

Article

A New Dual Image Based Reversible Data Hiding Method Using Most Significant Bits and Center Shifting Technique

Serdar Solak *  and Gökhan Tezcan

Department of Information Systems Engineering, Kocaeli University, 41001 Kocaeli, Turkey

* Correspondence: serdars@kocaeli.edu.tr

Abstract: In this article, a new reversible data hiding method using most significant bits and center shifting technique in dual images is proposed. The proposed reversible data hiding method aims to securely hide high-capacity secret data. Instead of directly embedding the secret data, the method calculates new values with $(n + 1)$ bits secret data and the n most significant bits of the cover image pixel values. Thus, it is impossible to extract secret data without obtaining the original cover image. Also, the center shifting process is performed to minimize the mean square error. After this process, the secret data to be hidden in the dual images are in the range $[-3 \times 2^{(n-1)} + 1, 3 \times 2^{(n-1)} - 1]$. The pixel values of stego images are obtained by using the secret data in this range value and cover image pixel values. As a result of experimental studies, when the payload is 2.5 bits per pixel (bpp), the peak signal-to-noise ratio value (PSNR), which expresses the visual quality, is above 34 (dB). In addition, the proposed method has proven secure against RS (regular and singular) analysis attacks.

Keywords: data security; reversible data hiding; dual-image steganography; center folding strategy; center shifting strategy; most significant bits



Citation: Solak, S.; Tezcan, G. A New Dual Image Based Reversible Data Hiding Method Using Most Significant Bits and Center Shifting Technique. *Appl. Sci.* **2022**, *12*, 10933. <https://doi.org/10.3390/app122110933>

Received: 30 September 2022

Accepted: 25 October 2022

Published: 28 October 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

People generally exchange information on the internet using a computer and smart phone, since it provides easy and rapid communication in recent years. Malicious people may monitor illegally, steal, and disrupt this information during the transmission, thus it is an important topic to preserve data security and integrity. We utilize common cryptography [1] and steganography [2] techniques to provide the data security and integrity. While the cryptography encrypts the secret data in such a way that it has puzzling data to third parties, the steganography hides secret data unobtrusively in various files such as text, audio, image and video. In data hiding studies, selecting image files to embed data is known as image steganography. Image Steganography consists of the cover image, secret data, data embedding algorithm and the stego image [3–5]. The cover image indicates the carrier media used to hide secret data, while the stego image represents the result media containing the secret data and cover image [4]. In the algorithm studies of image steganography, it is expected that the cover and stego images are highly similar and the high embedding capacity [6,7]. Most studies in literature have focused only on retrieving secret data, not dealing with restoring the original image [8]. Steganography techniques involving such literature studies are called irreversible data hiding. In the techniques used in some literature studies, both the secret data and the original image must be recovered, which are called reversible data hiding (RDH) [9,10]. RDH methods have been popular in recent years for many reasons, such as security, capacity, and reversibility [11–13]. The most widely used RDH techniques are the difference expansion [14–16], histogram shifting [17–20], pixel value order [21], interpolation [22–29], and dual image [30–38] based methods.

The difference expansion method, known as the expansion of the difference between two non-overlapping pixels to hide a bit, was proposed by Tian in 2003 [14]. The payload (0.5 bpp) and visual quality of the stego image are low in this method and have the fall of

boundary problem. Due to its low computational complexity, it can be preferred reversible methods to hide a small amount of data. There are many studies in the literature to increase the visual quality and payload in the method. Li et al. (2011) offered an adaptive data concealing method that separates pixel complexities into rough and flat parts. In addition, this study decided on the embedded pixel estimation error and the amount of embedded secret data according to diverse classification results [15]. Gui et al. (2014) developed the method of Li et al. (2011) by increasing the types of complexity to increase the embedding capacity of the prediction error [16].

The histogram shifting algorithm utilizes statistical techniques to create the histogram of pixel values or differences and embed the secret data at the highest value. Ni et al. (2006) concealed the secret data into the most frequently repeated pixels using the histogram shifting technique [17]. Tsai et al. (2009) suggested a histogram-based approach. To improve data embedding capacity, secret data are hidden in the residual images after linear prediction and used the pairs of peaks and zero points for extra capacity [18]. In the method proposed by Zhao et al. (2011), firstly, they created positive and negative difference histograms by using pixel differences with a linear estimation method. Then, the blank columns are obtained because of the shifting process on these histograms. And finally, they have implemented data hiding by distributing a zero-center range to these blank columns [19]. Wang et al. (2013) developed a new approach that produces two differences per pixel, first creating a two-dimensional histogram based on the differences and then reducing this histogram to several single dimensions for data hiding, aiming to achieve high embedding capacity [20].

Li et al. (2013) proposed a pixel value order-based data hiding method [21]. Their method's aim is to reduce the number of shifted pixels and achieve high image quality. In the method, firstly, 2×2 blocks are taken from the cover image and the pixel values are ordered in descending. If the two largest values are equal to one, one bit data hiding is performed. If it is greater than one, the difference is increased by one. During data extraction, the difference of one or two indicates that it is hidden data, zero and one, respectively. During the recovery of the cover image, differences greater than one are reduced by one.

In interpolation-based methods, new expendable pixels are created by enlarging the size of the cover image. The embedding capacity is increased by the expansion process. Later, without changing the original pixel values, these expendable pixel values are changed and embedded secret data. Since the original pixel values are preserved, the cover image can be easily restored by combining the pixels in the correct positions. In addition, the initial values of intermediate pixels produced by interpolation can be recalculated over the original pixel values. Thanks to this process, the need to associate pixel values with each other in data hiding is eliminated [22–29].

In addition to these methods, dual image based reversible data hiding techniques are also widely used in the literature in recent years. These techniques create two identical duplicate images from a cover image to increase the overall embedding capacity while hiding secret data. Also, a dual image-based data hiding scheme can ensure higher data embedding capacity, more secure communication, and high visual quality. Because without obtaining two stego images at the same time, it is impossible for third parties to receive all secret messages. Chang et al. (2007 and 2013) combined EMD method with dual image based reversible data hiding technique. Their technique uses a 256×256 function matrix. It converts bit streams data in the 5-ary notational system data streams ranging from zero to four. Two 5-ary notational system data are embedded into one cover image pixel pair at a time [30,31]. Lee et al. (2009) developed a dual image based reversible method using a four-way cross pattern. Firstly, the two bits of the four-bit secret data are used to determine the starting position of the pattern, and the other two bits to determine the direction of movement of the pattern. Then, it applies changes to the selected pixels in the pattern to calculate stego pixels [32]. Lu et al. (2015) proposed a new dual image-based data hiding approach using the center folding strategy. Their method firstly decreased the secret data

values via a folding strategy technique to obtain high image quality, and then hidden the folded secret data with an averaging method in two stego image pixels [33]. Chi et al. (2018) proposed a new dual image based reversible data hiding method involving the center folding strategy. The method uses a dynamic coding strategy, which utilizes joint neighbor coding, to develop the center folding strategy [34]. Shastri et al. (2019) developed a dual image based reversible data hiding scheme using the center folding strategy and the slidable pixel coordinate choosing technique [35]. Meikap et al. (2021) developed a center folding based data hiding scheme through the directional pixel value of orders with different block size [36]. Lu et al. (2021) proposed a reversible data hiding scheme for interpolation images featuring a multilayer center folding strategy [37].

Most dual image-based methods convert secret data from the binary system to decimal or other numeric bases to hide the secret data and add or subtract them to obtain stego pixel values. If the secret data value is too large, the difference between the values of stego image and cover image pixels is also high. Therefore, it is obtained low image quality, and it can be understood by third parties that there is secret data in the stego image. We propose a new dual image based reversible data hiding method using most significant bits and center shifting techniques to avoid this problem in this paper. The temporary values are obtained by calculating the difference between the most significant bit values of the relevant pixels and the numerical values of the secret data to reduce the numerical values of the secret data. The most significant bits are shifted by the average value of the change interval to minimize the effect of this operation on the character change interval. Thus, the mean square error values are minimized in theory. The contributions of the proposed data hiding method are listed:

- This paper proposes a new reversible data hiding method based on dual images and center shifting technique for image steganography. In the proposed technique, data hiding and extracting processes can be performed completely lossless.
- The proposed technique ensures a resolution for the fall of the boundary problem.
- Even if the two stego images are obtained from third parties, the secret data cannot be obtained unless the original cover image can be created.
- The reversible data hiding algorithm is a higher payload than the similar existing algorithms.
- The proposed technique is resistant to the RS analysis technique according to the experimental results.

The remainder of our article is organized as follows. In Section 2, related works are presented in detail, which contains the dual image based reversible data hiding technique and center folding strategy algorithm. The proposed method, dual image and center shifting technique for image steganography, is represented in Section 3. The experimental results and comparisons to evaluate the proposed algorithm is given in Section 4. Finally, the conclusion is presented in Section 5.

2. Related Works

2.1. Location Based Dual Image Reversible Data Hiding Technique

Location based dual image reversible data hiding technique was proposed by Lee et al. [32]. In the method, the cover image pixel pairs are taken as a set of coordinates on the X and Y axes, respectively. This pixel pair accepts the center point of the cross pattern in Figure 1 as consecutive pixels ($X_{i,j}$, $X_{i,j+1}$). The pixel pairs on the four sides (top, bottom, left, and right) of the center pixel pair represent different combinations of secret data of two bits each (S_1 or S_2).

	$X_{i,j}, X_{i,j+1} + 1$ $S_1 = 10$	
$X_{i,j} - 1, X_{i,j+1}$ $S_1 = 11$	$X_{i,j}, X_{i,j+1}$	$X_{i,j} + 1, X_{i,j+1}$ $S_1 = 00$
	$X_{i,j}, X_{i,j+1} - 1$ $S_1 = 01$	

Figure 1. The cross pattern of indicating the pixel pair sets.

