et al.’s scheme. Yao et al. used the diagram to improve the scheme of Lu et al., and the selection strategy of the shiftable pixels’ coordinates was used to increase the embedding capacity. In this scheme, secret data are classified into even and odd numbers, and different embedding methods are applied. In 2019, Shastri and Thanikaiselvan proposed a scheme to improve the image quality of Yao et al.’s scheme. The CFS method, shiftable pixel coordinate selection strategy method, and lookup table were used to improve the image quality.\(^19\) In this article, we propose a dual image–based reversible data hiding scheme using the PVD method. The proposed scheme divides a cover image into sub-block and uses the maximum difference value in each sub-block to decide the length of embeddable secret data. Therefore, the proposed scheme can embed more secret data when the difference value of pixel values is larger in each sub-block.

The rest of the article is organized as follows. The PVD method and dual image–based reversible data hiding schemes are described in the “Related works” section. In the “The proposed scheme” section, the proposed embedding scheme is described and extracting and restoring scheme is explained in detail. The experimental results are explained and analyzed to demonstrate the superiority of the proposed scheme. The “Conclusion and discussion” section concludes the article.

**Related works**

**PVD**

Wu and Tsai proposed a PVD scheme that adjusts the size of secret data that can be embedded according to the difference between two neighboring pixels. In the grayscale cover image, two consecutive pixels are used as one block. The image is divided by blocking. When the pixels of each block are denoted by \(C_i\) and \(C_{i+1}\), the difference value \(d_i\) is obtained using \(d_i = C_{i+1} - C_i\). If the lower and upper range values in the block are \(u_i\) and \(l_i\), the number \(n\) of bits that can be embedded in each block is calculated using equation (1)

\[
n = \log_2(u_i - l_i + 1)
\]
If a value obtained by converting \( n \) bits into a decimal form is given as \( b \), a new difference value \( d'_i \) is calculated using equation (2)

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

(2)

When the new difference value is \( d'_i \) and the difference value of the block is denoted as \( d_i \), the difference value \( m_i \) between two pixels is calculated using equation (3)

\[
m_i = d'_i - d_i
\]

(3)

Suppose that two consecutive pixels in a grayscale stego-image are denoted by \( S_i \) and \( S_{i+1} \), the stego-image pixels can be calculated using equation (4)

\[
f((g_i, g_{i+1}), m) = \begin{cases} (g_i - \frac{m}{2}, g_i + \frac{m}{2}) & \text{if } d_i \text{ is an odd number;} \\ (g_i - \frac{m}{2}, g_i + \frac{m}{2}) & \text{if } d_i \text{ is an even number.} 
\end{cases}
\]

(4)

\[
f((g_i, g_{i+1}), m) = \begin{cases} (g_i, g_i + m) & \text{if } d_i \text{ is an odd number;} \\ (g_i, g_i + m) & \text{if } d_i \text{ is an even number.} 
\end{cases}
\]

(4)

Zhang et al.’s scheme

In 2019, Zhang et al. proposed reversible data hiding scheme using histogram shifting for high embedding capacity. This scheme uses additive homomorphic encryption and block permutation for image encryption and consists of encryption, secret data embedding, secret data extraction, and image restoration phase.

The encryption phase consists of additive homomorphic encryption and block permutation. The cover image is divided into non-overlapped blocks, and a key stream \( R \) is generated to apply additive homomorphic encryption. When \( s \) is defined as the value of the original image and \( r \) is an element of the key stream \( R \), the value \( x \) of the encrypted image \( X' \) is defined by equation (5)

\[
s_i(i, j) = (s_i(i, j) + r_i) \mod N
\]

(5)

Then, block permutation is performed to enhance security. Block permutation uses the Logistic chaotic function to generate a key sequence and performs block permutation based on this key sequence to create a fully encrypted image \( X \).

The secret data embedding step consists of a prediction step, a histogram expansion, and a shifting step. In the prediction phase, three sets are used. In the case of set 0, the predicted value is calculated using MED. When \( x_{i,j} \) is located at \((i, j)\) of the image, the predicted value \( p_x \) is calculated using equation (6)

\[
p_x = \begin{cases} \min(x_{i,j+1}, x_{i+1,j}) & \text{if } x_d \geq \max(x_{i,j+1}, x_{i+1,j}) \\ \max(x_{i,j+1}, x_{i+1,j}) & \text{if } x_d \leq \max(x_{i,j+1}, x_{i+1,j}) \\ x_{i,j} - x_d + x_{i+1,j} & \text{otherwise.} 
\end{cases}
\]

(6)

