

# A hybrid steganography scheme with reduced difference expansion and pixel-value ordering

I Kadek Agus Ariesta Putra<sup>1</sup>, Ntivuguruzwa Jean De La Croix<sup>1,2</sup>, Tohari Ahmad<sup>1</sup>

<sup>1</sup>Department of Informatics, Faculty of Electrical Engineering and Intelligent Informatics, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia

<sup>2</sup>College of Science and Technology, University of Rwanda, Kigali, Rwanda

## Article Info

### Article history:

Received Jun 12, 2024

Revised Jun 30, 2025

Accepted Jul 13, 2025

### Keywords:

Information security

Pixel-value ordering

Reduced difference expansion

Reversible data hiding

Steganography

## ABSTRACT

Steganography embeds secret messages into public media while ensuring the stego content remains visually indistinguishable from the original. The primary challenge lies in maximizing embedding capacity and image quality without introducing noticeable distortions. This research proposes a novel reversible data hiding (RDH) scheme that integrates reduced difference expansion (RDE) with four directional pixel-value ordering (PVO) schemes, horizontal, vertical, diagonal-right, and diagonal-left, to enhance embedding efficiency and visual fidelity. Unlike existing RDH methods that apply RDE with fixed or limited PVO directions, the proposed scheme dynamically selects the optimal PVO orientation based on pixel pair characteristics, effectively improving local prediction accuracy and reducing embedding-induced distortion. Previous studies have largely overlooked this relationship between pixel pair selection and embedding performance. Experimental evaluation on medical images with secret data sizes ranging from 5 kb to 100 kb demonstrates significant gains over recent PVO-based methods. The proposed method increases the average embedding capacity from 0.8315 to 0.9781 bit per pixel (bpp) (a 17.6% improvement) and raises the average peak signal-to-noise ratio (PSNR) from 49.44 to 53.40 dB, reducing distortion by approximately 3.96 dB.

This is an open access article under the [CC BY-SA](#) license.



## Corresponding Author:

Tohari Ahmad

Department of Informatics, Faculty of Electrical Engineering and Intelligent Informatics

Institut Teknologi Sepuluh Nopember

Surabaya, Indonesia

Email: tohari@its.ac.id

## 1. INTRODUCTION

Steganography is the art of concealing secret information within other data so that the presence of the hidden message remains undetectable to unintended parties [1]. Steganography has been used since ancient times, where secret messages were hidden in various physical forms of media [2], and has since evolved in the digital era to embed data within files such as images [3]–[5], audio [6]–[8], video [9], [10], and electrocardiogram (ECG) signals [11]. Its applications span secret communication [12], digital watermarking [13], and copyright protection [14], enabling the secure embedding of information without perceptibly altering the host media. A significant subfield within steganography is reversible data hiding (RDH), which enables the exact recovery of the hidden data and the original cover media after extraction [3]. One of the foundational techniques in RDH is difference expansion, which embeds information by expanding the difference between paired pixel values [4]. Although difference expansion offers high embedding capacity, it tends to introduce noticeable distortion, particularly in smooth image regions [5].

To mitigate this, reduced difference expansion (RDE) was introduced to constrain the difference expansion and limit distortion [6]. Pixel-value ordering (PVO), another key concept in RDH, sorts pixel groups based on intensity and predicts differences more precisely, which helps improve embedding accuracy and reduce visual degradation [7]. However, most existing approaches apply PVO in a fixed orientation, often overlooking the impact of directional pixel pair selection on overall steganographic performance [8].

One of the main challenges in steganography is ensuring that the modified original media (stego) does not raise suspicion. High distortion in the original media due to the data hiding process can be a conspicuous sign that the media is carrying secret information. When images, audio, or video undergo significant changes in quality or visual/auditory structure, this can attract the attention of third parties observing. The main problem lies in the trade-off between embedding capacity and distortion. Increasing payload size often requires more aggressive modifications to the media, which exacerbates detectable anomalies and risks exposing hidden data [15]. Furthermore, reversibility itself presents another challenge. In certain contexts, such as medical imaging, legal documents, or digital media forensics, the integrity of the original media must be maintained after confidential data has been extracted. Based on this reversibility aspect, steganography is divided into reversible and irreversible techniques. RDH techniques allow full recovery of the cover media after the secret data extraction process, whereas irreversible techniques do not allow full recovery of the cover media.

Various steganography schemes have been proposed to address the issue of high distortion. One such scheme is RDE based on difference expansion, as introduced in [16], which embeds secret data by exploiting differences between pairs of pixels. However, difference expansion can lead to significant distortion when large differences are required to store data. This drawback is mitigated in RDE, a more advanced method proposed in [17], [18] that reduces the size of the differences using logarithmic and exponential functions. Previous research on difference expansion and RDE has focused on data embedding scheme algorithms, which require pixel pairs to perform the embedding process. The selection of these pixel pairs tends to be done by sorting the pixels in a flat sequence [19], which can result in the selection of pairs with high distortion. To address this issue, the study in [20], [21] proposed the concept of PVO, which focuses on sorting pixel values within blocks of pixels in data embedding. While this concept shares the same objective, the PVO technique's limitation is that it is only limited to specific pixel blocks.

This research presents an RDH scheme integrating an enhanced RDE technique with adaptive PVO to achieve high embedding capacity and low distortion. The key concept of this scheme is the computation of reduced difference values, which allows each pixel pair to store up to 2 bits of secret data. The proposed PVO scheme arranges pixel indices based on intensity to optimize embedding, guiding the selection of pixel pairs. Unlike previous methods that rely on fixed pixel blocks, this approach applies four directional PVO schemes, horizontal, vertical, right-diagonal, and left-diagonal, to exploit spatial correlations across different orientations. This adaptability reduces distortion and increases capacity by aligning pixel ordering with local image structures. This method is particularly suitable for real-world applications such as secret communication, copyright protection, and medical data security, where fidelity and confidentiality are essential. Thus, the main contributions of this research are:

- i) Introduction of a novel RDE-based RDH method: this study proposes an advanced RDH technique that integrates an enhanced reversible difference expansion mechanism. The innovation significantly minimizes the distortion typically introduced during data embedding, thereby preserving the original image's visual quality. Unlike traditional RDE schemes, this approach can embed up to 2 bits per pixel pair without causing noticeable artifacts, making it suitable for sensitive image applications such as medical imaging or secure communications.
- ii) Development of an adaptive PVO scheme to improve embedding efficiency: the research also presents a refined PVO mechanism that arranges pixel indices based on intensity levels to guide efficient embedding. Instead of relying on static pixel blocks, this method adapts to local image characteristics by employing four directional PVO strategies: horizontal, vertical, right-diagonal, and left-diagonal. This orientation-aware embedding framework utilizes spatial correlations within the image, leading to higher data capacity and reduced visual distortion.

This paper is organized into 4 sections. Section 1 provides an overview of the research problem. In section 2, several RDE and PVO schemes are introduced. Section 3 introduces and explains the proposed method in detail, including how this method is intended to solve the research problem. Section 4 presents an evaluation of the proposed method and compares the experimental results of this method with previous methods. Section 5, in conclusion, summarizes this research and discusses the potential future work.