The pattern in Figure 1 is expressed using Equation (1). Pixel value changes that will create the first stego image are realized by using Equation (1).

$$(X'_{i,j}, X'_{i,j+1}) = \begin{cases} (X_{i,j} + 1, X_{i,j+1}) & \text{if } S_1 = 00 \\ (X_{i,j}, X_{i,j+1} - 1) & \text{if } S_1 = 01 \\ (X_{i,j}, X_{i,j+1} + 1) & \text{if } S_1 = 10 \\ (X_{i,j} - 1, X_{i,j+1}) & \text{if } S_1 = 11 \end{cases} \quad (1)$$

According to the S_2 secret data, the expression in Equation (1) is applied as in Equation (2) to the second stego image.

$$(X''_{i,j}, X''_{i,j+1}) = \begin{cases} (X_{i,j} + 1, X_{i,j+1}) & \text{if } S_2 = 00 \\ (X_{i,j}, X_{i,j+1} - 1) & \text{if } S_2 = 01 \\ (X_{i,j}, X_{i,j+1} + 1) & \text{if } S_2 = 10 \\ (X_{i,j} - 1, X_{i,j+1}) & \text{if } S_2 = 11 \end{cases} \quad (2)$$

In the data hiding process, for example, $X_{1,1} = 45$, $X_{1,2} = 46$ and secret data = 0011. So, $S_1 = 00$ and $S_2 = 11$. Since $S_1 = 00$ according to Equation (1), the formula $(X'_{i,j}, X'_{i,j+1} = X_{i,j} + 1, X_{i,j+1})$ is applied. Accordingly, the first two pixels values of the first stego image will be $X'_{1,1} = 45 + 1 = 46$, and $X'_{1,2} = 46$, respectively. For $S_2 = 11$ according to Equation (2), the formula $(X''_{i,j}, X''_{i,j+1} = X_{i,j} - 1, X_{i,j+1})$ is applied. Accordingly, the first two pixels values of the second stego image will be $X''_{1,1} = 45 - 1 = 44$ and $X''_{1,2} = 46$, respectively.

In the data extraction process, first, the equality of the pixel groups in two stego images is examined. If the two consecutive pixel pairs are equal for two stego images $(X'_{i,j} = X''_{i,j} \text{ and } X'_{i,j+1} = X''_{i,j+1})$, it means that the secret data is not embedded there. To recover secret data, the difference between the pixel pairs values of two stego images is examined. It is observed that these differences are between the values of $[-2, 2]$. In this way, the data extraction process is performed by applying twelve different combinations. These combination states and the secret data that can be obtained are presented in Table 1.

Table 1. Combination states and secret data values for data extraction process.

Combination States	Secret Data
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} + 2, X''_{i,j+1})$	$S_1 = 00, S_2 = 11$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} - 2, X''_{i,j+1})$	$S_1 = 11, S_2 = 00$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j}, X''_{i,j+1} + 2)$	$S_1 = 10, S_2 = 01$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j}, X''_{i,j+1} - 2)$	$S_1 = 01, S_2 = 10$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} + 1, X''_{i,j+1} + 1)$	$S_1 = 00, S_2 = 01$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} + 1, X''_{i,j+1} - 1)$	$S_1 = 01, S_2 = 11$

Table 1. *Cont.*

Combination States	Secret Data
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} - 1, X''_{i,j+1} - 1)$	$S_1 = 11, S_2 = 01$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} - 1, X''_{i,j+1} + 1)$	$S_1 = 10, S_2 = 00$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} + 1, X''_{i,j+1})$	$S_1 = 00$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} - 1, X''_{i,j+1})$	$S_1 = 11$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j}, X''_{i,j+1} + 1)$	$S_1 = 10$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j}, X''_{i,j+1} - 1)$	$S_1 = 01$

To recover the cover image, twelve different combinations of pixel values in the two stego images are obtained as presented in Table 2.

Table 2. Combination states and cover image pixel values for the data extraction process.

Combination States	Cover Image Pixel Values
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} + 2, X''_{i,j+1})$	$(X_{i,j}, X_{i,j+1}) = \left(\frac{X'_{i,j} + X''_{i,j}}{2}, \frac{X'_{i,j+1} + X''_{i,j+1}}{2} \right)$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} - 2, X''_{i,j+1})$	$(X_{i,j}, X_{i,j+1}) = \left(\frac{X'_{i,j} + X''_{i,j}}{2}, \frac{X'_{i,j+1} + X''_{i,j+1}}{2} \right)$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j}, X''_{i,j+1} + 2)$	$(X_{i,j}, X_{i,j+1}) = \left(\frac{X'_{i,j} + X''_{i,j}}{2}, \frac{X'_{i,j+1} + X''_{i,j+1}}{2} \right)$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j}, X''_{i,j+1} - 2)$	$(X_{i,j}, X_{i,j+1}) = \left(\frac{X'_{i,j} + X''_{i,j}}{2}, \frac{X'_{i,j+1} + X''_{i,j+1}}{2} \right)$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} + 1, X''_{i,j+1} + 1)$	$(X_{i,j}, X_{i,j+1}) = (X''_{i,j}, X'_{i,j+1})$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} + 1, X''_{i,j+1} - 1)$	$(X_{i,j}, X_{i,j+1}) = (X'_{i,j}, X''_{i,j+1})$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} - 1, X''_{i,j+1} - 1)$	$(X_{i,j}, X_{i,j+1}) = (X''_{i,j}, X'_{i,j+1})$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} - 1, X''_{i,j+1} + 1)$	$(X_{i,j}, X_{i,j+1}) = (X'_{i,j}, X''_{i,j+1})$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} + 1, X''_{i,j+1})$	$(X_{i,j}, X_{i,j+1}) = (X''_{i,j}, X''_{i,j+1})$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} - 1, X''_{i,j+1})$	$(X_{i,j}, X_{i,j+1}) = (X''_{i,j}, X''_{i,j+1})$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j}, X''_{i,j+1} + 1)$	$(X_{i,j}, X_{i,j+1}) = (X''_{i,j}, X''_{i,j+1})$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j}, X''_{i,j+1} - 1)$	$(X_{i,j}, X_{i,j+1}) = (X''_{i,j}, X''_{i,j+1})$

2.2. Dual Image Based Reversible Data Hiding Using Center Folding Strategy

Dual image based reversible data hiding using center folding strategy was proposed by Lu et al. [33]. In the method, the number of k bits is determined during data hiding process. After the secret data is parsed into k -bit d packets, it is processed for each of these packets as presented in Equation (3).

$$d' = d - 2^{k-1} \quad (3)$$

Figure 2 shows an example of $k = 3$ for this transformation process at center folding strategy.

0	1	2	3	4	5	6	7
↓	↓	↓	↓	↓	↓	↓	↓
-4	-3	-2	-1	0	1	2	3

Figure 2. The example of $k = 3$.

Equation (4) is used to calculate the change in pixel values in the stego image during data hiding process. These values are used in obtaining the stego image pixel values by using the Equation (5).

$$d'_1 = \left\lfloor \frac{d'}{2} \right\rfloor \text{ and } d'_2 = \left\lceil \frac{d'}{2} \right\rceil \quad (4)$$

$$X'_{i,j} = X_{i,j} + d'_1 \text{ and } X''_{i,j} = X_{i,j} - d'_2 \quad (5)$$

To avoid the fall of the boundary problem (FOBP), the data hiding process is not performed in cases where the value d' is between $[-2^{(k-1)}, 2^{(k-1)} - 1]$. In briefly, the data hiding range in the method is $[2^{(k-1)}, 256 - (2^{(k-1)} - 1)]$.

In the data extraction process of the method, essentially, the difference between two stego image pixel values is calculated; the formula showing this process is presented in Equation (6).

$$d = [X'_{i,j} - X''_{i,j}] + 2^{(k-1)} \quad (6)$$

To recover the original cover image, the average of the two stego image pixel values must be computed and rounded up as shown in Equation (7).

$$X_{i,j} = \left\lceil \frac{X'_{i,j} + X''_{i,j}}{2} \right\rceil \quad (7)$$

In the data hiding process, for an example, the cover image pixel values are $X = \{45, 46\}$, $k = 3$, Secret data (S), $S = 001111$, $S_1 = 001$, $S_2 = 111$ (binary system), $S_1 = 1$, $S_2 = 7$ (decimal system), $d = \{1, 7\}$, we apply Equation (3), $d' = \{1, 7\} - 4 = \{-3, 3\}$, then, we use folding strategy in Equation (4), $d'_1 = \{-2, 1\}$, and $d'_2 = \{-1, 2\}$, finally we apply Equation (5), $X'_{i,j} = X' = X + d'_1 = \{45, 46\} + \{-2, 1\} = \{43, 47\}$, $X'' = X - d'_2 = \{45, 46\} - \{-1, +2\} = \{46, 44\}$.

In the data extraction process, for an example, $X' = \{43, 47\}$ and $X'' = \{46, 44\}$, $X' - X'' + 2^{(k-1)} = \{43, 47\} - \{46, 44\} + 4 = \{-3, 3\} + 4 = \{1, 7\}$, $S_1 = 1$, $S_2 = 7$, Secret data (S) = 001111. To recover the original cover image, $X = \lceil (X' + X'')/2 \rceil = \lceil (\{43, 47\} + \{46, 44\})/2 \rceil = \lceil \{89, 91\}/2 \rceil$, $X = \lceil \{89, 91\}/2 \rceil = \{45, 46\}$.

3. Proposed Method

In this section, a new dual image based reversible data hiding method using most significant bits and the center shifting technique is proposed. During the data hiding process, the proposed method securely hides data by generating two different stego images from a single cover image. During the data extraction process, the secret data and the original cover image are obtained from these two stego images with lossless.

The flowchart of data hiding process is presented in Figure 3. In the first step of data hiding process, the number n , which represents how many of the most significant bits of the pixel value will be used, is determined. The size of secret data or the maximum acceptable rates of distortion are decisive factors in choosing the n number. In the second step, the secret data is converted into a $(n + 1)$ bit binary series, and each element of the series is converted to a decimal system to obtain the s series, which represents the symbols to be hidden. Briefly, $(n + 1)$ bit hiding is performed for the selected value of n . Therefore, $(n + 1)/2$ bits of secret data per pixel (bpp) in the original cover image is hidden. In this way, the payload is always greater than 1 (bpp). For the determined number of n , the initial

series is created by using the most significant n bits of the pixel values, and the range of this series is between $[0, 2^n - 1]$. Equation (8) presents the formula used to calculate this initial series.

$$d = \left\lfloor \frac{X_{i,j}}{2^{8-n}} \right\rfloor \quad (8)$$

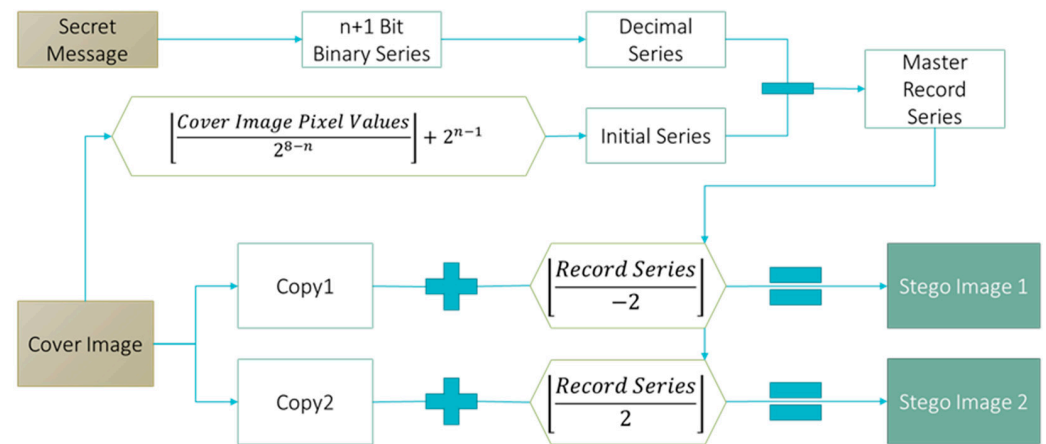


Figure 3. Data hiding process.