In case of set 1, the predicted value \( p_i \) is calculated using the rhombus predictor of equation (7). When \( x_{i,j} \) is located at \((i, j)\) of the block, adjacent pixels are \( x_{i-1,j}, x_{i+1,j}, \) and \( x_{i,j+1} \), and \( \lfloor \rfloor \) is a rounding function

\[
p_x = \left\lfloor \frac{x_{i,j-1} + x_{i-1,j} + x_{i+1,j} + x_{i,j+1}}{4} \right\rfloor
\]

(7)

The case of set 2 is similar to set 1. The \( p_x \) value in set 2 is the domain mean value of the vertical and horizontal directions. When the predicted value \( p_x \) is calculated, the prediction error \( d \) is calculated using the following equation

\[
d(i, j) = x(i, j) - p_x(i, j)
\]

(8)

After the prediction error value \( d \) is calculated, the histogram right expansion and shifting steps are performed. When the range of this step is defined \([t_n, t_{n+1}]\), the number of histograms extended to the right is calculated using the following equation

\[
t_{exp} = t_{n+2} - t_n + 1
\]

(9)

The prediction error \( d(i, j) \) is calculated using equation (10)

\[
d_e(i, j) = \begin{cases} d(i, j) & \text{if } d(i, j) < t_{n+1} \\ 2d(i, j) - t_n & \text{if } t_{n+1} \leq d(i, j) \leq t_{n+2} \\ 2d(i, j) + t_{exp} & \text{if } d(i, j) > t_{n+2} 
\end{cases}
\]

(10)

If the secret data are \( s_r \), the original pixel value is \( x(i, j) \), and the prediction error is \( d(i, j) \), then \( x_{rm}(i, j) \) with the secret data embedded is calculated using equation (11)

\[
x_{rm}(i, j) = \begin{cases} x(i, j) & \text{if } d(i, j) < t_{n+1} \\ x(i, j) + d(i, j) - t_n + s_r & \text{if } t_{n+1} \leq d(i, j) \leq t_{n+2} \\ x(i, j) + t_{exp} & \text{if } d(i, j) > t_{n+2} 
\end{cases}
\]

(11)

To generate a stego-image, a similar process is performed for histogram left expansion and shifting.

Lu et al.’s scheme

Lu et al.’s scheme used CFS method to reduce image distortion in embedding of secret data. Lu et al.’s scheme selects \( k \) bits of binary secret data and converts it into decimal form. The secret data are \( d \), and the secret data range for \( k \) is given as \( R \). When the data to which CFS can apply are \( d \), equation (12) is used to calculate \( d \).
In order to generate two stego-images, the $d$ value is divided into two types using the following equation:

$$d_1 = \left\lfloor \frac{d}{2} \right\rfloor, \quad d_2 = \left\lceil \frac{d}{2} \right\rceil$$

(13)

When a pixel value of the cover image is defined as $x_{i,j}$, the first stego-image pixel is defined as $x'_{i,j}$, and the second stego-image pixel is defined as $x''_{i,j}$. And, equation (14) is used to embed the secret data into the two stego-images

$$x'_{i,j} = x_{i,j} + d_1, \quad x''_{i,j} = x_{i,j} - d_2$$

(14)

Yao et al.’s scheme

In 2017, Yao et al. improved Lu et al.’s scheme by using selection strategy of shiftable pixel coordinates. Yao et al. improved the embedding capacity of secret data by improving Lu et al.’s scheme as shown in Figure 1, where Figure 1 shows a diagram of the embedding of secret data for both schemes. As shown in Figure 1, Yao et al.’s scheme increased the embedding capacity since the number of cases of embedding is larger than that of Lu et al.’s scheme. If the number of bits of the binary secret data that can be embedded is $k$, then the $k$ binary secret bits are converted into a decimal secret data $d$. If $d$ is equal to $2^k - 1$, additional bits can be embedded. The pixel value ($x_i, x_j$) of the image changes into $(x_i - 1, x_j + 1)$ when the additional bit is 0 and $(x_i, x_j)$ is converted into $(x_i + 1, x_j + 1)$ when the additional bit is 1.

If $d$ is not equal to $2^k - 1$, then the secret data are embedded by following two cases. When each pixel of two stego-images is called $x'_i$ and $x''_i$, $d$ is embedded by using equation (15).