## 2. RELATED WORKS

Research related to RDE was first introduced in [17]. The authors identified limitations to traditional difference expansion techniques, particularly the degradation of visual quality when used for multilayer embedding and the risk of overflow or underflow. An RDE scheme was proposed to reduce the difference value in traditional difference expansion methods by implementing transformation functions based on exponential and logarithmic operations to address these issues. Further developments were conducted in [22], introducing a new transformation function with a wider range. This function proved more effective in improving image quality damaged by multilayer embedding. However, key challenges such as low embedding capacity are still a significant limitation in applying such methods.

To improve the security and quality of data embedding in medical images, studies in [23], [24] proposed an RDE method that operates on  $2 \times 2$  pixel blocks ( $p_1, p_2, p_3, p_4$ ). These blocks are categorized into three types: expandable, changeable, and unchangeable. To overcome the problem of overflow or underflow, only blocks with expandable and changeable categories are used to embed 1-bit secret data. This method adjusts the base point used to calculate the difference value for the other three pixels, such as at  $p_2$  for the method in [23] and in order  $p_3$  for the method in [24]. In expandable blocks, absolute difference values greater than 1 are reduced using a transformation function before the secret data is embedded, while values outside this range are handled using traditional difference expansion. The secret data is embedded in the least significant bit or using traditional difference expansion [23] for mutable blocks. Although this RDE concept successfully addresses the problem of high distortion and improves image quality, the pixel block selection process remains a challenge, especially in finding the optimal base point to achieve minimal difference values and still results in many unchangeable blocks affecting the embedding capacity.

Shifting the focus to PVO-based approaches, Lee *et al.* [21] present an approach for RDH schemes by utilizing a combination of PVO and two-layer embedding to improve the efficiency of hiding secret data in digital images. By dividing the data embedding process into two layers, the first and second layers utilize different block partition models to avoid the overuse of pixels, thus improving the overall performance. This scheme utilizes the PVO technique to predict and embed secret data by sorting the pixel values within each block. Despite its advantages, there is a limitation of the PVO technique used: it is only limited to certain blocks of pixels. This limitation reduces its flexibility and embedding capacity as complex blocks with high variations in pixel values are often skipped, thus limiting the amount of secret data that can be embedded in the image.

Advancing PVO-based methodologies, Ren *et al.* [25] presents a dynamic hybrid RDH technique designed to enhance data embedding capacity and image quality. The approach refines the traditional PVO method by classifying image blocks into three categories: extremely smooth, smooth, and rough, based on their complexity. A block subdivision algorithm is applied for smooth blocks, allowing up to 6 bits of data to be embedded. In extremely smooth blocks, a median pixel prediction technique is utilized to predict the remaining pixels, enabling the embedding of up to 8 bits of data. Rough blocks are excluded from embedding to avoid distortion. The experimental results demonstrate that this method offers significantly higher embedding capacity and better image quality than traditional PVO techniques. However, the method's effectiveness is influenced by the texture characteristics of the image, particularly the smoothness of the blocks being processed.

Furthermore, various studies have been conducted on applying PVO in prediction error expansion (PEE) schemes. Kaur *et al.* [20] proposed an RDH scheme involving PVO in the form of a sorting strategy combined with PEE by embedding secret data into the least significant pixels sorted by their prediction error. Similarly, Chi *et al.* [26] explored PVO and PEE, a scheme that derives predicted values from the sorted pixel values, which utilizes two steps of prediction error triplet expansion based on PVO. Overall, previous research on the PVO concept has similarities in sorting pixel values within blocks of pixels in data embedding. However, the fundamental difference lies in the approach proposed in this method, where PVO is more focused on sorting the pixel indices to select the right pixel block rather than sorting the pixel values within the block.

## 3. PROPOSED METHOD

Traditional difference expansion, as proposed in [27], embeds secret data by expanding the difference values of adjacent pixel pairs. Specifically, given a pair of pixels  $(x, y)$ , difference expansion first calculates the average value  $l = \lfloor (x + y)/2 \rfloor$  and the difference value  $h = x - y$ . Next, the secret bit will be embedded by modifying the difference value  $h$ , which will also be used to perform reversible reconstruction. Although difference expansion is quite simple and effective, it tends to have high distortion especially when it has a large difference value.

To address this limitation, RDE is introduced as an improvement that reduces the difference value by applying transformation functions such as logarithmic or exponential scaling [17]. By limiting the reduced difference value, RDE is not only able to reduce distortion, but is also able to increase the embedding

capacity as more smooth pixel pairs will be embeddable. To achieve this, RDE requires two additional components: a secret table (ST) and a location map (LM). The ST stores the selected pixel pairs' location for data hiding, ensuring that only suitable locations (with low visual impact) are used. The LM records the information required during the extraction and restoration process. Based on these principles, we design a novel embedding algorithm that integrates RDE with an improved pixel selection mechanism using the PVO scheme, thus enabling efficient RDE with minimized distortion.

### 3.1. The proposed data hiding scheme using reduced difference expansion

#### 3.1.1. Data embedding

The proposed scheme requires a pair of  $x$  and  $y$  pixels to embed 2 bits of secret data. As seen in Figure 1, this process begins with calculating the difference value  $d$  based on the values of  $x$  and  $y$  using (1).

$$d = \begin{cases} y - x, & \text{if } y > x \\ x - y, & \text{otherwise} \end{cases} \quad (1)$$

Once the  $d$  value is obtained, we then need to check whether this  $d$  value can be expanded or not. In this context, the  $d$  value is considered expendable if it exceeds 3. If this condition is met, then the  $d$  value can be expanded, and it will be adjusted according to (2). Conversely, if the  $d$  value is less than or equal to 3, it is deemed non-expandable. In such instances, the  $ST$  value is updated to 2.

$$d' = \begin{cases} \left\lfloor \frac{d}{4} \right\rfloor - \left\lfloor \frac{\lceil \log_2 d \rceil}{\sqrt{d}} \right\rfloor, & \text{if } d > 3 \\ d, & \text{otherwise} \end{cases} \quad (2)$$

The next stage in this procedure involves embedding the secret data ( $S$ ). This is accomplished by utilizing (3). Once the secret data is successfully embedded, it's necessary to update the most recent  $x$  and  $y$  values as  $x'$  and  $y'$ . This update is done using (4).

$$d'' = d' \times 4 + S \quad (3)$$

$$x', y' = \begin{cases} x' = y + d'' \text{ and } y' = y, & \text{if } x > y \\ y' = x + d'' \text{ and } x' = x, & \text{otherwise} \end{cases} \quad (4)$$

After successfully obtaining the new values of  $x$  and  $y$ , the subsequent step involves validating these values. This validation aims to ensure that the values of  $x'$  and  $y'$  remain within the acceptable range of 0 to 255, corresponding to the valid color range. This step is crucial as it prevents overflow or underflow, which could cause errors in the subsequent processes. Preventing this overflow or underflow follows what is shown in (5).

$$\text{overflow/underflow} = \begin{cases} \text{true}, & \text{if } 0 \leq x \leq 255 \\ \text{false}, & \text{otherwise} \end{cases} \quad (5)$$

If the updated values of  $x$  and  $y$  fall outside the valid color range, it implies that this pixel pair is unsuitable for embedding secret data. In such a case, the  $ST$  value is then updated to 0 as an indicator of a non-embeddable pair. Therefore, we need to look for other pixel pairs as an alternative. However, if this pixel pair can embed the secret message ( $ST \neq 0$ ), then the next step is to determine the  $LM$  value by using the (6).

$$LM = d \bmod 4 \quad (6)$$

#### 3.1.2. Data extraction process

In the secret data extraction stage, the first step that must be taken is to obtain pixel pairs from the stego image. The stego image is an image that has been used to hide secret data within it. After obtaining the pixel pairs and the locations where the secret data is hidden, the next step is performing a series of calculations. These calculations are the reverse of the data insertion process, intending to reveal again the secret data that has been hidden. The process of extracting this secret data is carried out, as seen in Figure 2.