The difference between the initial series values and the secret data is calculated to aim to reduce the average of the secret data to be embedded in the stego image. This operation causes the range of $[0, 2^{n+1} - 1]$ coming from secret data to expand and take values in the range of $[-2^n + 1, 2^{n+1} - 1]$. Equation (9) shows the computation of these secret data.

$$d' = s_i - d_i \quad (9)$$

This difference needs to be shifted in the opposite direction by half the interval of the initial series to minimize mean square error. To achieve this, Equation (10) is used, and the master record series is obtained, which will be hidden in the cover images. Subtracting the value 2^{n-1} from the obtained hidden symbols series, the interval of change $[-2^n - 2^{(n-1)} + 1, 2^{(n+1)} - 2^{(n-1)} - 1]$. This range expression, when simplified, becomes $[-3 \times 2^{(n-1)} + 1, 3 \times 2^{(n-1)} - 1]$.

$$d'' = d' - 2^{(n-1)} \quad (10)$$

The change of the first and second stego images are obtained by dividing the master record series into 2 and -2 , respectively. These changes are achieved using Equation (11).

$$d_1 = \left\lfloor \frac{d''}{2} \right\rfloor, d_2 = \left\lfloor \frac{d''}{-2} \right\rfloor \quad (11)$$

By adding these differences to the cover image as in Equation (12), two stego images are obtained and the data hiding process is completed.

$$X' = X + d_1 \text{ and } X'' = X + d_2 \quad (12)$$

During data hiding process, the change range is also divided into two, as the master record series is divided into two. Therefore, the range of change from $[-3 \times 2^{(n-1)} + 1, 3 \times 2^{(n-1)} - 1]$ to $[-3 \times 2^{(n-2)} + 1/2, 3 \times 2^{(n-2)} - 1/2]$. By rounding down the obtained stego pixel values, the change intervals are obtained as $[-3 \times 2^{(n-2)}, 3 \times 2^{(n-2)} - 1]$. To avoid FOBP, the data hiding process is performed only

for pixels in the range of $\left[3 \times 2^{(n-2)}, 256 - 3 \times 2^{(n-2)}\right]$. Figure 4 shows how the change difference ranges with the changes made in the secret data for $n = 4$.

Recording Differences		Secret Data	
		0	31
Initial Values	0	0	31
	15	-15	16

Shifting -8		Secret Data	
		0	31
Initial Values	0	-8	23
	15	-23	8

Stego 1 Difference Range		Secret Data	
		0	31
Initial Values	0	-4	11
	15	-12	4

Stego 2 Difference Range		Secret Data	
		0	31
Initial Values	0	4	-12
	15	11	-4

Figure 4. The state of change interval for $n = 4$.

During the data extraction process, if any of the pixel values in the same position of the two stego images are within this range and are not equal, it means that secret data is hidden there. (Due to FOBP, the secret data is not embedded for all cover image pixels.) If these two values are equal and boundary of the range $\left[3 \times 2^{(n-2)}, 256 - 3 \times 2^{(n-2)}\right]$, it means that the secret data in these pixels in the recording series is zero. If the pixel values in two stego images are outside this interval and are equal, it is understood that no secret data is hidden there. The flow chart of the data extraction process is given in Figure 5.

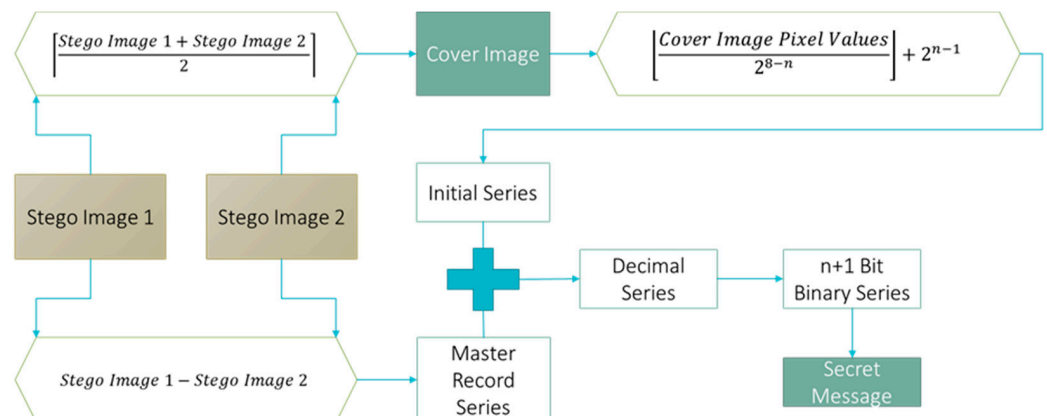


Figure 5. The flow chart of the data extraction process.

In the data extraction process, the initial series cannot be directly acquired as the pixel values of two stego images change. For this reason, the original cover image must first be

obtained in the data extraction process. In other words, it is impossible to extract the secret data intact without the recovery of the original cover image.

$$X_{i,j} = \left\lceil \frac{X'_{i,j} + X''_{i,j}}{2} \right\rceil \quad (13)$$

To recover the original cover image, the two stego images are averaged and rounded up, as in Equation (13). The main reason for rounding up is to neutralize the rounding down process performed during data hiding.

After the original cover image has been recovered, the initial series can be obtained using Equation (7). The extraction of the master record series is accomplished by subtracting the first stego image from the second stego image as shown in Equation (14).

$$d'' = X'_{i,j} - X''_{i,j} \quad (14)$$

Finally, the initial series and shift amount are added to the master record series and the secret data symbols expressed as s are obtained using Equation (15).

$$s = d + d'' + 2^{n-1} \quad (15)$$

For an example, the pixel values of the cover image are $X_{10} = \{164, 63, 120, 135\}$. When we consider the value of $n = 3$, we can embed $k = n + 1 = 4$ for each pixel. The sum of that makes 16 bits secret data for 4 pixels. When we assume the secret data as $S_{10} = \{232, 34\}$ and get the binary system of it, we get $S_2 = \{11101000, 00100010\}$. If this expression is converted to $k = 4$ -bit data, $S_2 = \{1110, 1000, 0010, 0010\}$ data are obtained. These data are equal to $s = \{14, 8, 2, 2\}$ in decimal system. At the next step, we need to compute initial series by Equation (8). Then, we find the initial series as $d = \{5, 1, 3, 4\}$. When we add secret data to initial series by Equation (9), we get $d' = \{9, 7, -1, -2\}$. In the next step, the shifting operation is performed in an amount of 2^{n-1} by Equation (10), and $d'' = \{5, 3, -5, -6\}$ series is obtained. Using Equation (11), it is calculated as $d_1 = \{2, 1, -3, -3\}$ and $d_2 = \{-3, -2, 2, 3\}$. These two series are added to the cover image pixel values according to Equation (12), $X' = \{166, 64, 117, 132\}$ and $X'' = \{161, 61, 122, 138\}$ stego images pixel values are obtained.

For extraction of secret data, we need to first calculate to original cover image pixel values by Equation (13). After computing Equation (13), we get $X = \{164, 63, 120, 135\}$. In the second step, we must get difference of these two stego image pixel values by Equation (14). So, we obtain $d'' = \{5, 3, -5, -6\}$. Then the initial series is computing as $d = \{5, 1, 3, 4\}$ by using Equation (8), by the same method with the data hiding process. For the last step, the secret data $s = \{14, 8, 2, 2\}$ are found by Equation (15). And these secret data are converted to binary series as $S_2 = \{1110, 1000, 0010, 0010\}$ to obtain a binary system of secret data. Then, secret data ($S_{10} = \{232, 34\}$) are obtained by converting them from a binary to a decimal system.

4. Experimental Studies

This section presents comparisons and experimental results of our proposed method. The proposed algorithm is tested on a series of standard colored and grayscale cover images to evaluate by the data hiding measurement metrics such as embedding capacity (EC), payload (P), and peak signal-to-noise ratio (PSNR). The article also presents histogram analysis, Regular Singular (RS) analysis and pixel distributions for the security tests of the proposed method. We tested our proposed method with many images in the USC-SIPI dataset [39] that is a collection of digitized images. This dataset is utilized to support research in image processing, image analysis, and image steganography. Figure 6 presents four 512×512 grayscale original cover images, which are utilized to embed secret data with diverse data hiding capacity in the experimental studies. Also, the secret data, by the computer randomly generates, are embedded into these original cover images in the

experiments. In addition, experimental studies have been carried out on the same color cover images of 512×512 sizes to demonstrate the validity of the algorithm.