Case 1: $d$ is an even number

$$x'_i = x_i + \frac{d}{4}$$

$$x''_i = x_i + \frac{d}{2}$$

Case 2: $d$ is an odd number

$$x'_i = x_i - \frac{d}{4}$$

$$x''_i = x_i + \frac{d}{2}$$

(15)

Shastri and Thanikaiselvan’s scheme

In 2019, Shastri and Thanikaiselvan proposed a scheme to improve the quality of the image while maintaining the amount of secret data capacity in Yao et al.’s scheme. This scheme uses the CFS method and the shiftable pixel coordinate selection strategy method and creates a lookup table to improve the PSNR of the image. Three-bit binary secret data are converted to decimal secret data $d$. If the value of the converted decimal secret data is 7, one additional bit (0 or 1) can be embedded. CFS method is applied to decimal secret data using equation (12) to generate $d$. As shown in
The created lookup table, Table 2, is as follows.

| Trinary mapping | Initial shifts | Final shifts |
|-----------------|----------------|--------------|
| $m_1$ | $m_2$ | $\delta_1$ | $\delta_1$ | $s$ | $s'$ |
| -1 | -1 | -0.5 | -1 | -1 | 1 |
| -1 | 0 | -0.5 | 0 | -1 | 1 |
| -1 | 1 | 0 | 0.5 | 0 | -1 |
| 0 | -1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | -0.5 | 0 | -1 |
| 1 | -1 | -0.5 | 0 | -1 | 0 |
| 1 | 0 | -0.5 | 0 | -1 | 1 |
| 1 | 1 | -0.5 | 1 | 1 | -1 |

Table 1, trinary mapping is performed on $d$ to obtain the values of $m_1$ and $m_2$.

Initial shifts are calculated using equation (16).

Case 1: $d$ is an even number

$$\delta_1 = -m_1 \frac{[d/3]}{2}, \delta_2 = -m_2 \frac{[d/3]}{2}$$

Case 2: $d$ is an odd number

$$\delta_1 = -m_1 \frac{[d/3]}{2}, \delta_2 = -m_1 \frac{[d/3]}{2}$$

The final shifts $s'$ and $s''$ are calculated using equation (17).

Case 1: $d < 7$

$$s' = \lfloor \delta \rfloor$$

$$s'' = \begin{cases} \lfloor \delta_1 + \delta_2 \rfloor, & d \text{ is even} \\ \lfloor \delta_1 + \delta_2 \rfloor, & d \text{ is odd} \end{cases}$$

Case 2: $d \geqslant 7$

$$s' = -\lfloor \delta \rfloor$$

$$s'' = \begin{cases} \lfloor \delta_1 + \delta_2 \rfloor, & d \text{ is even} \\ \lfloor \delta_1 + \delta_2 \rfloor, & d \text{ is odd} \end{cases}$$

The proposed scheme

The proposed scheme uses PVD method to dual image-based reversible data hiding scheme for high embedding capacity. The cover image divides into sub-blocks with non-overlapping and the maximum difference value is calculated between the pixels in each sub-block. The maximum difference value and log function are used to determine the number of embedding secret bits. The binary secret bits that can be embedded into each pixel are converted into decimal secret data. The decimal secret data are embedded by using the floor function and ceil function into the cover image to generate two stego-images. In the extraction process, the two stego-images are divided into non-overlapping blocks. The cover image is recovered using the average value of the pixel values of the two stego-images. The maximum difference value is calculated within each block of the cover image, and secret data are extracted using the maximum difference value and the log function. In this section, we describe a new dual image-based reversible data hiding scheme that embeds secret data according to the difference value of the pixels in the block for high embedding capacity.

Embedding algorithm

The detailed embedding algorithm is as follows. Each pixel in the block calculates the difference value with the other pixels in the block and embeds the decimal secret data based on the maximum difference value.

Algorithm 1. The embedding algorithm

Input: A cover image with width $W$ and height $H$ and the binary secret data

Output: The two stego-images of $W \times H$

Step 1. Divide a cover image into non-overlapping blocks with $M \times M$ size.

Step 2. Define the $i$th block as $B_i$, and each pixel in $B_i$ as $c^*_{i,k}$ ($j, k = 0, 1, \ldots, M$). And, calculate the max difference value $d^*_{i,k}(j, k = 0, 1, \ldots, M)$ using equation (19). The $\max$ function returns the maximum value

$$d^*_{i,0} = \max(|c^*_{i,0} - c^*_{i,1}|, \ldots, |c^*_{i,0} - c^*_{i,M}|, |c^*_{i,0} - c^*_{i,1}|, \ldots, |c^*_{i,0} - c^*_{i,M}|, |c^*_{i,0} - c^*_{i,1}|, \ldots, |c^*_{i,0} - c^*_{i,M}|)$$

$$\ldots$$

$$d^*_{i,k} = \max(|c^*_{i,k} - c^*_{i,0}|, \ldots, |c^*_{i,k} - c^*_{i,k-1}|, |c^*_{i,k} - c^*_{i,k+1}|, \ldots, |c^*_{i,k} - c^*_{i,k-1}|, \ldots, |c^*_{i,k} - c^*_{i,k-1}|)$$

$$d^*_{i,k} = \max(|c^*_{i,k} - c^*_{i,0}|, \ldots, |c^*_{i,k} - c^*_{i,k-1}|, |c^*_{i,k} - c^*_{i,k+1}|, \ldots, |c^*_{i,k} - c^*_{i,k-1}|, \ldots, |c^*_{i,k} - c^*_{i,k-1}|)$$