To carry out the extraction of secret data, there are two important values needed, namely the  $ST$  value and the  $LM$  value. These two values are usually transmitted differently and are required for extraction. The first step in the extraction process is to calculate the difference value  $d''$ . This value is obtained using (7). If the  $ST$  value is -1, 1, or 2, then secret data is hidden in that pixel pair. Conversely, if the

$ST$  value is 0, then there is no secret data hidden in that pixel pair. After obtaining the  $d''$  value, the next step is to extract the secret data and regain the original  $d$  value. The secret data  $S$  value is obtained using the (8).

$$d'' = \begin{cases} x' - y', & \text{if } ST = -1 \\ y' - x', & \text{if } ST \in \{1, 2\} \end{cases} \quad (7)$$

$$S = d'' \bmod 4 \quad (8)$$

To restore the difference value  $d''$  to its original value  $d$ , several steps must be taken depending on the  $ST$  value. If  $ST \in \{1, 2\}$ , the  $d'$  value can be obtained using (9), and the original  $d$  value can be obtained using (10). If the  $ST$  value is 2, then the original  $d$  value can be obtained using (11). After all these steps are completed, the initial values of  $x$  and  $y$  can be calculated using the (12). Thus, the secret data extraction process is complete. The previously hidden secret data within the image has now been successfully obtained, and we can also retrieve the original cover image.

$$d' = \left\lfloor \frac{d'' - S}{4} \right\rfloor \quad (9)$$

$$d = 4 \times \left( d' + \left\lfloor \log_2 d' \right\rfloor \sqrt{d'} \right) + LM \quad (10)$$

$$d = \left\lfloor \frac{d'' - S}{4} \right\rfloor \quad (11)$$

$$x, y = \begin{cases} y = y' \text{ and } x = y + d, & \text{if } ST = -1 \\ x = x' \text{ and } y = x + d, & \text{if } ST \in \{1, 2\} \end{cases} \quad (12)$$

In general, the comparison between the proposed method and the previous methods [24], [28] is illustrated in Table 1. Another key difference is that methods [24], [28] embed 1 secret message for each difference value  $d$ . In contrast, the proposed method embeds 2 bits of secret message for each difference value  $d$ , resulting in a larger embedding capacity.