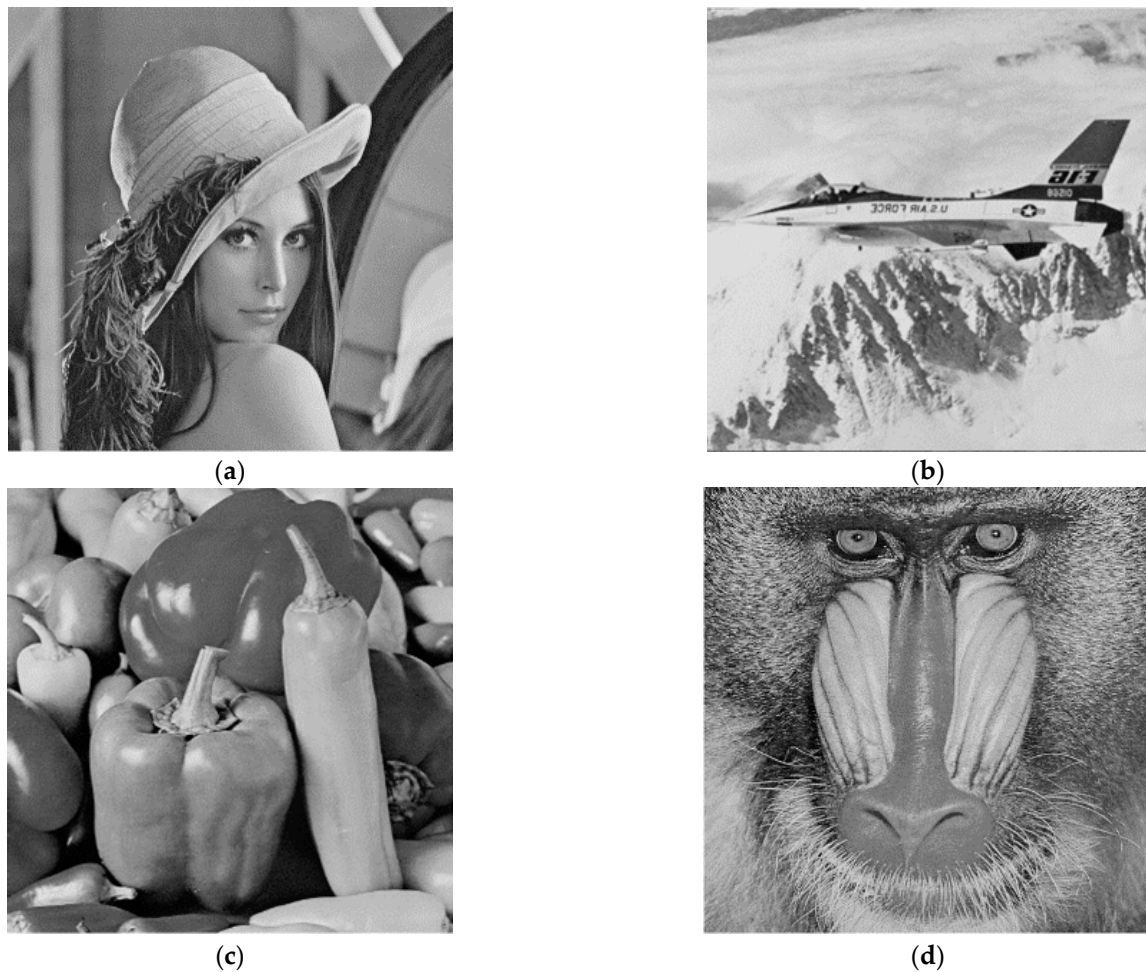


Figure 6. The flow chart of the data extraction process. (a) Lena; (b) Airplane; (c) Peppers; (d) Baboon.

The PSNR value is utilized to measure the similarity between the original cover image and the stego image. The higher this value, the better the stego image quality. Formulas showing the calculation of the mean square error (MSE), which is between the original cover image and the stego image, and PSNR values are calculated in (16) and (17), respectively. The H and W values represent the size of the cover image in (16).

$$\text{MSE} = \frac{1}{H \times W} \sum_{i=1}^H \sum_{j=1}^W (C(i,j) - S(i,j))^2 \quad (16)$$

$$\text{PSNR} = 10 \times \log_{10} \frac{255^2}{\text{MSE}} \quad (17)$$

The embedding capacity (EC) is expressed as the total secret data bits that are embedded into two stego images, while the payload (P) value in (18) represents that hidden secret data bits per pixel.

$$P = \frac{\text{EC}}{2 \times H \times W} \quad (18)$$

Table 3 presents a comparison of embedding capacity and PSNR value of different stego images for $n = 1$. As can be seen from experimental studies, when 100% secret data is in hidden on different cover images, the PSNR values of stego image 1 and stego image

2 are around 51.15 (dB). Tables 4–7 show the relationship between payload, embedding capacity and PSNR values for $n = 1$ –5, respectively. When these tables are examined, in the proposed method, PSNR values are obtained above 46 (dB) to 28.5 (dB) for payload values between 1.5 (bpp) and 3 (bpp), respectively.

Table 3. Comparison of embedding capacity and PSNR value of different stego images for $n = 1$.

EC (Ratio)	Lena				Baboon				Airplane				Peppers			
	EC (bits)	PSNR			EC (bits)	PSNR			EC (bits)	PSNR			EC (bits)	PSNR		
		Psnr1	Psnr2	Avg		Psnr1	Psnr2	Avg		Psnr1	Psnr2	Avg		Psnr1	Psnr2	Avg
10%	52,480	61.13	61.17	61.15	52,256	61.15	61.20	61.18	52,264	61.21	61.19	61.20	52,264	61.14	61.13	61.14
20%	104,912	58.11	58.11	58.11	104,680	58.16	58.14	58.15	104,704	58.12	58.12	58.12	104,696	58.13	58.11	58.12
30%	157,344	56.36	56.38	56.37	157,104	56.37	56.38	56.38	157,136	56.37	56.38	56.38	157,120	56.39	56.40	56.40
40%	209,768	55.16	55.08	55.12	209,520	55.13	55.13	55.13	209,560	55.12	55.14	55.13	209,552	55.12	55.13	55.13
50%	262,200	54.14	54.17	54.16	261,944	54.13	54.14	54.14	261,992	54.17	54.16	54.17	261,976	54.15	54.16	54.16
60%	314,632	53.38	53.37	53.38	314,360	53.38	53.37	53.38	314,416	53.35	53.38	53.37	314,400	53.36	53.38	53.37
70%	367,056	52.68	52.69	52.69	366,776	52.70	52.70	52.70	366,848	52.69	52.70	52.70	366,824	52.69	52.68	52.69
80%	419,488	52.10	52.12	52.11	419,200	52.11	52.09	52.10	419,280	52.11	52.11	52.11	419,256	52.12	52.12	52.12
90%	471,912	51.58	51.60	51.59	471,616	51.60	51.59	51.60	471,704	51.60	51.60	51.60	471,680	51.61	51.60	51.61
100%	524,288	51.14	51.14	51.14	524,190	51.14	51.13	51.14	524,288	51.13	51.13	51.13	524,104	51.15	51.14	51.15

Table 4. Comparison of embedding capacity and PSNR value of different stego images for $n = 2$.

EC (Ratio)	Lena				Baboon				Airplane				Peppers			
	EC (bits)	PSNR			EC (bits)	PSNR			EC (bits)	PSNR			EC (bits)	PSNR		
		Psnr1	Psnr2	Avg		Psnr1	Psnr2	Avg		Psnr1	Psnr2	Avg		Psnr1	Psnr2	Avg
10%	78,354	56.36	56.12	56.24	78,330	56.29	56.21	56.25	78,354	54.79	56.29	55.54	78,345	56.13	55.60	55.87
20%	157,002	53.31	53.00	53.16	156,960	53.29	53.09	53.19	157,002	51.87	53.23	52.55	156,984	53.16	52.58	52.87
30%	235,650	51.57	51.20	51.39	235,584	51.53	51.28	51.41	235,650	50.08	51.47	50.78	235,626	51.38	51.05	51.22
40%	314,289	50.31	49.82	50.07	314,202	50.25	50.06	50.16	314,289	48.84	50.23	49.54	314,256	50.12	49.77	49.95
50%	392,928	49.35	48.90	49.13	392,826	49.27	49.09	49.18	392,928	47.92	49.28	48.60	392,889	49.19	48.88	49.04
60%	471,576	48.49	48.16	48.33	471,450	48.46	48.33	48.40	471,576	47.16	48.52	47.84	471,528	48.39	48.15	48.27
70%	550,218	47.72	47.50	47.61	550,074	47.77	47.66	47.72	550,218	46.47	47.83	47.15	550,161	47.71	47.49	47.60
80%	628,866	47.12	46.90	47.01	628,698	47.20	47.08	47.14	628,866	45.90	47.25	46.58	628,794	47.15	46.92	47.04
90%	707,505	46.61	46.39	46.50	707,313	46.68	46.58	46.63	707,505	45.34	46.76	46.05	707,794	46.63	46.37	46.50
100%	786,432	46.12	45.92	46.02	786,222	46.23	46.14	46.19	786,432	44.84	46.31	45.58	786,351	46.16	45.94	46.05

Table 5. Comparison of embedding capacity and PSNR value of different stego images for $n = 3$.

EC (Ratio)	Lena				Baboon				Airplane				Peppers			
	EC (bits)	PSNR			EC (bits)	PSNR			EC (bits)	PSNR			EC (bits)	PSNR		
		Psnr1	Psnr2	Avg		Psnr1	Psnr2	Avg		Psnr1	Psnr2	Avg		Psnr1	Psnr2	Avg
10%	104,440	50.37	50.44	50.41	104,368	50.44	50.57	50.51	104,440	49.67	50.07	49.87	104,376	50.20	50.02	50.11
20%	209,296	47.43	47.36	47.40	209,152	47.46	47.47	47.47	209,296	46.73	47.07	46.90	209,160	47.20	47.05	47.13
30%	314,160	45.70	45.58	45.64	313,936	45.62	45.62	45.62	314,160	44.97	45.35	45.16	313,952	45.43	45.41	45.42
40%	419,016	44.44	44.30	44.37	418,720	44.31	44.36	44.34	419,016	43.71	44.12	43.92	418,744	44.15	44.10	44.13
50%	523,872	43.46	43.31	43.39	523,504	43.37	43.42	43.40	523,872	42.75	43.16	42.96	523,536	43.24	43.14	43.19
60%	628,728	42.66	42.59	42.63	628,280	42.62	42.67	42.65	628,728	41.97	42.38	42.18	628,320	42.49	42.40	42.45
70%	733,584	41.94	41.91	41.93	733,064	41.90	41.98	41.94	733,584	41.31	41.72	41.52	733,112	41.86	41.76	41.81
80%	838,456	41.34	41.29	41.32	837,856	41.36	41.41	41.39	838,456	40.73	41.16	40.95	837,912	41.25	41.17	41.21
90%	943,312	40.82	40.78	40.80	942,640	40.87	40.92	40.90	943,312	40.22	40.64	40.43	942,696	40.73	40.63	40.68
100%	1,048,576	40.37	40.33	40.35	1,047,832	40.40	40.44	40.42	1,048,576	39.73	40.18	39.96	1,047,896	40.30	40.21	40.26

Table 6. Comparison of embedding capacity and PSNR value of different stego images for $n = 4$.