Step 3. Apply the log function to the maximum difference value $d^*_{i,k}$ of each pixel in the block for obtaining embedding size $E^*_{i,k}(j, k = 1, 2, \ldots, M)$ by the following equation
\[ \hat{t}_i^{j,k} = \left\lfloor \log_2 d_i^{j,k} \right\rfloor \]  

**Step 4.** Convert the \( t_i^{j,k} \) size binary secret bits to decimal secret data \( s_i^{j,k} \), and the value to be embedded is defined using the following formula. \( T_i^{j,k} \) and \( t_i^{j,k} \) are temporary values for embedding secret data

\[ T_i^{j,k} = \left\lfloor \frac{s_i^{j,k}}{2} \right\rfloor, \quad t_i^{j,k} = \left\lfloor \frac{s_i^{j,k}}{2} \right\rfloor \]

**Step 5.** Calculate the following equation to combine the temporary values and cover image pixel values to generate two stego-images. When two stego-images are defined as \( S_1 \) and \( S_2 \), the pixels in each stego-image are called \( S_1 p_i^{j,k} \) and \( S_2 p_i^{j,k} \)

\[ S_1 p_i^{j,k} = c_i^{j,k} + T_i^{j,k}, \quad S_2 p_i^{j,k} = c_i^{j,k} - t_i^{j,k} \]  

**Step 6.** Repeat the above steps for all blocks.

An example of the embedding algorithm is as follows. The cover image is divided into \( 2 \times 2 \) size blocks. The first block is \( B_1 \) and the pixels of \( B_1 \) are \( c_{1,0} = 120, c_{1,1} = 140, c_{1,0} = 125 \), and \( c_{1,1} = 112 \). And, the maximum values \( d_{1,0} = 20, d_{1,1} = 28, d_{1,0} = 15 \), and \( d_{1,1} = 28 \) are calculated using equation (19). The size of the secret data \( \rho_{1,0} = 4, \rho_{1,1} = 4, \rho_{1,0} = 3, \) and \( \rho_{1,1} = 4 \) is calculated by equation (20). If the binary secret bit stream is 1011001110111112, then the secret bits are brought according to the size of \( t_i^{j,k} \). The binary secret bits are then converted to decimal secret, such as \( s_{1,0} = 11, s_{1,1} = 3, s_{1,0} = 5, \) and \( s_{1,1} = 15 \). Each pixel defines temporary pixels, \( T_{1,0}^{0,0} = 5, T_{1,0}^{0,1} = 6, T_{1,1}^{0,0} = 1, T_{1,1}^{0,1} = 2, T_{1,0}^{1,0} = 2, T_{1,0}^{1,1} = 3, T_{1,1}^{1,0} = 7, \) and \( t_{1,1}^{1,1} = 6 \). Each temporary pixel generates \( S_1 p_{1,0}^{0,0} = 125, S_2 p_{1,0}^{0,0} = 114, S_2 p_{1,1}^{0,1} = 138, S_2 p_{1,0}^{1,0} = 127, S_2 p_{1,0}^{1,1} = 122, S_1 p_{1,1}^{0,1} = 119, \) and \( S_2 p_{1,1}^{1,1} = 104 \) using equation (22). This embedding example is shown in Figure 2.

**Extraction and recovering algorithm**

The detailed extraction algorithm is as follows. In the recovering process, the cover image is restored by using the average value between the two stego-images. The secret data are extracted using the maximum difference value among the pixels in the restored cover image.

**Algorithm 2.** The extraction and recovering algorithm

**Input:** The two stego-images of \( W \times H \)

**Output:** A cover image with width \( W \) and height \( H \) and the binary secret data

**Step 1.** Divide the two stego-images into \( M \times M \) size blocks.

**Step 2.** Restores cover image pixel \( c_i^{j,k} \) using pixels in the same position of two stego-images

\[ c_i^{j,k} = \left\lfloor \frac{(S_1 p_i^{j,k} + S_2 p_i^{j,k})}{2} \right\rfloor \]

**Step 3.** Calculate the maximum difference value \( d_i^{j,k} \) for each pixel using equation (19).

**Step 4.** Calculate the number of bits embedded into the pixel using the following equation. The number of secret bits in each pixel is defined as \( \hat{t}_i^{j,k} \)

\[ \hat{t}_i^{j,k} = \left\lfloor \log_2 d_i^{j,k} \right\rfloor \]