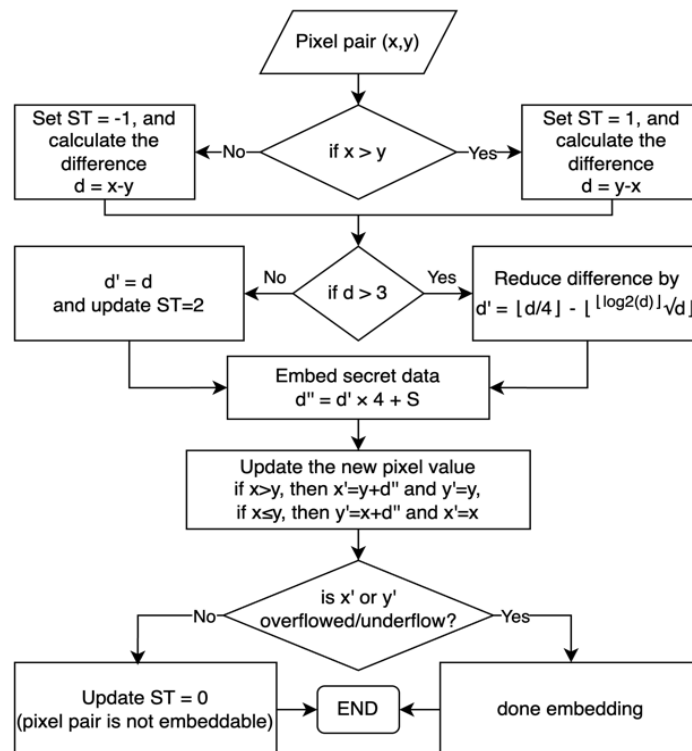


Figure 1. Data embedding process

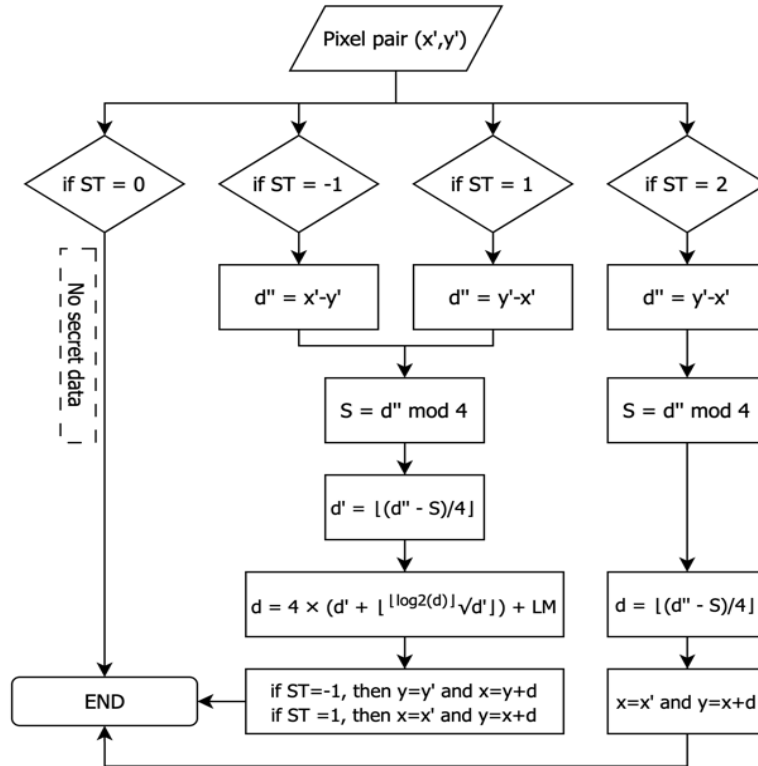


Figure 2. Data extraction process

Table 1. Comparison between the method in [24], [28], and the proposed method

Method	Pixel block (p)	Difference (d <sub>n</sub> )	Reduced difference expansion (d' <sub>n</sub> )	New pixel computation (p')
Method in [24]	2 × 2 (p <sub>0</sub> , p <sub>1</sub> , p <sub>2</sub> , p <sub>3</sub> )	$\begin{cases} d_0 = p_0 - p_2 \\ d_1 = p_1 - p_2 \\ d_2 = 0 \\ d_3 = p_3 - p_2 \end{cases}$	$\begin{cases} d_n - (2 + 2^{\lfloor \log_2(d_n) \rfloor}) + \lfloor \frac{\log_2(d_n)}{\sqrt{d_n}} \rfloor, \text{ if } d_n > 1 \\ d_n + (2 + 2^{\lfloor \log_2(d_n) \rfloor}) + \lfloor \frac{\log_2(d_n)}{\sqrt{d_n}} \rfloor, \text{ if } d_n < 1 \end{cases}$	$\begin{cases} p'_0 = d''_0 + p_2 \\ p'_1 = p_1 + p_2 \\ p'_2 = p_2 \\ p'_3 = h''_3 + p_2 \end{cases}$
Method in [28]	3 × 3 (p <sub>0</sub> , p <sub>1</sub> , ..., p <sub>8</sub> )	$\begin{cases} d_0 = p_0 - p_4 \\ d_1 = p_1 - p_4 \\ \dots \\ d_3 = p_3 - p_4 \end{cases}$	$\begin{cases} d_n - 2^{\lfloor \log_2(d_n) \rfloor - 1}, \\ \text{ if } 2 \times 2^{\lfloor \log_2(d_n) \rfloor - 1} \leq d_n \leq 3 \times 2^{\lfloor \log_2(d_n) \rfloor - 1} \\ d_n - 2^{\lfloor \log_2(d_n) \rfloor}, \\ \text{ if } d_n < 3 \times 2^{\lfloor \log_2(d_n) \rfloor - 1} \leq d_n \leq 4 \times 2^{\lfloor \log_2(d_n) \rfloor} - \end{cases}$	$\begin{cases} p'_0 = d''_0 + p_2 \\ p'_1 = p_1 + p_2 \\ \dots \\ p'_3 = h''_3 + p_1 \end{cases}$
Proposed method	1 × 2 (p <sub>0</sub> , p <sub>1</sub> )	p <sub>1</sub> - p <sub>0</sub>	$\begin{cases} \lfloor \frac{d}{4} \rfloor - \lfloor \frac{\log_2 d}{\sqrt{d}} \rfloor, \text{ if } d > 3 \\ d, \text{ otherwise} \end{cases}$	$\begin{cases} p'_0 = p_1 + d'', \text{ if } p_0 \geq p_1 \\ p'_1 = p_1 \\ p'_0 = p_0 \\ p'_1 = p_1 + d'', \text{ if } p_0 < p_1 \end{cases}$

### 3.1.3. Embedding capacity and distortion measurement

Embedding capacity is measured in terms of bit per pixel (bpp), quantifying how much secret data can be embedded in each cover image pixel. The embedding capacity for a given image can be calculated using the (13).

$$\text{Embedding capacity} = \frac{\text{total embedded bits}}{\text{height} \times \text{width}} \quad (13)$$

Distortion is evaluated using peak signal-to-noise ratio (PSNR) as seen in (14) and structural similarity index measurement (SSIM). Mean squared error (MSE) is calculated by averaging the squared differences between the pixel values of the original image  $I_{jk}$  and the stego image  $I'_{jk}$  at the position  $(j, k)$ , where  $N$  and  $M$  represent the image dimensions as seen in (15).

$$PSNR = 10 \log_{10} \left( \frac{255^2}{MSE} \right) \quad (14)$$

$$MSE = \frac{1}{N \cdot M} \sum_{j=1}^N \sum_{k=1}^M (I_{jk} - I'_{jk})^2 \quad (15)$$

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (16)$$

SSIM, as seen in formula (16), measures the perceptual similarity between the original and stego images by considering structural information, luminance, and contrast. SSIM is based on comparing local pixel intensity patterns normalized for luminance and contrast. Where  $\mu_x$  and  $\mu_y$  are the mean intensities,  $\sigma_x^2$  and  $\sigma_y^2$  are the variances and  $\sigma_{xy}$  is the covariance between the two images. The constants  $C_1$  and  $C_2$  are used to stabilize the division with weak denominator values. SSIM values range from -1 to 1, 1 indicating perfect structural similarity.

### 3.2. Pixel-value ordering scheme

Most developed steganography methods focus solely on embedding a secret message into a pre-determined pair of pixels, known as fixed pixel pair position. In the methods cited in [29], the position of the pixel pairs is determined before assessing whether the pixel pair can be embedded with a secret message. There is concern that this fixed pixel pair placement could be problematic when faced with pixels whose positions are not adjacent, as shown in Figure 3. This figure illustrates the selection of pixel pairs using a common function usually used to change a 2-dimensional array into a 1-dimensional array, as found in [30], thus finding pixel pairs that are not adjacent, as seen in pair 3, which has a large difference value. Therefore, pixel pairs like "pair 3" tend to have the potential to become pixels that cannot be embedded with secret messages.

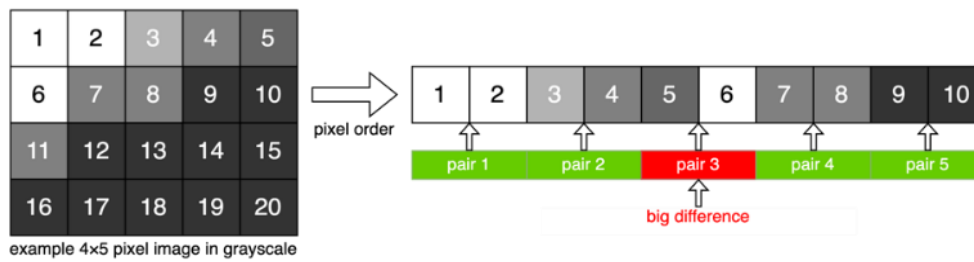


Figure 3. A problem in flatten-array PVO

In this study, a method was proposed that explores four different ways of selecting pixel pairs. The inspiration for this method came from the way a painter works. With his unique skills and style, a painter can move his brush in various directions, whether horizontally, vertically, or diagonally, to the right or left. By applying the same principle, the position of colors that are not much different can be found by scanning the image according to the assumed brush movement direction. Figure 4 illustrates these four ways of sorting pixels in detail. Horizontal pixel-value ordering (H-PVO) can be seen in Algorithm 1, vertical pixel-value ordering (V-PVO) in Algorithm 2, diagonal-right pixel-value ordering (R-PVO) in Algorithm 3, and diagonal-left pixel-value ordering (L-PVO) in Algorithm 4. By applying this method, we can ensure that the sequence of pixels obtained will be adjacent. Using this method, we can ensure the selected pixels will be adjacent, thus facilitating an efficient pixel pair selection and a more effective steganography process.