EC (Ratio)	Lena			Baboon			Airplane			Peppers		
	EC (bits)	PSNR			EC (bits)	PSNR			EC (bits)	PSNR		
		Psnr1	Psnr2	Avg		Psnr1	Psnr2	Avg		Psnr1	Psnr2	Avg
10%	131,050	44.47	44.46	44.47	130,915	44.47	44.53	44.50	131,050	43.71	43.99	43.85
20%	262,120	41.48	41.40	41.44	261,840	41.46	41.47	41.47	262,120	40.81	41.05	40.93
30%	393,195	39.75	39.65	39.70	392,770	39.70	39.68	39.69	393,195	39.04	39.28	39.16
40%	524,265	38.49	38.37	38.43	523,705	38.38	38.40	38.39	524,265	37.81	38.05	37.93
50%	655,330	37.48	37.38	37.43	654,635	37.44	37.45	37.45	655,340	36.85	37.11	36.98
60%	786,400	36.68	36.62	36.65	785,570	36.65	36.68	36.67	786,410	36.08	36.33	36.21
70%	917,480	36.00	35.96	35.98	916,505	35.99	36.02	36.01	917,490	35.42	35.67	35.55
80%	1,048,555	35.39	35.35	35.37	1,047,440	35.42	35.44	35.43	1,048,560	34.84	35.09	34.97
90%	1,179,625	34.87	34.84	34.86	1,178,370	34.90	34.91	34.91	1,179,635	34.32	34.57	34.45
100%	1,310,710	34.40	34.38	34.39	1,309,315	34.48	34.50	34.49	1,310,720	33.81	34.09	33.95

Table 7. Comparison of embedding capacity and PSNR value of different stego images for $n = 5$.

EC (Ratio)	Lena			Baboon			Airplane			Peppers		
	EC (bits)	PSNR			EC (bits)	PSNR			EC (bits)	PSNR		
		Psnr1	Psnr2	Avg		Psnr1	Psnr2	Avg		Psnr1	Psnr2	Avg
10%	157,218	38.46	38.46	38.46	156,570	38.49	38.52	38.51	157,098	37.86	37.99	37.93
20%	314,484	35.45	35.41	35.43	313,194	35.50	35.50	35.50	314,244	34.82	34.94	34.88
30%	471,744	33.70	33.65	33.68	469,812	33.70	33.69	33.70	471,384	33.10	33.22	33.16
40%	629,010	32.42	32.37	32.40	626,436	32.43	32.44	32.44	628,536	31.89	32.01	31.95
50%	786,276	31.46	31.41	31.44	783,048	31.50	31.51	31.51	785,682	30.94	31.07	31.01
60%	943,548	30.66	30.64	30.65	939,672	30.70	30.71	30.71	942,834	30.17	30.29	30.23
70%	1,100,820	29.97	29.95	29.96	1,096,296	30.01	30.02	30.02	1,099,980	29.51	29.63	29.57
80%	1,258,080	29.37	29.36	29.37	1,252,914	29.45	29.46	29.46	1,257,120	28.92	29.04	28.98
90%	1,415,346	28.85	28.84	28.85	1,409,538	28.94	28.94	28.94	1,414,266	28.37	28.50	28.44
100%	1,572,648	28.39	28.38	28.39	1,566,192	28.48	28.49	28.49	1,571,454	27.89	28.02	27.96

Figure 7 indicates average embedding capacity and PSNR values for $n = 1$ to 5 in all grayscale images used in experimental studies. In the proposed algorithm, it is seen from the graph that the highest PSNR values are obtained for $n = 1$ and the maximum payload value is acquired for $n = 5$.

Table 8 gives the table presenting the comparison of payload, embedding capacity and PSNR values for colored cover images. When $n = 1$, the PSNR value is more than 51 (dB) and up to 1,561,416 bits of secret data can be embedded. When $n = 4$, the PSNR value is more than 34 (dB) and up to 3,847,636 bits of secret data can be embedded, which is the most appropriate relationship between embedding capacity and PSNR in this study. When $n = 5$, the embedding capacity increases significantly, but it is observed that the PSNR value is lower than acceptable (30 dB).

The speed tests of the proposed method for data hiding and extraction are presented in Table 9. For $n = 1$ and 5, the random secret data generated by the computer were hidden and extracted into different grayscale cover images in speed test studies. When the speed tests performed are examined, it is seen that data hiding and extraction times are close to each other and are measured in milliseconds. It has been observed that with the increase in the payload, the times of data hiding and extraction increase.

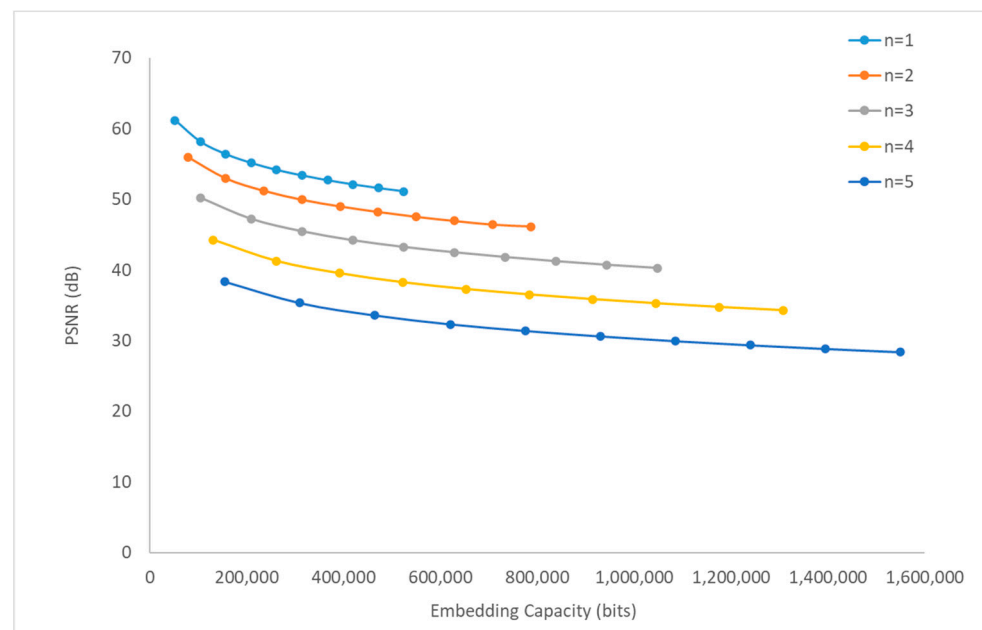


Figure 7. Comparisons of embedding capacity and PSNR values for $n = 1$ to 5 in grayscale images.

Table 8. Comparison of average P, EC and PSNR values for $n = 1$ to 5 in all colored images used in experimental studies.

		Embedding Capacity (EC) Ratio									
		10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
$n = 1$	EC (bits)	156,148	312,306	468,466	624,624	780,780	936,950	1,093,106	1,249,262	1,405,424	1,561,416.5
	PSNR	61.17	58.17	56.40	55.16	54.18	53.39	52.72	52.15	51.63	51.18
$n = 2$	EC (bits)	233,880	467,809.5	701,741	935,678	1,169,605	1,403,535	1,637,465	1,871,393	2,105,321	2,339,292
	PSNR	55.93	52.84	51.09	49.83	48.85	48.06	47.39	46.81	46.30	45.84
$n = 3$	EC (bits)	310,680	621,446	932,218	1,242,986	1,553,752	1,864,518	2,175,286	2,486,050	2,796,818	3,107,663
	PSNR	50.21	47.11	45.37	44.10	43.14	42.34	41.67	41.09	40.58	40.13
$n = 4$	EC (bits)	384,641	769,402	1,154,175	1,538,936	1,923,702	2,308,465	2,693,227	3,077,991	3,462,753	3,847,631
	PSNR	44.29	41.22	39.47	38.21	37.23	36.45	35.77	35.19	34.68	34.23
$n = 5$	EC (bits)	446,355	892,873.5	1,339,386	1,785,895	2,232,403	2,678,914	3,125,422	3,571,933	4,018,444	4,465,063
	PSNR	38.49	35.42	33.67	32.41	31.44	30.65	29.97	29.39	28.87	28.42

Table 10 presents the comparison of dual image-based data hiding methods in the literature with the proposed reversible data hiding method. Our proposed reversible data hiding method gives similar results to the methods in the literature. Some studies provide better PSNR values than our proposed method. However, in some of these studies, it has been expressed in related studies that distortions occurred during the obtaining of the original cover image. Even at high payload values, the PSNR values of the two stego images obtained are very close to each other. Although the payload value was 2 bpp, the PSNR value was obtained over 40 (dB). In the study, it was aimed to keep the PSNR value at an acceptable level while performing high embedding capacity. When the comparison table is examined, it is seen that PSNR values are obtained with similar capacities. In the proposed study, it reached 2.5 bpp using a new method and is resistant to RS analysis attacks. In addition, with the proposed new method, secret data cannot be obtained without the original cover image.

Table 9. Comparison of data hiding and extraction process speed tests of the proposed algorithm.

		Test 1 (sec)	Test 2 (sec)	Test 3 (sec)	Test 4 (sec)	Test 5 (sec)	Average (sec)
$n = 1$	Data Embedding	0.0249	0.0263	0.0263	0.0271	0.0252	0.0259
	Data Extraction	0.0307	0.0298	0.0297	0.0298	0.0298	0.0299
$n = 2$	Data Embedding	0.0319	0.0304	0.0297	0.0344	0.0304	0.0313
	Data Extraction	0.0455	0.0393	0.0370	0.0381	0.0381	0.0395
$n = 3$	Data Embedding	0.0416	0.0364	0.0406	0.0375	0.0379	0.0388
	Data Extraction	0.0554	0.0531	0.0541	0.0558	0.0530	0.0543
$n = 4$	Data Embedding	0.0429	0.0425	0.0455	0.0429	0.0441	0.0435
	Data Extraction	0.0702	0.0677	0.0616	0.0707	0.0706	0.0681
$n = 5$	Data Embedding	0.0551	0.0437	0.0595	0.0489	0.0504	0.0515
	Data Extraction	0.0729	0.0697	0.0775	0.0799	0.0785	0.0757

Table 10. Comparison of previous data hiding algorithm and the proposed algorithm.