**Step 5.** Extract the embedded secret data \( s_i^{j,k} \) using \( \hat{t}_i^{j,k} \) and the following equation

\[ s_i^{j,k} = \left\lfloor (S_1 p_i^{j,k} - c_i^{j,k}) + (S_2 p_i^{j,k} - c_i^{j,k}) \right\rfloor \]

**Step 6.** Repeat the above steps for all blocks.

**Figure 2.** Embedding example.
An example of the extraction and recovering algorithm is as follows. The stego-image is divided into $2 \times 2$ size blocks. In the first block, the cover pixels $c_{1,0}^0 = (125 + 114)/2 = 120, c_{1,1}^0 = (141 + 138)/2 = 140, c_{1,0}^1 = (127 + 122)/2 = 125$, and $c_{1,1}^1 = (119 + 104)/2 = 112$ are restored using equation (23). And, the maximum values $d_{1,0}^0 = 20, d_{1,1}^0 = 15$, and $d_{1,1}^1 = 28$ are calculated using equation (19). The size of the secret data $s_{1,0}^0 = 125 - 120 = 11, s_{1,1}^0 = 141 - 140 + 138 - 140 = 11, s_{1,1}^1 = 127 - 125 + 122 - 125 = 5$, and $s_{1,1}^1 = 119 - 112 + 104 - 112 = 15$ are extracted using $l'_{j, k}$ and equation (25). This extraction and recovering example is shown in Figure 3.

### Experiment results and analysis

The reversible data hiding scheme measures the image quality and embedding capacity to evaluate the performance of the proposed algorithm. The embedding capacity of the secret data means the amount of secret data that can be inserted into a cover image. The visual image quality means the degree of distortion of the stego-image. The PSNR is used to evaluate the quality of an image in general. If the PSNR is more than 30 dB, image distortion cannot be detected easily by the human visual system. Therefore, most reversible data hiding schemes aim to keep the PSNR value above 30 dB. There is a trade-off relationship between the embedding capacity and the PSNR. In the data hiding scheme, the goal is to increase the embedding capacity while maintaining good image quality. The PSNR is defined as equation (26)

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

When the pixels of the cover image are $p_i$ and the pixels of the stego-image are defined as $p'_i$, the mean squared error MSE is defined in equation (27)

$$MSE = \frac{W \times H \sum_{i=1}^{w} (p_i - p'_i)^2}{W \times H}$$

In the proposed method, two $512 \times 512$-sized stego-images are generated using a cover image of $512 \times 512$ sizes as shown in Figures 4–6. In 2002, Wang and Bovik proposed a method to measure the quality index of images using correlation loss, luminance distortion, and contrast distortion

$$Q = \frac{48 \delta_x \delta_y p_x p_y}{(\delta_x^2 + \delta_y^2)(p_x^2 + p_y^2)}$$

Each element of the equation is given in equations (29)–(31)

$$p_x = \frac{1}{wh} \sum_{i=0}^{wh-1} p_i, \quad p_y = \frac{1}{wh} \sum_{i=0}^{wh-1} p'_i$$

$$\delta_x = \frac{1}{wh} \sum_{i=0}^{wh-1} (p_i - p_x)^2, \quad \delta_y = \frac{1}{wh} \sum_{i=0}^{wh-1} (p'_i - p_y)^2$$

$$\delta_{xy} = \frac{1}{wh - 1} \sum_{i=0}^{wh-1} (p_i - p_x)(p'_i - p_y)$$

The exponent is defined as the combination of loss of correlation, luminance distortion, and contrast distortion, and is redefined as equation (32)

$$Q = \frac{\delta_{xy}}{\delta_x \delta_y} \frac{2p_x p_y}{p_x^2 + p_y^2} \frac{2\delta_x \delta_y}{\delta_x^2 + \delta_y^2}$$
\( \delta_{xy} / \delta_x \delta_y \) is the correlation coefficient between the two images. The second element \( \frac{2p_x p_y}{p_x^2 + p_y^2} \) measures the luminance between the two images, and the third element \( 2\delta_x \delta_y / \delta_x^2 + \delta_y^2 \) compares the two images to measure the similarity of the two images.

**Visual image quality**

The first stego-images with PSNR values are shown in Figure 5, and the second stego-images with PSNR values are shown in Figure 6. Figures 5 and 6 show that all images of the proposed scheme maintain a PSNR value over 30 dB.

Table 3 compares the PSNR of the proposed scheme and other schemes when the embedding capacity is about 500,000 bits. In Table 3, the average PSNR of the proposed scheme is 50.9679 dB. Yao et al.’s average PSNR is 51.1431 dB, and Shastri and Thanikaiselvan’s average PSNR is 53.0077 dB. Shastri and Thanikaiselvan’s PSNR is about 2 dB higher than the proposed scheme. However, the proposed scheme keeps the PSNR value more than 42 dB, so there is no problem.