Algorithm 1: Horizontal pixel-value ordering

Input: P as  $N \times M$  pixel array

Output:  $P\_idx$  as a list of pixel pair position

```

1 row, col  $\leftarrow$  0;
2 col_inc  $\leftarrow$  1;
3  $P\_idx \leftarrow []$ ;
4 while length( $P\_idx$ ) <  $N \times M$  do
5    $P\_idx[] \leftarrow (row, col)$ 
6    $col = col + col\_inc$ 
```

Algorithm 2: Vertical pixel-value ordering

Input: P as  $N \times M$  pixel array

Output:  $P\_idx$  as a list of pixel pair position

```

1 row, col  $\leftarrow$  0;
2 row_inc  $\leftarrow$  1;
3  $P\_idx \leftarrow []$ ;
4 while length( $P\_idx$ ) <  $N \times M$  do
5    $P\_idx[] \leftarrow (row, col)$ 
6    $row = row + row\_inc$ 
```

```

7   if col ≥ M then
8       col = col + 1; row = row + 1;
10      col_inc = -1;
11  else if col < 0 then
12      col = 0; row = row + 1;
14      col_inc = 1;
15  end if
16 end while

```

Algorithm 3: Diagonal-right pixel-value ordering

Input:  $P$  as  $N \times M$  pixel arrayOutput:  $P\_idx$  as a list of pixel pair position

```

1   row, col ← 0; row_inc ← -1;
3   col_inc ← 1; P_idx ← [];
5   while length(P_idx) < N × M do
6       P_idx[] ← (row, col)
7       row = row + row_inc
8       col = col + col_inc
9       if row < 0 then
10          row = 0;
11          row_inc = 1; col_inc = -1;
13      else if row ≥ N then
14          col = col + 2; row = row - 1;
16          row_inc = -1; col_inc = 1;
18      else if col < 0 then
19          col = 0;
20          row_inc = -1; col_inc = 1;
22      else if col ≥ M then
23          row = row + 2; col = col - 1;
25          row_inc = 1; col_inc = -1;
27      end if
28  end while

```

```

7   if row ≥ N then
8       col = col + 1; row = row - 1;
10      row_inc = -1;
11  else if row < 0 then
12      col = col + 1; row = 0;
14      row_inc = 1;
15  end if
16 end while

```

Algorithm 4: Diagonal-left pixel-value ordering

Input:  $P$  as  $N \times M$  pixel arrayOutput:  $P\_idx$  as a list of pixel pair position

```

1   row, col ← 0; row_inc ← -1;
3   col_inc ← -1; P_idx ← [];
5   while length(P_idx) < N × M do
6       P_idx[] ← (row, col)
7       row = row + row_inc
8       col = col + col_inc
9       if row < 0 then
10          col = col + 2; row = 0;
12          row_inc = 1; col_inc = 1;
14      else if row ≥ N then
15          row = row - 1;
16          row_inc = -1; col_inc = -1;
18      else if col < 0 then
19          col = 0;
20          row_inc = 1; col_inc = 1;
22      else if col ≥ M then
23          col = col - 1; row = row - 1;
24          row_inc = -1; col_inc = -1;
27      end if
28  end while

```

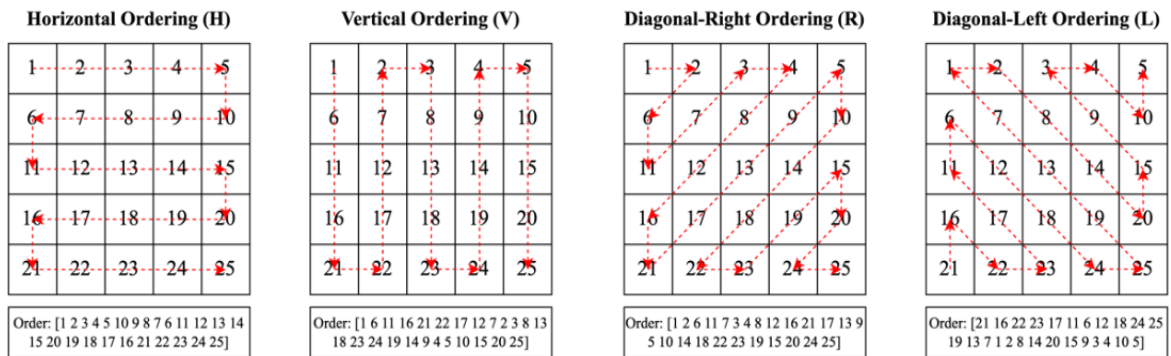


Figure 4. The proposed PVO scheme

Furthermore, the proposed method's scheme effects on the embedding capacity are illustrated in Figure 5. The figure shows the embedding of 6 bits of secret data (11, 11, and 00) into a  $3 \times 5$  grayscale image. The figure compares the flattened pixel array ordering with our PVO schemes. The pixel pairs used in each scheme are highlighted with a green border in the resulting stego image. The PSNR results show that the flattened pixel array ordering has the lowest PSNR. This is due to the high distortion when applied to our proposed RDE scheme. Meanwhile, the highest PSNR result of 38.888 dB is achieved with the diagonal-left pixel ordering. This indicates that the cover image characteristics are better suited for the diagonal-left pixel ordering scheme.



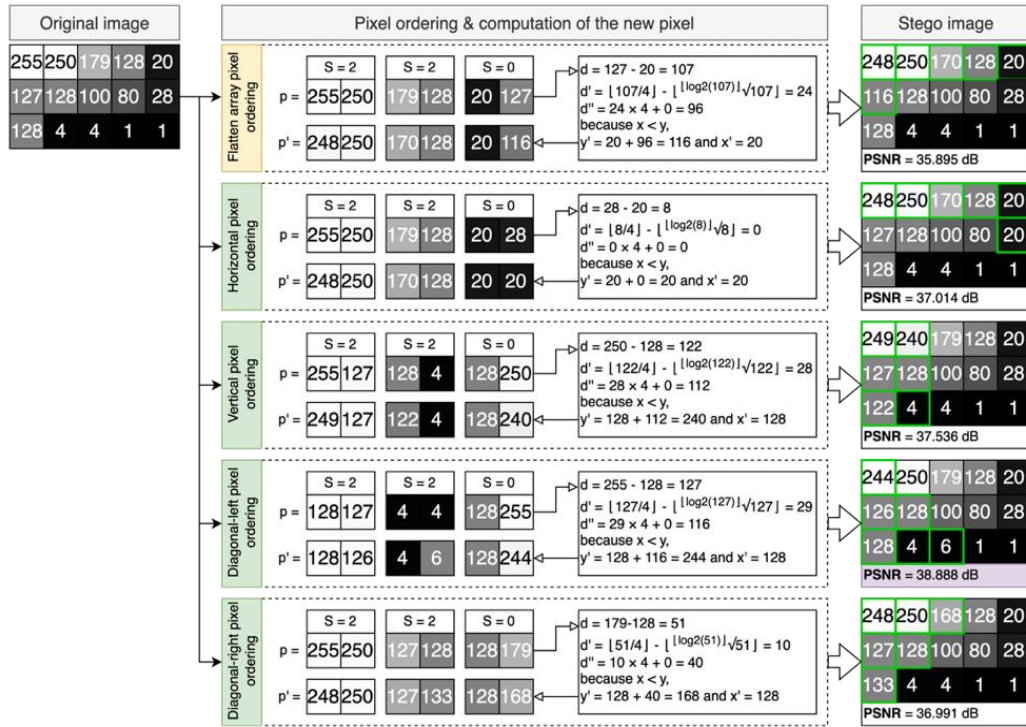


Figure 5. Illustration exemplifying the embedding process and its distortion impact

#### 4. RESULTS AND DISCUSSION

In this section, we will discuss the experimental results of the method we proposed. The experiment involved medical image pictures sized  $512 \times 512$  pixels as a medium for data hiding, including abdominal, chest, hand, head, and leg images from the public dataset [31]. The experiment was conducted against three different payload sizes, 5 kb, 10 kb, and 20 kb, compared to the method in [28] which has also shown the improvement of the method in [24]. Additionally, the experiments extended up to 100 kb to demonstrate the effects of PVO on each image.