References	Measurement Metrics	Lena	Baboon	Peppers	Barbara	Goldhill	Average
[33]	PSNR (dB) (Stego-1)	46.37	47.34	46.72	46.15	46.16	46.66
	PSNR (dB) (Stego-2)	46.36	46.56	46.12	46.71	46.64	46.55
	PSNR(Average)	46.37	46.95	46.42	46.43	46.40	46.61
	EC (bits)	786,432	786,258	786,670	786,432	786,432	786,442
	P (bpp)	1.50	1.50	1.50	1.50	1.50	1.50
[35] (with distortion)	PSNR (dB) (Stego-1)	51.15	51.16	51.16	51.14	50.13	51.15
	PSNR (dB) (Stego-2)	50.18	50.17	50.18	50.16	50.18	50.17
	PSNR(Average)	50.66	50.66	50.66	50.65	50.65	50.66
	EC (bits)	818,914	818,814	818,948	819,315	819,386	819,085
	P (bpp)	1.56	1.56	1.56	1.56	1.56	1.56
[40]	PSNR (dB) (Stego-1)	48.70	48.71	48.71	48.70	48.72	48.71
	PSNR (dB) (Stego-2)	48.71	48.71	48.71	48.71	48.71	48.71
	PSNR(Average)	48.71	48.71	48.71	48.71	48.72	48.71
	EC (bits)	650,369	650,799	650,637	650,781	650,726	650,568
	P (bpp)	1.24	1.24	1.24	1.24	1.24	1.24
[41] (with distortion)	PSNR (dB) (Stego-1)	45.93	46.38	47.20	46.38	46.83	46.65
	PSNR (dB) (Stego-2)	45.35	47.43	46.79	46.57	46.62	46.66
	PSNR(Average)	45.64	46.91	47.00	46.48	46.73	46.66
	EC (bits)	819,356	819,080	818,342	819,156	819,269	819,034
	P (bpp)	1.56	1.56	1.56	1.56	1.56	1.56
[42]	PSNR (dB) (Stego-1)	49.63	49.63	49.64	49.62	49.63	49.63
	PSNR (dB) (Stego-2)	49.63	49.61	49.63	49.63	49.62	49.63
	PSNR(Average)	49.63	49.62	49.64	49.63	49.63	49.63
	EC (bits)	560,801	560,686	560,572	561,223	560,740	560,880
	P (bpp)	1.07	1.07	1.07	1.07	1.07	1.07

Table 10. Cont.

References	Measurement Metrics	Lena	Baboon	Peppers	Barbara	Goldhill	Average
[43]	PSNR (dB) (Stego-1)	49.20	49.21	49.19	49.22	49.23	49.21
	PSNR (dB) (Stego-2)	49.21	49.20	49.21	49.20	49.18	49.20
	PSNR(Average)	49.21	49.21	49.20	49.21	49.21	49.21
	EC (bits)	524,288	524,204	524,192	524,288	524,288	524,257
	P (bpp)	1.00	1.00	1.00	1.00	1.00	1.00
[44]	PSNR (dB) (Stego-1)	47.34	47.34	47.34	47.34	47.34	47.34
	PSNR (dB) (Stego-2)	47.41	47.41	47.41	47.41	47.41	47.41
	PSNR(Average)	47.37	47.38	47.37	47.37	47.37	47.37
	EC (bits)	917,504	917,504	917,504	917,504	917,504	917,504
	P (bpp)	1.75	1.75	1.75	1.75	1.75	1.75
Proposed ($n = 1$)	PSNR (dB) (Stego-1)	51.14	51.14	51.15	51.15	51.15	51.15
	PSNR (dB) (Stego-2)	51.14	51.13	51.14	51.15	51.14	51.14
	PSNR(Average)	51.14	51.14	51.15	51.15	51.15	51.14
	EC (bits)	524,288	524,190	524,104	524,136	524,136	524,171
	P (bpp)	1.00	1.00	1.00	1.00	1.00	1.00
Proposed ($n = 2$)	PSNR (dB) (Stego-1)	46.12	46.23	46.16	46.07	46.11	46.14
	PSNR (dB) (Stego-2)	45.92	46.14	45.94	45.77	45.93	45.94
	PSNR(Average)	46.02	46.19	46.05	45.92	46.02	46.04
	EC (bits)	786,432	786,222	786,351	786,144	786,144	786,259
	P (bpp)	1.50	1.50	1.50	1.50	1.50	1.50
Proposed ($n = 3$)	PSNR (dB) (Stego-1)	40.37	40.40	40.30	40.23	40.33	40.33
	PSNR (dB) (Stego-2)	40.33	40.44	40.21	40.14	40.18	40.26
	PSNR(Average)	40.35	40.42	40.26	40.19	40.26	40.29
	EC (bits)	1048,576	1047,832	1047,896	1048,168	1,048,168	1,048,128
	P (bpp)	2.00	2.00	2.00	2.00	2.00	2.00

In addition, we applied three steganalysis tests, namely histogram analysis, pixel difference histogram (PDH) and RS analysis, to prove the security of our proposed data hiding algorithm. First, the histogram analysis was performed, showing the pixel value distributions of cover, stego1 and stego2 images according to $n = 1$ and 3. Figures 8–10 present histogram analyzes for $n = 1$ to 3 in a grayscale Lena image. In addition, the comb effect, which indicates that there is secret data in the stego images, was not observed.

The second method used in security tests is to obtain the distribution of pixel differences as called PDH. In the PDH diagram, the cover image is expected to be according to the zero mean normal distribution. In the stego image PDH, using some data hiding methods, it is possible that the distribution curve is zigzagging, periodically flats (e.g., PVD), multiple peaks (e.g., Histogram Shifting) or deviation from normal distribution. In addition, the similarity of the distributions of two stego images to each other can be a criterion in dual image based reversible data hiding methods. For the proposed data hiding method, PDHs are presented in Figure 11 for $n = 1$ –4 values. It can be seen from Figure 11 that, for all n values, the PDH graphics of two stego images overlap with each other. It is also seen that cover and stego images PDH analyzes for $n = 1$ to 3 are close.

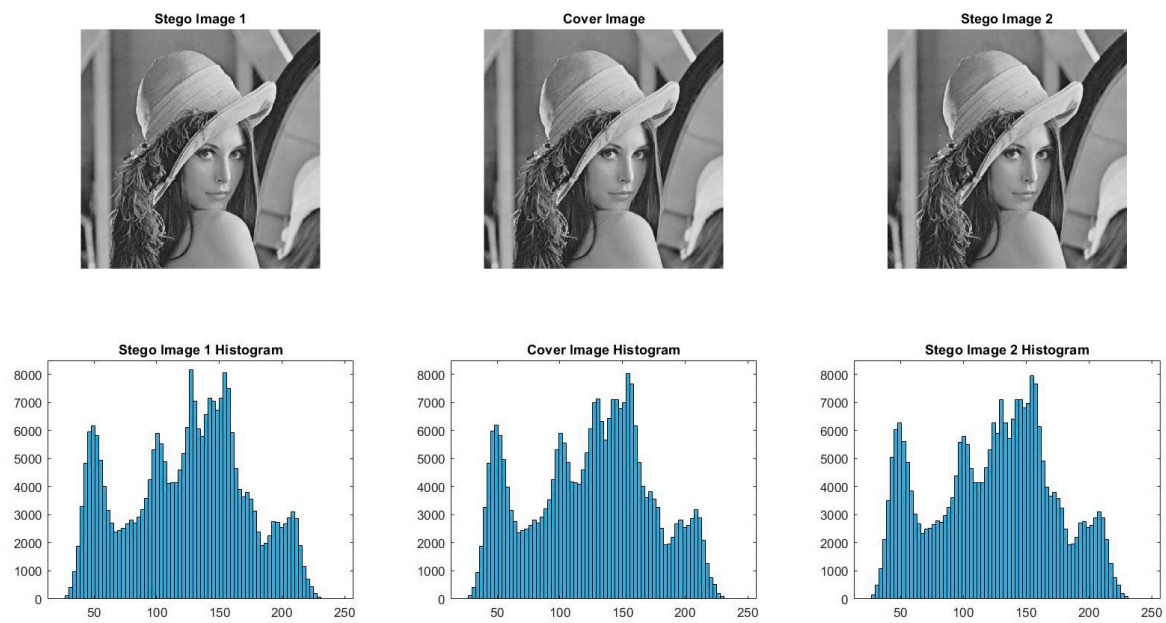


Figure 8. Comparisons of histogram analysis for $n = 1$ in grayscale Lena image.

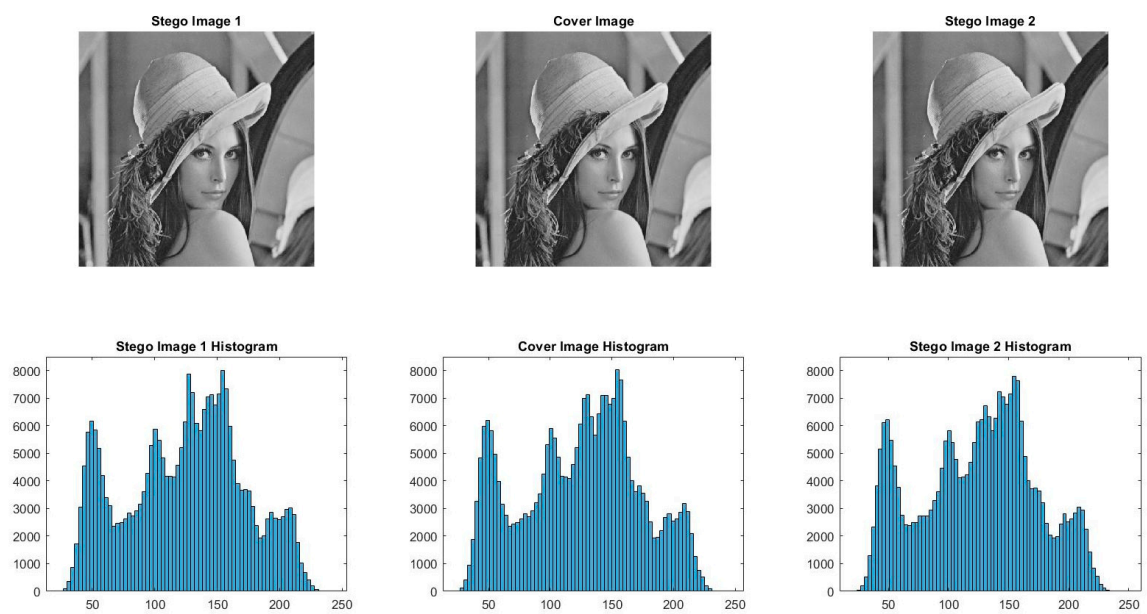


Figure 9. Comparisons of histogram analysis for $n = 2$ in grayscale Lena image.