**Embedding capacity**

The maximum embedding capacity of the proposed scheme and other schemes is compared in Table 5. The average embedding capacity of the proposed scheme is at least about 100,000 bits higher than Lu et al.’s scheme and Yao et al.’s scheme on average. And, the average embedding capacity of the proposed scheme is at least about 600,000 bits higher than Shastri and Thanikaiselvan’s scheme on average. Shastri and Thanikaiselvan’s scheme aims to improve the image quality when the embedding capacity is not large, so the maximum embedding capacity is low. As a result, the proposed scheme can embed more secret data than
other schemes while maintaining the degree of image distortion that cannot be detected by the human visual system. Figure 7 compares the maximum embedding capacity using a histogram. The histogram shows that the proposed scheme has higher embedding capacity than other schemes in most images. And, the embedding capacity of secret data is almost constant in other schemes. However, the proposed scheme can embed the secret data up to 1,800,000 bits depending on the characteristics of the image. In the case of Baboon image and Bridge image, the embedding capacity of secret data is high because of the large difference between adjacent pixels.

Quality index

Figure 8 shows the quality index values for each cover image. The quality index measures the loss of correlation, luminance distortion, and contrast distortion between the cover image and the stego-image. The proposed scheme maintains a similar quality index to Lu et al.’s scheme, Yao et al.’s scheme, and Shastri and Thanikaiselvan’s scheme. Therefore, the proposed scheme has a higher embedding capacity than other schemes, and the image quality is similar to other schemes.

PSNR and embedding capacity

Figure 9 shows PSNR and embedding capacity of the six images of the proposed scheme in the graph. The proposed scheme embedded more than 1,300,000 bits secret data while keeping PSNR more than 40 dB in tank image. In the case of truck image and Elaine image, the proposed scheme embedded more than 1,300,000 bits secret data while keeping PSNR about 39 dB. In other images, the PSNR can be maintained at more than 34 dB while maintaining an embedding capacity of more than 1,300,000 bits. The proposed scheme has lower PSNR than other schemes when the embedding capacity is low. However, when the embedding capacity is increased, PSNR is higher than other
schemes. In the case of embedding capacity is 1,300,000 bits, PSNR is higher than other schemes for most images.

Figure 6. Second stego-images: (a) Lena (38.2845 dB), (b) Peppers (38.2407 dB), (c) Baboon (30.7269 dB), (d) Boat (35.9289 dB), (e) Barbara (32.9912 dB), (f) Airport (34.0230 dB), (g) Elaine (37.9787 dB), (h) Man and woman (35.5408 dB), (i) Crowd (36.3602 dB), (j) Tank (38.4224 dB), (k) Bridge (32.6074 dB), and (l) Truck (38.6272 dB).

Table 3. Comparison of PSNR values (embedding capacity: 500,000 bits).

| Images          | Embedding capacity: about 500,000 bits |
|-----------------|----------------------------------------|
|                 | PSNR(dB)                               |
|                 | Lu et al.’s scheme                     |
|                 | Yao et al.’s scheme                    |
|                 | Shastri and Thanikaiselvan’s scheme    |
|                 | Proposed scheme                        |
|                 | Stego image 1  | Stego image 2  | Stego image 1  | Stego image 2  | Stego image 1  | Stego image 2  | Stego image 1  | Stego image 2  |
| Lena            | 51.1411     | 51.1411     | 54.6650     | 54.6563     | 54.3882     | 49.0005     | 54.3882     | 49.0005     |
| Peppers         | 51.1410     | 51.1410     | 54.1421     | 54.6563     | 54.3882     | 49.0005     | 54.3882     | 49.0005     |
| Boat            | 51.1411     | 48.1477     | 51.1412     | 54.6929     | 53.9046     | 49.1195     | 53.9046     | 49.1195     |
| Airport         | 51.1410     | 51.1411     | 54.6863     | 51.6446     | 52.6487     | 48.2680     | 52.6487     | 48.2680     |
| Elaine          | 51.1411     | 51.1411     | 54.6563     | 51.6495     | 54.1089     | 49.1711     | 54.1089     | 49.1711     |
| Man and woman   | 45.7249     | 45.7250     | 54.2411     | 51.1011     | 49.2490     | 46.6389     | 49.2490     | 46.6389     |
| Crowd           | 51.1411     | 51.1411     | 54.6648     | 51.6525     | 50.3859     | 47.5465     | 50.3859     | 47.5465     |
| Tank            | 51.1411     | 51.1411     | 54.6542     | 51.6470     | 55.6880     | 49.9683     | 55.6880     | 49.9683     |
| Bridge          | 28.0364     | 28.0364     | 54.3411     | 51.0411     | 52.7151     | 48.3978     | 52.7151     | 48.3978     |
| Truck           | 51.1411     | 51.1411     | 54.6455     | 51.6422     | 55.6468     | 48.8563     | 55.6468     | 48.8563     |
| Average         | 48.2889     | 47.9896     | 54.5335     | 51.4819     | 53.2452     | 48.6907     | 53.2452     | 48.6907     |