To evaluate the quality of the stego image, we measure the PSNR value in decibels (dB), a metric commonly used to evaluate image quality after data insertion. We also include a comparison between our method and the existing RDE-based data hiding [28], to show the strengths of our method. We also included PSNR measurement results based on four ways of performing PVO: H-PVO, V-PVO, R-PVO, and L-PVO.

To evaluate the performance of the proposed method against state-of-the-art techniques, comparative results are presented in Tables 2 to 4, corresponding to payload capacities of 5 kb, 10 kb, and 20 kb, respectively. The experimental results show that the proposed method consistently achieves higher PSNR values than the existing method [30]. For example, at a payload of 10 kb, the proposed scheme records PSNR values of 58.42 dB (abdominal), 59.75 dB (chest), and 60.03 dB (hand), whereas the method in [28] achieves 56.18 dB, 57.33 dB, and 58.07 dB, respectively. This improvement of approximately 2 to 3 dB demonstrates the effectiveness of our pixel difference reduction strategy in preserving image quality. Similar trends are observed across all tested payload sizes. Regarding embedding capacity, Table 5 shows that L-PVO consistently achieves the highest values, 0.959 bpp for abdominal, 0.991 bpp for chest, 1.0 bpp for hand, and 0.997 bpp for leg images. For the head image, R-PVO delivers the best result with 0.958 bpp. These findings highlight the importance of choosing the appropriate PVO based on image structure to maximize quality and capacity.

Additionally, the proposed scheme enhances both PSNR and embedding capacity by adapting pixel pair ordering to the specific characteristics of each medical image. H-PVO achieves the highest PSNR for abdominal and chest images, while R-PVO is most effective for the leg image. Hand and head images perform best with either R-PVO or V-PVO. Although vertical ordering shows lower PSNR compared to other schemes, it still outperforms the method in [28]. As shown in Figure 6, the method maintains strong PSNR performance across payloads ranging from 40 kb to 100 kb.

Table 2. PSNR (dB) and SSIM values of embedding 5 kb secret message

Image	Method in [28]		Proposed							
			H-PVO		V-PVO		R-PVO		L-PVO	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Abdominal	51.3193	0.9990	51.7980	0.9991	58.4020	0.9988	51.3800	0.9984	53.0570	0.9983
Chest	51.2390	0.9988	51.2460	0.9991	58.7630	0.9988	53.3610	0.9985	53.3760	0.9982
Hand	52.1842	0.9987	51.2840	0.9994	57.3200	0.9997	51.0900	0.9989	57.2320	0.9992
Head	53.9669	0.9990	53.8890	0.9990	59.2610	0.9988	53.8530	0.9985	59.8250	0.9983
Leg	51.4348	0.9990	50.6110	0.9992	55.8280	0.9995	58.4660	0.9995	49.2040	0.9979

Table 3. PSNR (dB) and SSIM values of embedding 10 kb secret message

Image	Method in [28]		Proposed							
			H-PVO		V-PVO		R-PVO		L-PVO	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Abdominal	48.1542	0.9974	51.7980	0.9980	58.4020	0.9969	51.3800	0.9967	53.0570	0.9961
Chest	50.3226	0.9981	51.2460	0.9977	58.7630	0.9969	53.3610	0.9968	53.3760	0.9961
Hand	47.0188	0.9968	51.2840	0.9988	57.3200	0.9991	51.0900	0.9978	57.2320	0.9985
Head	50.0749	0.9975	53.8890	0.9980	59.2610	0.9969	53.8530	0.9967	59.8250	0.9965
Leg	48.8994	0.9970	50.6110	0.9981	55.8280	0.9988	58.4660	0.9989	49.2040	0.9958

Table 4. PSNR (dB) and SSIM values of embedding 20 kb secret message

Image	Method in [28]		Proposed							
			H-PVO		V-PVO		R-PVO		L-PVO	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Abdominal	45.8774	0.9940	47.9570	0.9945	55.2730	0.9931	48.1260	0.9927	48.9220	0.9915
Chest	49.1203	0.9941	49.3070	0.9942	55.3900	0.9931	51.8170	0.9930	49.3900	0.9919
Hand	45.3506	0.9947	48.3620	0.9974	54.0360	0.9980	49.0150	0.9960	54.6430	0.9972
Head	48.6546	0.9941	50.1810	0.9946	55.6700	0.9930	50.6010	0.9934	55.6660	0.9926
Leg	48.0024	0.9960	48.5530	0.9956	52.6400	0.9975	52.7860	0.9970	46.9050	0.9924

Table 5. Comparison of the maximum embedding capacity (bpp) between the proposed method and the state-of-the-art

Image	Method in [24]	Method in [28]	Proposed			
			H-PVO	V-PVO	R-PVO	L-PVO
Abdominal	0.742	0.832	0.955	0.953	0.957	0.959
Chest	0.737	0.842	0.985	0.984	0.988	0.991
Hand	0.750	0.881	1	1	1	1
Head	0.711	0.740	0.952	0.952	0.958	0.954
Leg	0.746	0.862	0.992	0.991	0.994	0.997