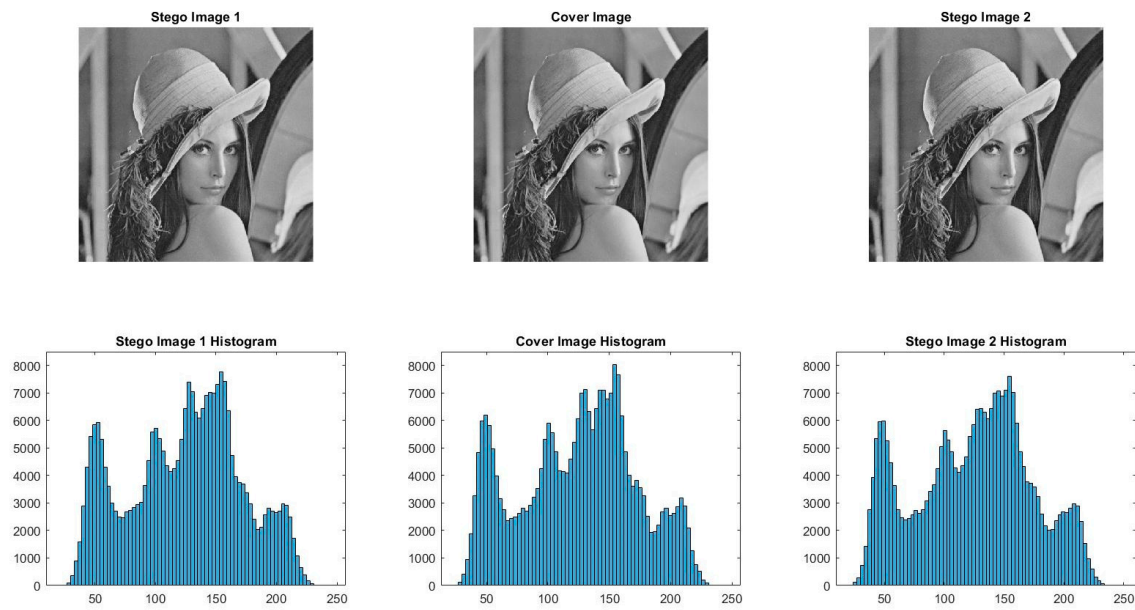


Figure 10. Comparisons of histogram analysis for $n = 3$ in grayscale Lena image.

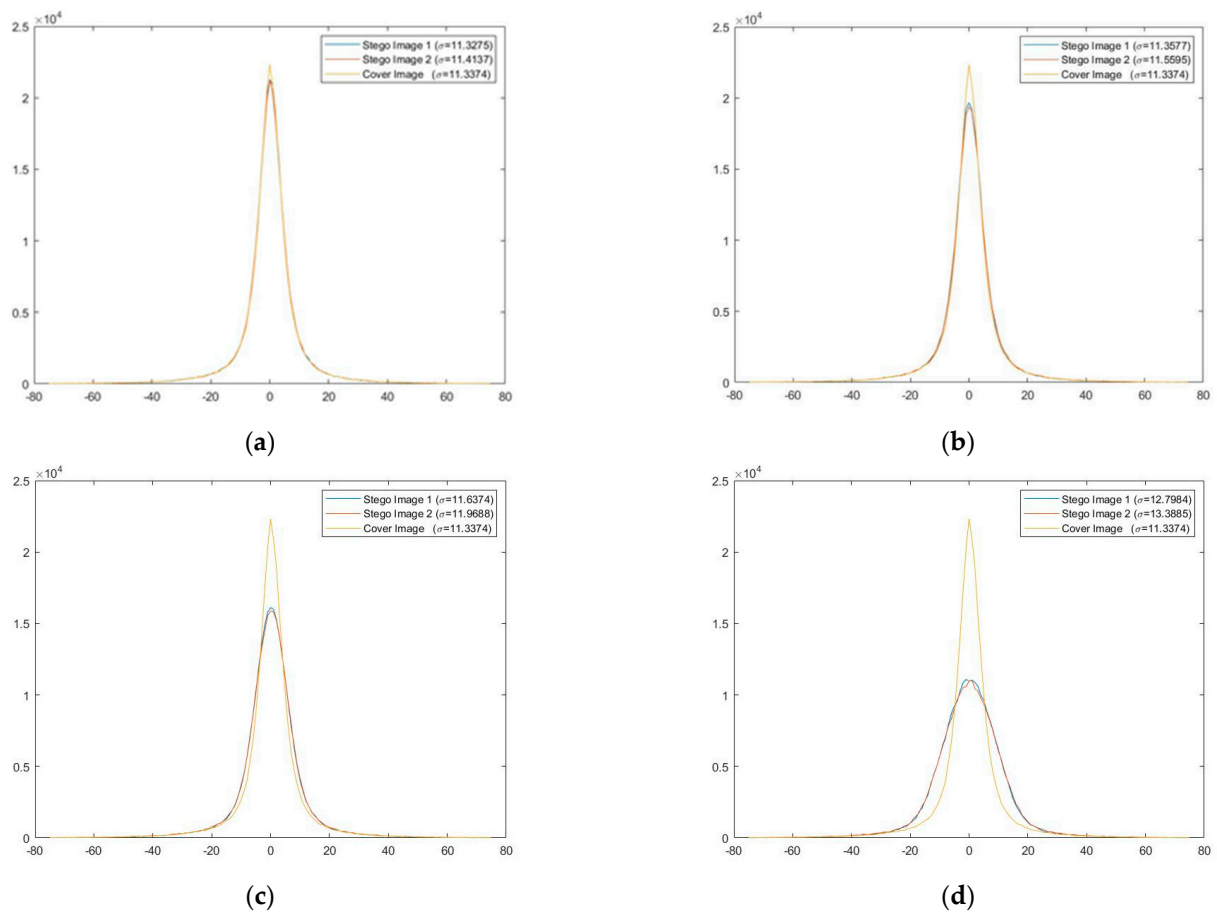


Figure 11. Comparisons of PDH analysis for $n = 1$ to 4 in grayscale Lena image. (a) $n = 1$; (b) $n = 2$; (c) $n = 3$; (d) $n = 4$.

Finally, a statistical steganalysis method called RS analysis, which measures the ratio of Regular (R) and Singular (S) pixel groups, was used to measure the security of the algorithm. In this analysis, the ratio of regular pixel groups (R_m , $R-m$) to less than the ratio

of the singular pixel group (Sm, S-m) indicates that there is distortion in the image, that is, secret data may be embedded. In other words, that image is normal when the expression " $S_m \approx S-m < R_m \approx R-m$ " is provided. When the difference between (Rm, R-m) values and (Sm, S-m) values increase, it is understood that there is secret data in the image. Figure 12 presents RS analysis results for the proposed method. The proposed method proves to be resistant to steganalysis attacks, even when there is high capacity of secret data in the stego image, when examining Figure 12a–d.

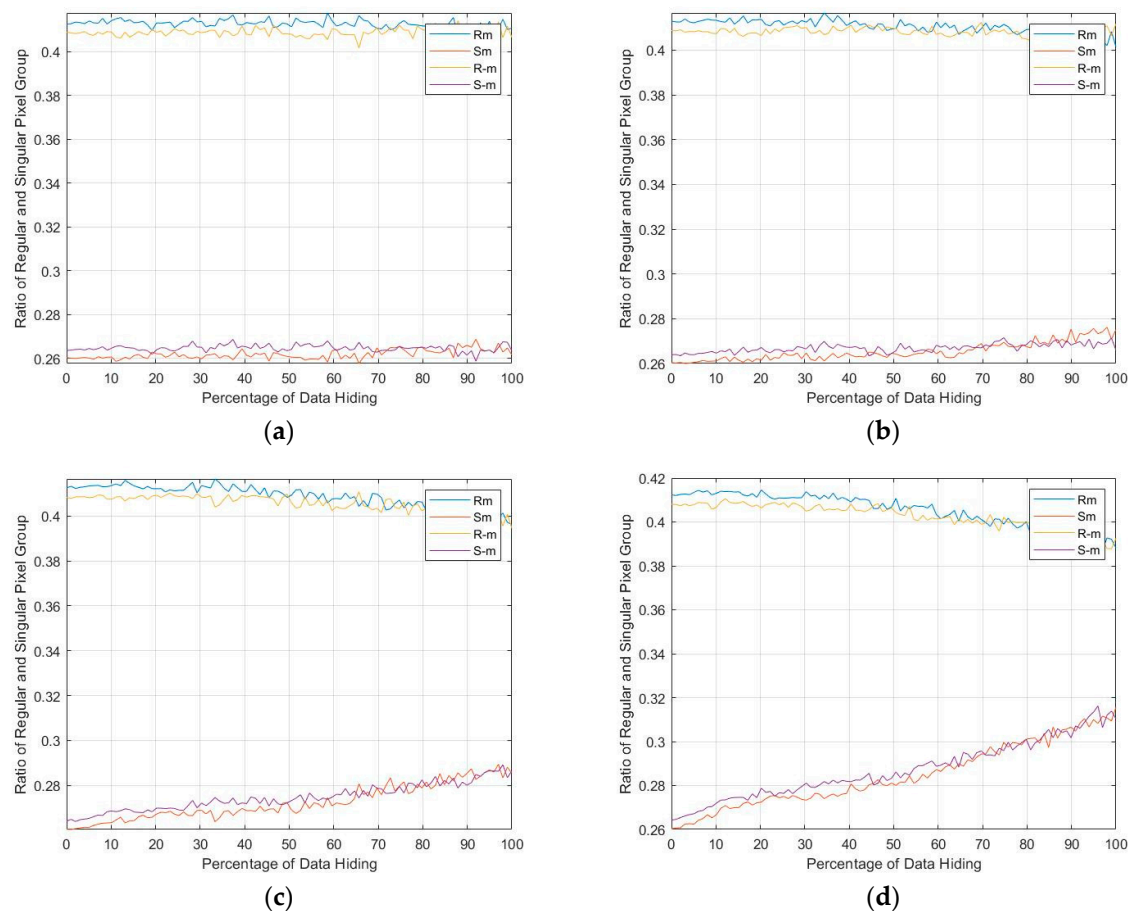


Figure 12. Comparisons of RS analysis for $n = 1$ to 4 in grayscale Lena image. (a) $n = 1$; (b) $n = 2$; (c) $n = 3$; (d) $n = 4$.

5. Conclusions

This paper proposed a new dual image based reversible data hiding algorithm. The data hiding algorithm utilizes center shifting technique and the most significant bits to ensure high embedding capacity and security. The algorithm hides secret data lossless in the data hiding process and obtains the original cover image without distortion in the data extraction process. In addition, during the data extraction stage, the secret data cannot be extracted before the original cover image can be obtained, which provides additional security. The algorithm provides that if the payload is 2.5 bpp, the PSNR value is higher than 34 (dB). Also, experimental results show that the algorithm is resistant to RS attacks.