Conclusion and discussion

In this article, a dual image–based reversible data hiding scheme using PVD has been proposed. The cover image
Table 4. Comparison of PSNR values (embedding capacity: 800,000 bits).

| Images          | Embedding capacity: about 800,000 bits | PSNR (dB) |
|-----------------|----------------------------------------|-----------|
|                 | Lu et al.’s scheme | Yao et al.’s scheme | Shastri and Thanikaiselvan’s scheme | Proposed scheme |
|                 | Stego image 1 | Stego image 2 | Stego image 1 | Stego image 2 | Stego image 1 | Stego image 2 | Stego image 1 | Stego image 2 |
| Lena            | 46.3669 | 44.1555 | 46.3806 | 46.3777 | 50.6910 | 49.8983 | 41.9185 | 40.8975 |
| Peppers         | 46.2210 | 44.1201 | 46.2510 | 46.1211 | 50.6812 | 49.8921 | 41.6747 | 40.6505 |
| Boat            | 45.1355 | 43.3782 | 46.3821 | 46.378 | 50.6754 | 49.8839 | 41.7740 | 40.7788 |
| Airport         | 46.3753 | 44.1496 | 46.3825 | 46.3812 | 50.7011 | 49.8971 | 40.4291 | 39.5992 |
| Elaine          | 46.3632 | 44.1528 | 46.3775 | 46.3674 | 50.6918 | 49.8900 | 44.6722 | 43.1341 |
| Man and woman   | 46.7249 | 44.1350 | 46.1229 | 46.0519 | 50.6956 | 49.8900 | 41.5937 | 40.6720 |
| Crowd           | 46.4022 | 44.1653 | 46.3630 | 46.3663 | 50.6892 | 49.9021 | 39.8101 | 39.0848 |
| Tank            | 46.3639 | 44.1586 | 46.3833 | 46.3782 | 50.6848 | 49.8997 | 44.9897 | 43.4184 |
| Bridge          | 45.1264 | 44.0162 | 46.1626 | 46.1201 | 50.7123 | 49.9110 | 45.8635 | 43.7844 |
| Truck           | 46.3605 | 44.1366 | 46.3611 | 46.3689 | 50.6795 | 49.8892 | 46.6001 | 44.3163 |
| Average         | 46.1439 | 44.0567 | 46.3166 | 46.2910 | 50.6901 | 49.8953 | 42.9298 | 41.6336 |

Table 5. Comparison of maximum embedding capacity.

| Images          | Embedding capacity (bits) |
|-----------------|--------------------------|
|                 | Lu et al.’s scheme | Yao et al.’s scheme | Shastri and Thanikaiselvan’s scheme | Proposed scheme |
| Lena            | 1,310,720 | 1,310,928 | 844,386 | 1,193,320 |
| Peppers         | 1,352,538 | 1,310,220 | 844,740 | 1,272,538 |
| Baboon          | 1,310,480 | 1,318,738 | 844,735 | 1,893,914 |
| Boat            | 1,310,640 | 1,319,012 | 844,429 | 1,471,024 |
| Barbara         | 1,310,720 | 1,318,939 | 844,237 | 1,472,104 |
| Airport         | 1,310,690 | 1,318,866 | 844,373 | 1,532,374 |
| Elaine          | 1,310,715 | 1,318,877 | 844,709 | 1,478,328 |
| Man and woman   | 1,310,525 | 1,318,742 | 844,609 | 1,460,710 |
| Crowd           | 1,310,576 | 1,318,826 | 844,783 | 1,138,294 |
| Tank            | 1,310,720 | 1,318,960 | 844,462 | 1,424,864 |
| Bridge          | 1,310,220 | 1,318,220 | 844,611 | 1,818,296 |
| Truck           | 1,310,720 | 1,318,937 | 844,869 | 1,335,548 |
| Average         | 1,314,105 | 1,317,435 | 844,579 | 1,457,610 |

Figure 7. Comparison of embedding capacity of the proposed scheme and other schemes.
Figure 8. Comparison of the quality index about four images.