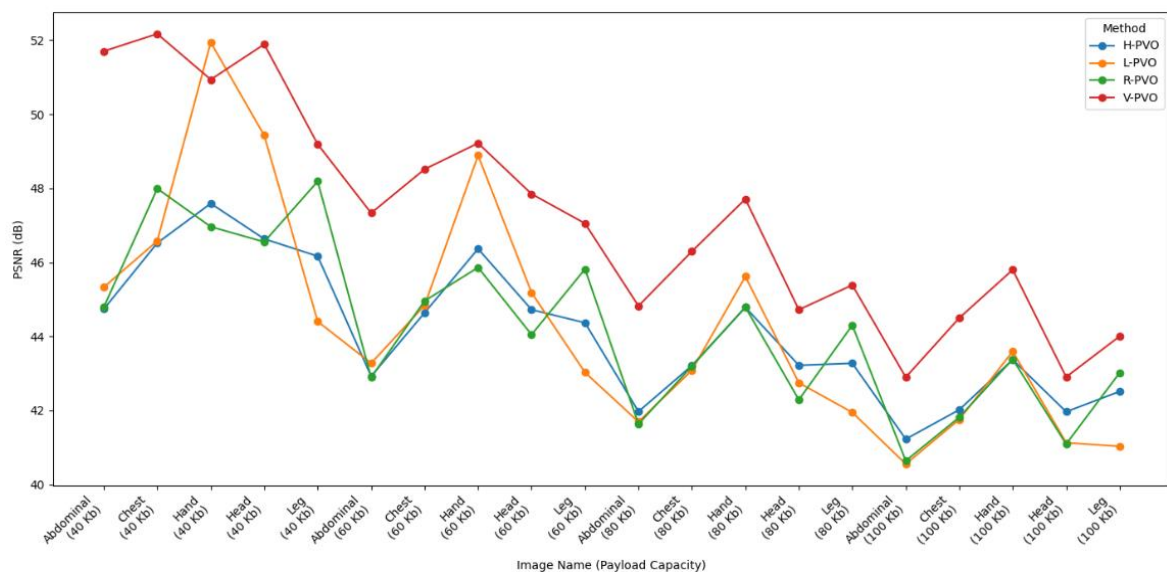


Figure 6. The obtained PSNR value (dB) for 40-100 kb secret message

Figure 7 illustrates the original image before hiding the secret data and the stego image obtained. We can see that the visual quality of the cover image can still be maintained. In addition, the original image and the stego image presented in Figures 7(a) to 7(d) where the two images are almost similar and comparatively difficult to identify the difference between the original image and the stego images.

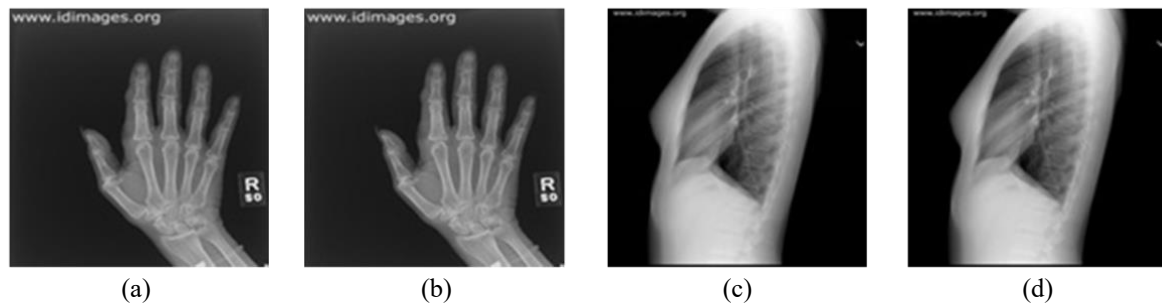


Figure 7. An example medical image (a) hand image before hiding data (b) hand image after hiding 100 kb, (c) chest image before hiding data, and (d) chest image after hiding 100 kb

## 5. CONCLUSION

This research introduces a novel RDH method that combines enhanced reversible difference expansion with adaptive predictive vector quantization (PVO) to significantly improve embedding capacity and image quality. Experimental results show an increase in embedding capacity from 0.8315 bpp to 0.9781 bpp and an improvement in average PSNR from 49.44 dB to 53.40 dB, SSIM remaining high at 0.997, indicating minimal perceptual distortion. The adaptive use of multiple directional PVO schemes proves effective in aligning pixel ordering with image structure, thereby reducing distortion and enhancing efficiency. These findings highlight the method's potential for high-fidelity, high-capacity steganography. Future work may explore dynamic pixel pair selection, multi-layer embedding, and applications in other media.

## ACKNOWLEDGMENTS

The authors thank the members of the Cyber Security Research Group, Net-Centric Computing Laboratory, Department of Informatics, Institut Teknologi Sepuluh Nopember, for the support and discussion.

## FUNDING INFORMATION

This research was funded by the Institut Teknologi Sepuluh Nopember for this work, under project scheme of the Publication Writing and IPR Incentive Program (PPHKI) 2025.

## AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
I Kadek Agus Ariesta Putra	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓
Ntivuguruzwa Jean De La Croix	✓	✓		✓	✓	✓	✓		✓	✓				
Tohari Ahmad	✓	✓			✓		✓			✓		✓	✓	✓

C : **C**onceptualization

M : **M**ethodology

So : **S**oftware

Va : **V**alidation

Fo : **F**ormal analysis

I : **I**nterpretation

R : **R**esources

D : **D**ata Curation

O : **O**riginal Draft

E : **E**diting

Vi : **V**isualization

Su : **S**upervision

P : **P**roject administration

Fu : **F**unding acquisition

## CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

## DATA AVAILABILITY

The payload data that support the findings of this study are available from the corresponding author, [TA], upon reasonable request.