Author Contributions: Conceptualization, S.S.; methodology, S.S. and G.T.; software, G.T.; investigation, S.S. and G.T.; writing—original draft preparation, S.S.; writing—review and editing, S.S. and G.T.; visualization, G.T.; supervision, S.S.; project administration, S.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been supported by Kocaeli University Scientific Research and Development Support Program (BAP) in Turkey under project FBA-2021-2488.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

- Diffie, W.; Hellman, M. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [\[CrossRef\]](#)
- Johnson, N.F.; Jajodia, S. Exploring steganography: Seeing the unseen. *Computer* **1998**, *31*, 26–34. [\[CrossRef\]](#)
- Solak, S.; Altınışık, U. Image steganography based on LSB substitution and encryption method: Adaptive LSB+ 3. *J. Electron. Imaging* **2019**, *28*, 043025. [\[CrossRef\]](#)
- Solak, S. High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms. *IEEE Access* **2020**, *8*, 166513–166524. [\[CrossRef\]](#)
- Solak, S.; Altınışık, U. A new approach for Steganography: Bit shifting operation of encrypted data in LSB (SED-LSB). *Bilişim Teknol. Derg.* **2019**, *12*, 75–81. [\[CrossRef\]](#)
- Konyar, M.Z.; Solak, S. Efficient data hiding method for videos based on adaptive inverted LSB332 and secure frame selection with enhanced Vigenere cipher. *J. Inf. Secur. Appl.* **2021**, *63*, 103037. [\[CrossRef\]](#)
- Solak, S.; Altınışık, U. Image Steganography-Based GUI Design to Hide Agricultural Data. *Gazi Univ. J. Sci.* **2021**, *34*, 748–763. [\[CrossRef\]](#)
- Sondas, A.; Kurnaz, H. HNMH: A New Hybrid Approach Based on Near Maximum Histogram and LSB Technique for Image Steganography. *Wirel. Pers. Commun.* **2022**, *126*, 2579–2595.
- Lu, T.C.; Vo, T.N. Introduction of Reversible Data Hiding Schemes. In *International Conference on Security with Intelligent Computing and Big-Data Services*; Springer: Cham, Switzerland, 2019; pp. 170–183.
- Kim, P.H.; Ryu, K.W.; Jung, K.H. Reversible data hiding scheme based on pixel-value differencing in dual images. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 1550147720911006. [\[CrossRef\]](#)
- Motomura, R.; Imaizumi, S.; Kiya, H. A Reversible Data-Hiding Method with Prediction-Error Expansion in Compressible Encrypted Images. *Appl. Sci.* **2022**, *12*, 9418. [\[CrossRef\]](#)
- Manikandan, V.M.; Murthy, K.S.R.; Siddineni, B.; Victor, N.; Maddikunta, P.K.R.; Hakak, S. A High-Capacity Reversible Data-Hiding Scheme for Medical Image Transmission Using Modified Elias Gamma Encoding. *Electronics* **2022**, *11*, 3101. [\[CrossRef\]](#)
- Nguyen, T.S.; Huynh, V.T.; Vo, P.H. A Novel Reversible Data Hiding Algorithm Based on Enhanced Reduced Difference Expansion. *Symmetry* **2022**, *14*, 1726. [\[CrossRef\]](#)
- Tian, J. Reversible data embedding using a difference expansion. *IEEE Trans. Circuits Syst. Video Technol.* **2003**, *13*, 890–896. [\[CrossRef\]](#)
- Li, X.; Yang, B.; Zeng, T. Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection. *IEEE Trans. Image Process.* **2011**, *20*, 3524–3533. [\[PubMed\]](#)
- Gui, X.; Li, X.; Yang, B. A high capacity reversible data hiding scheme based on generalized prediction-error expansion and adaptive embedding. *Signal Process.* **2014**, *98*, 370–380. [\[CrossRef\]](#)
- Ni, Z.; Shi, Y.Q.; Ansari, N.; Su, W. Reversible data hiding. *IEEE Trans. Circuits Syst. Video Technol.* **2006**, *16*, 354–362.
- Tsai, P.; Hu, Y.C.; Yeh, H.L. Reversible image hiding scheme using predictive coding and histogram shifting. *Signal Process.* **2009**, *89*, 1129–1143. [\[CrossRef\]](#)
- Zhao, Z.; Luo, H.; Lu, Z.M.; Pan, J.S. Reversible data hiding based on multilevel histogram modification and sequential recovery. *AEU-Int. J. Electron. Commun.* **2011**, *65*, 814–826. [\[CrossRef\]](#)
- Wang, S.Y.; Li, C.Y.; Kuo, W.C. Reversible data hiding based on two-dimensional prediction errors. *IET Image Process.* **2013**, *7*, 805–816. [\[CrossRef\]](#)
- Li, X.; Li, J.; Li, B.; Yang, B. High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion. *Signal Process.* **2013**, *93*, 198–205. [\[CrossRef\]](#)
- Jung, K.H.; Yoo, K.Y. Data hiding method using image interpolation. *Comput. Stand. Interfaces* **2009**, *31*, 465–470. [\[CrossRef\]](#)
- Hu, J.; Li, T. Reversible steganography using extended image interpolation technique. *Comput. Electr. Eng.* **2015**, *46*, 447–455. [\[CrossRef\]](#)
- Malik, A.; Sikka, G.; Verma, H. A Reversible Data Hiding Scheme for Interpolated Images Based on Pixel Intensity Range. *Multimed. Tools Appl.* **2020**, *79*, 18005–18031. [\[CrossRef\]](#)
- Hassan, F.S.; Gutub, A. Efficient reversible data hiding multimedia technique based on smart image interpolation. *Multimed. Tools Appl.* **2020**, *79*, 30087–30109. [\[CrossRef\]](#)
- Yang, C.N.; Hsu, S.C.; Kim, C. Improving stego image quality in image interpolation based data hiding. *Comput. Stand. Interfaces* **2017**, *50*, 209–215. [\[CrossRef\]](#)
- Jung, K.H. A survey of interpolation-based reversible data hiding methods. *Multimed. Tools Appl.* **2018**, *77*, 7795–7810. [\[CrossRef\]](#)

28. Wang, X.T.; Chang, C.C.; Nguyen, T.S.; Li, M.C. Reversible data hiding for high quality images exploiting interpolation and direction order mechanism. *Digit. Signal Process.* **2013**, *23*, 569–577. [\[CrossRef\]](#)
29. Chen, Y.Q.; Sun, W.J.; Li, L.Y.; Chang, C.C.; Wang, X. An efficient general data hiding scheme based on image interpolation. *J. Inf. Secur. Appl.* **2020**, *54*, 102584. [\[CrossRef\]](#)
30. Chang, C.C.; Kieu, T.D.; Chou, Y.C. Reversible data hiding scheme using two steganographic images. In Proceedings of the TENCON 2007–2007 IEEE Region 10 Conference, Taipei, Taiwan, 30 October–2 November 2007; pp. 1–4.
31. Chang, C.C.; Lu, T.C.; Horng, G.; Huang, Y.H.; Hsu, Y.M. A high payload data embedding scheme using dual stego-images with reversibility. In Proceedings of the 2013 9th International Conference on Information, Communications & Signal Processing, Tainan, Taiwan, 2–4 December 2013; pp. 1–5.
32. Lee, C.F.; Wang, K.H.; Chang, C.C.; Huang, Y.L. A reversible data hiding scheme based on dual steganographic images. In Proceedings of the 3rd international conference on ubiquitous information management and communication, Suwon, Korea, 15 February 2009; pp. 228–237.
33. Lu, T.C.; Wu, J.H.; Huang, C.C. Dual-image-based reversible data hiding method using center folding strategy. *Signal Process.* **2015**, *115*, 195–213. [\[CrossRef\]](#)
34. Chi, L.P.; Wu, C.H.; Chang, H.P. Reversible data hiding in dual stegano-image using an improved center folding strategy. *Multimed. Tools Appl.* **2018**, *77*, 8785–8803. [\[CrossRef\]](#)
35. Shastri, S.; Thanikaiselvan, V. Dual image reversible data hiding using trinary assignment and centre folding strategy with low distortion. *J. Vis. Commun. Image Represent.* **2019**, *61*, 130–140. [\[CrossRef\]](#)
36. Meikap, S.; Jana, B. Improved center-folding based directional pixel value ordering for reversible data hiding scheme. *Multimed. Tools Appl.* **2021**, *80*, 5617–5652. [\[CrossRef\]](#)
37. Lu, T.C.; Huang, S.R.; Huang, S.W. Reversible hiding method for interpolation images featuring a multilayer center folding strategy. *Soft Comput.* **2021**, *25*, 161–180. [\[CrossRef\]](#)
38. Qin, C.; Chang, C.C.; Hsu, T.J. Reversible data hiding scheme based on exploiting modification direction with two steganographic images. *Multimed. Tools Appl.* **2015**, *74*, 5861–5872. [\[CrossRef\]](#)
39. USC-SIPI. Image Database. Available online: <http://sipi.usc.edu/database/> (accessed on 15 October 2022).
40. Jafar, I.F.; Darabkh, K.A.; Al-Zubi, R.T.; Saifan, R.R. An efficient reversible data hiding algorithm using two steganographic images. *Signal Process.* **2016**, *128*, 98–109. [\[CrossRef\]](#)
41. Yao, H.; Qin, C.; Tang, Z.; Tian, Y. Improved dual-image reversible data hiding method using the selection strategy of shiftable pixels' coordinates with minimum distortion. *Signal Process.* **2017**, *135*, 26–35. [\[CrossRef\]](#)
42. Lee, C.F.; Huang, Y.L. Reversible data hiding scheme based on dual stegano-images using orientation combinations. *Telecommun. Syst.* **2013**, *52*, 2237–2247. [\[CrossRef\]](#)
43. Lu, T.C.; Tseng, C.Y.; Wu, J.H. Dual imaging-based reversible hiding technique using LSB matching. *Signal Process.* **2015**, *108*, 77–89. [\[CrossRef\]](#)
44. Lu, T.C.; Chang, T.C.; Shen, J.J. An Effective Maximum Distortion Controlling Technology in the Dual-Image-Based Reversible Data Hiding Scheme. *IEEE Access* **2020**, *8*, 90824–90837. [\[CrossRef\]](#)