Figure 9. Comparison of embedding capacity and PSNR of dual stego-images: (a) Tank, (b) Truck, (c) Boat, (d) Airport, (e) Barbara, and (f) Elaine.
was divided into blocks of size $M \times M$, and the maximum difference value between the pixels in each block was calculated to decide the length of the embeddable bits. The proposed scheme increased the embedding capacity by using the maximum difference value in the sub-block. Two types of temporary values were generated by applying the ceil function and floor function to secret data. The temporary values have been combined with the pixel values of the cover image to generate two stego-images. The correlation of two stego-images was used to restore the cover image. The secret data could be extracted using the reconstructed cover image, where the maximum difference value and log function were used. Experimental results showed that the proposed scheme maintains the high embedding capacity and good image quality that has less distortion by the human visual system than the previous schemes. Also, the proposed scheme had the different embedding capacity depending on the characteristics of the cover image that makes robust to some attacks. In future work, we will plan to adopt interpolation techniques on dual images to increase the embedding capacity with good image quality.

Acknowledgements

We thank the anonymous reviewers for their valuable suggestions that improved the clarity of this article.

Author contributions

All authors discussed the contents of the manuscript and contributed to its preparation. P.-H.K. conducted all experiments and wrote the manuscript. K.-W.R. designed and conducted the literature review. K.-H.J. proposed the concept of algorithm and wrote the manuscript.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication 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 Korea Research Fellowship Program through the NRF funded by the Ministry of Science and ICT (2019H1D3A1A01101687).

ORCID iD

Ki-Hyun Jung https://orcid.org/0000-0002-0662-8355

References

1. Ker A. Improved detection of LSB steganography in grayscale images. In: Fridrich J (ed.) Information hiding workshop. Berlin: Springer, 2004, pp. 97–115.
2. Wu DC and Tsai WH. A steganographic method for images by pixel-value differencing. Pattern Recogn Lett 2003; 24: 1613–1626.
3. Jung KH. A survey of reversible data hiding methods in dual images. IETE Tech Rev 2016; 33: 441–452.
4. Kumar R, Kim DS and Jung KH. Enhanced AMBTC based data hiding method using hamming distance and pixel value differencing. I Inf Secur Appl 2019; 47: 94–103.
5. Kumar R and Jung KH. Robust reversible data hiding method based on two-layer embedding strategy. Inform Sciences 2019; 512; 96–107.
6. Wu NI, Wu KC and Wang CM. Exploiting pixel-value differencing and base decomposition for low distortion data embedding. Appl Soft Comput 2012; 12: 942–960.
7. Shen SY and Huang LH. A data hiding scheme using pixel value differencing and improving exploiting modification directions. Comput Secur 2015; 48: 131–141.
8. Hussain M, Wahab AWA, Anthony TS, et al. A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement. Signal Process 2017; 50: 44–57.
9. Tian J. Reversible data embedding using a difference expansion. IEEE T Circ Syst Vid 2003; 13: 890–896.
10. Ni Z, Shi Y, Ansari N, et al. Reversible data hiding. IEEE T Circ Syst Vid 2006; 13: 354–362.
11. Hussain M, Wahab AWA, Javed N, et al. Hybrid data hiding scheme using right-most digit replacement and adaptive least significant bit for digital images. Symmetry 2016; 8: 41.
12. Zhang R, Lu C and Liu K. A high capacity reversible data hiding scheme for encrypted covers based on histogram shifting. J Inf Secur Appl 2019; 47; 199–207.
13. Chang CC, Kieu T and Chou Y. Reversible data hiding scheme using two steganographic images. In: Proceeding of IEEE region 10 international conference, Taipei, 30 October–2 November 2007. IEEE.
14. Zhang X and Wang S. Efficient steganographic embedding by exploiting modification direction. IEEE Commun Lett 2006; 10; 781–783.
15. Lee C, Wang K, Chang C, et al. A reversible data hiding scheme based on dual steganographic images. In: Proceeding of the third international conference on ubiquitous information management and communication, Suwon, 15–16 January 2009, pp. 228–237. ACM.
16. Qin C, Chang C and Hsu T. Reversible data hiding scheme based on exploiting modification direction with two steganographic images. Multimed Tools Appl 2015; 74; 5861–5872.
17. Lu T, Wu J and Huang C. Dual-image-based reversible data hiding method using center folding starategy. Signal Process 2015; 115; 195–213.
18. Yao H, Qin C, Tang T, et al. Improved dual-image reversible data hiding method using the selection strategy of shiftable pixles' coordinates with minimum distortion. Signal Process 2017; 135; 26–35.
19. Shastrli S and Thanikaiselvan V. Dual image reversible data hiding using trinary assignment and centre folding strategy with low distortion. J Vis Commun Image R 2019; 61: 130–140.
20. Wang Z and Bovik AC. A universal image quality index. IEEE Signal Proc Let 2002; 9; 81–84.