## REFERENCES

- [1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, no. 3–4, pp. 313–335, 1996, doi: 10.1147/sj.353.0313.
- [2] S. Gandhi and R. Kumar, "Survey of reversible data hiding: statistics, current trends, and future outlook," *Computer Standards and Interfaces*, vol. 94, 2025, doi: 10.1016/j.csi.2025.104003.
- [3] J. Tan, X. Liao, J. Liu, Y. Cao, and H. Jiang, "Channel attention image steganography with generative adversarial networks," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 2, pp. 888–903, 2022, doi: 10.1109/TNSE.2021.3139671.
- [4] Y. Luo, J. Qin, X. Xiang, and Y. Tan, "Coverless image steganography based on multi-object recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 7, pp. 2779–2791, 2021, doi: 10.1109/TCSVT.2020.3033945.
- [5] X. Liao, J. Yin, M. Chen, and Z. Qin, "Adaptive payload distribution in multiple images steganography based on image texture features," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 897–911, 2022, doi: 10.1109/TDSC.2020.3004708.
- [6] M. M. Mahmoud and H. T. Elshoush, "Enhancing LSB using binary message size encoding for high capacity, transparent and secure audio steganography—an innovative approach," *IEEE Access*, vol. 10, pp. 29954–29971, 2022, doi: 10.1109/ACCESS.2022.3155146.
- [7] H. T. Elshoush and M. M. Mahmoud, "Ameliorating LSB using piecewise linear chaotic map and one-time pad for superlative capacity, imperceptibility and secure audio steganography," *IEEE Access*, vol. 11, pp. 33354–33380, 2023, doi: 10.1109/ACCESS.2023.3259902.
- [8] J. Wu, B. Chen, W. Luo, and Y. Fang, "Audio steganography based on iterative adversarial attacks against convolutional neural networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2282–2294, 2020, doi: 10.1109/TIFS.2019.2963764.
- [9] R. J. Mstafa, Y. M. Younis, H. I. Hussein, and M. Atto, "A new video steganography scheme based on Shi-Tomasi corner detector," *IEEE Access*, vol. 8, pp. 161825–161837, 2020, doi: 10.1109/ACCESS.2020.3021356.
- [10] S. He, D. Xu, L. Yang, and W. Liang, "Adaptive HEVC video steganography with high performance based on attention-Net and PU partition modes," *IEEE Transactions on Multimedia*, vol. 26, pp. 687–700, 2024, doi: 10.1109/TMM.2023.3269663.
- [11] S. Banerjee and G. K. Singh, "A new approach of ECG steganography and prediction using deep learning," *Biomedical Signal Processing and Control*, vol. 64, 2021, doi: 10.1016/j.bspc.2020.102151.
- [12] H. A. Rehman, U. I. Bajwa, R. H. Raza, S. Alfahhood, M. Safran, and F. Zhang, "Leveraging coverless image steganography to hide secret information by generating anime characters using GAN," *Expert Systems with Applications*, vol. 248, 2024, doi: 10.1016/j.eswa.2024.123420.
- [13] R. Singh, L. I. Izhar, I. Elamvazuthi, A. Ashok, S. Aole, and N. Sharma, "Efficient watermarking method based on maximum entropy blocks selection in frequency domain for color images," *IEEE Access*, vol. 10, pp. 52712–52723, 2022, doi: 10.1109/ACCESS.2022.3174964.
- [14] N. Mir and M. A. U. Khan, "Copyright protection for online text information: using watermarking and cryptography," in *2020 3rd International Conference on Computer Applications and Information Security (ICCAIS)*, 2020, pp. 1–4, doi: 10.1109/ICCAIS48893.2020.9096817.
- [15] S. Kumar, A. Gupta, and G. S. Walia, "Reversible data hiding: a contemporary survey of state-of-the-art, opportunities and challenges," *Applied Intelligence*, vol. 52, no. 7, pp. 7373–7406, 2022, doi: 10.1007/s10489-021-02789-2.
- [16] F. Kabir, T. K. Araghi, and D. Megías, "Privacy-preserving protocol for high-frequency smart meters using reversible watermarking and Paillier encryption," *Computers and Electrical Engineering*, vol. 119, 2024, doi: 10.1016/j.compeleceng.2024.109497.
- [17] L. Han, W. Gao, X. Zhang, and S. Tao, "Reversible data hiding with automatic contrast enhancement and high embedding capacity based on multi-type histogram modification," *Journal of Visual Communication and Image Representation*, vol. 109, 2025, doi: 10.1016/j.jvcir.2025.104450.
- [18] T. S. Nguyen, V. T. Huynh, and P. H. Vo, "A novel reversible data hiding algorithm based on enhanced reduced difference expansion," *Symmetry*, vol. 14, no. 8, 2022, doi: 10.3390/sym14081726.
- [19] G. S. Septinaputri, A. W. C. D'Layla, N. J. D. La Croix, and T. Ahmad, "Enhanced spatial domain image steganography for improved IoT security and privacy applications," in *2024 IEEE 21st International Conference on Mobile Ad-Hoc and Smart Systems (MASS)*, 2024, pp. 635–640, doi: 10.1109/MASS62177.2024.00101.
- [20] G. Kaur, S. Singh, R. Rani, R. Kumar, and A. Malik, "High-quality reversible data hiding scheme using sorting and enhanced pairwise PEE," *IET Image Processing*, vol. 16, no. 4, pp. 1096–1110, 2022, doi: 10.1049/ipr2.12212.
- [21] C. F. Lee, J. J. Shen, Y. J. Wu, and S. Agrawal, "PVO-based reversible data hiding exploiting two-layer embedding for enhancing image fidelity," *Symmetry*, vol. 12, no. 7, 2020, doi: 10.3390/sym12071164.
- [22] I. F. Ramadhan, N. J. D. La Croix, T. Ahmad, and A. Uzamurenga, "Huffman coding-based data reduction and quadristego logic for secure image steganography," *Engineering Science and Technology, an International Journal*, vol. 65, 2025, doi: 10.1016/j.jestch.2025.102033.
- [23] L. Qu, X. Wang, Y. Yuan, J. Zhou, and Y. Xin, "Reversible data hiding in redundancy-free cipher images through pixel rotation and multi-MSB replacement," *Journal of Information Security and Applications*, vol. 89, 2025, doi: 10.1016/j.jisa.2025.104003.
- [24] Z. Syahlan and T. Ahmad, "Reversible data hiding method by extending reduced difference expansion," *International Journal of Advances in Intelligent Informatics*, vol. 5, no. 2, pp. 101–112, 2019, doi: 10.26555/ijain.v5i2.351.
- [25] F. Ren, Y.-P. Yang, and Z.-L. Zhang, "Dynamic hybrid reversible data hiding based on pixel-value-ordering," *Journal of Computers*, vol. 34, no. 6, pp. 15–29, 2023, doi: 10.53106/199115992023123406002.
- [26] H. X. Chi, J. H. Horng, and C. C. Chang, "Reversible data hiding based on pixel-value-ordering and prediction-error triplet expansion," *Mathematics*, vol. 9, no. 14, 2021, doi: 10.3390/math9141703.



- [27] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003, doi: 10.1109/TCSVT.2003.815962.
- [28] A. Arham and H. A. Nugroho, "Block-based optimization for enhancing reversible watermarking using reduced difference expansion," *Communications in Science and Technology*, vol. 9, no. 1, pp. 57–64, 2024, doi: 10.21924/cst.9.1.2024.1368.
- [29] T. Li, H. Li, L. Hu, and H. Li, "A reversible steganography method with statistical features maintained based on the difference value," *IEEE Access*, vol. 8, pp. 12845–12855, 2020, doi: 10.1109/ACCESS.2020.2964830.
- [30] A. Vishwakarma and M. P. Parsai, "Image steganography using improved exploiting modification direction," in *2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2022, pp. 306–311, doi: 10.1109/Confluence52989.2022.9734163.
- [31] Mass General Brigham, "Infectious disease images," *eMicrobes Digital Library*. 2023. Accessed: May 25, 2024. [Online]. Available: <https://www.idimages.org/images/>

## BIOGRAPHIES OF AUTHORS






**I Kadek Agus Ariesta Putra**    received the bachelor's degree in informatics engineering from Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia, in 2023. He is currently pursuing the Master of Informatics Engineering degree with the Institut Teknologi Sepuluh Nopember (ITS), Indonesia. Since September 2023, he has been a Research Assistant with the Net-Centric Computing Laboratory. His research interests include steganography, digital forensics, natural language processing, and deep learning. He can be contacted at email: 6025231078@student.its.ac.id.



**Ntivuguruzwa Jean De La Croix**    received a B.Sc. degree in computer science and systems from the National University of Rwanda, Rwanda, a master's degree in information technology from the University of Madras, India, a master's degree in internet of things-embedded computing systems from the University of Rwanda (UR). He is pursuing a Ph.D. in computer science at Institut Teknologi Sepuluh Nopember (ITS), Indonesia. He is a reviewer of several journals, including IEEE Access. His current research interests include steganography, steganalysis, and deep learning for data security in the public network. He can be contacted at email: 7025221024@student.its.ac.id.



**Tohari Ahmad**    received a bachelor's degree in computer science from the Institut Teknologi Sepuluh Nopember (ITS), Indonesia, a master's degree in information technology from Monash University, Australia, and a Ph.D. degree in computer science from RMIT University, Australia, in 2012. From 2001 to 2003, he was a consultant for some international companies. In 2003, he moved to ITS, where he is currently a professor. His research interests include network security, information security, data hiding, and computer networks. He currently in the top 2% world's scientists, is a member of ACM, IEEE. His awards and honors include the Hitachi Research Fellowship and JICA Research Program for conducting research in Japan. He is a reviewer of a number of journals. He can be contacted at email: tohari@its.ac.id or tohari@if.its.ac.id.