applied sciences

MDPI

Article

Advanced Dual Reversible Data Hiding: A Focus on Modification Direction and Enhanced Least Significant Bit (LSB) Approaches

Cheonshik Kim [1,*], Luis Cavazos Quero [1], Ki-Hyun Jung [2] and Lu Leng [3,*]

[1] Department of Computer Engineering, Sejong University, Seoul 05006, Republic of Korea; luis@sejong.ac.kr
[2] Department of Software Convergence, Andong National University, Andong 36729, Republic of Korea; kingjung@anu.ac.kr
[3] School of Software, Nanchang Hangkong University, Nanchang 330063, China
* Correspondence: mipsan@sejong.ac.kr (C.K.); leng@nchu.edu.cn (L.L.)

Abstract: In this study, we investigate advances in reversible data hiding (RDH), a critical area in the era of widespread digital data sharing. Recognizing the inherent vulnerabilities such as unauthorized access and data corruption during data transmission, we introduce an innovative dual approach to RDH. We use the EMD (Exploiting Modification Direction) method along with an optimized LSB (Least Significant Bit) replacement strategy. This dual method, applied to grayscale images, has been carefully developed to improve data hiding by focusing on modifying pixel pairs. Our approach sets new standards for achieving a balance between high data embedding rates and the integrity of visual quality. The EMD method ensures that each secret digit in a 5-ary notational system is hidden by 2 cover pixels. Meanwhile, our LSB strategy finely adjusts the pixels selected by EMD to minimize data errors. Despite its simplicity, this approach has been proven to outperform existing technologies. It offers a high embedding rate (ER) while maintaining the high visual quality of the stego images. Moreover, it significantly improves data hiding capacity. This enables the full recovery of the original image without increasing file size or adding unnecessary data, marking a significant breakthrough in data security.

Keywords: Data Hiding (DH); Reversible DH (RDH); Exploiting Modification Direction (EMD); Least Significant Bit (LSB)

Citation: Kim, C.; Cavazos Quero, L.; Jung, K.-H.; Leng, L. Advanced Dual Reversible Data Hiding: A Focus on Modification Direction and Enhanced Least Significant Bit (LSB) Approaches. *Appl. Sci.* **2024**, *14*, 2437. https://doi.org/10.3390/app14062437

Academic Editors: Andres Alvarez-Meza and David Cárdenas-Peña

Received: 12 February 2024
Revised: 9 March 2024
Accepted: 12 March 2024
Published: 14 March 2024

1. Introduction

The Internet's public accessibility facilitates the easy exchange of data. Yet, this openness also increases the risk of surveillance, theft, and corruption of transmitted data. To mitigate these risks, data hiding (DH) technology offers a robust solution to enhance the security of data in transit. DH techniques protect data by embedding it within another file or message, often within a 'cover image', to create what is known as a 'stego image' [1,2].

This technique allows the cover image to conceal the secret data, effectively shielding it from unauthorized viewers, and it is then transmitted to the intended recipient [3,4]. The alterations to the cover image are typically imperceptible, making the hidden data nearly undetectable without specialized analysis tools. This characteristic significantly enhances the confidentiality of messages hidden within stego images, positioning DH as an excellent strategy for secure communication via the Internet.

DH techniques are categorized into the following two main types: reversible and irreversible. Reversible data hiding (RDH) [5] technology is vital for ensuring information security and maintaining data integrity. The primary advantage of RDH is its ability to perfectly restore the original cover image to its original state after the extraction of the embedded data, thus preserving the quality of the cover image without any loss of the original data. This feature not only enhances information security, but also maintains

the high quality of the original data and images, offering a robust level of security. RDH is especially beneficial in fields requiring high precision and protection, including legal documents, medical images, and copyrighted content, due to its unique capability of the complete recovery of the original data and strict security requirements. This makes RDH an invaluable tool in areas where data integrity and security are of the utmost importance.

Building on the foundation of RDH's significance, various methods [5–8] have been developed to optimize its application while addressing specific challenges. The difference expansion (DE) method, introduced by Tian [5], and the histogram shift (HS) method, developed by Ni [6], illustrate RDH's versatility; moreover, while DE offers substantial data capacity by modifying the pixel value differences, it may introduce visual distortions in sensitive applications. Conversely, HS [6,7] aims to minimize such distortions by adjusting the image's histogram for data embedding, thus preserving the visual integrity of the cover image. The strategic application of RDH highlights its indispensable role in ensuring both the secure transmission of information and the impeccable recovery of the original data.

The predictive coding (PE) method, proposed by Tsai [8], leverages the correlation between neighboring pixels to accurately predict their values, embedding data within the prediction's error margins. By capitalizing on the inherent redundancy in images, Tsai's method discreetly embeds data, minimizes noticeable alterations, and preserves the original image's quality more effectively than the DE method [5].

The field of DH technology has seen significant advancements with the introduction of various techniques, notably, the least significant bit (LSB) substitution method. Pioneered by Chan and Cheng in 2004 [9], this technique embeds hidden data into an image by altering its LSB. In this method, the k secret bits are used to replace the k least significant bits of each cover pixel, thus embedding the hidden data into the image. Building on this foundational approach, numerous enhancements have been proposed, driving the continuous evolution of DH technology.

Initially introduced by Mielikainen in 2006, the LSB matching method [10–14] embeds messages by altering the least significant bit (LSB) of the cover pixel. This technique, also recognized as $\pm$ embedding, adjusts the pixel value by randomly adding or subtracting one to ensure the message bit aligns with the cover pixel's LSB when they do not match. Such a strategy is designed to minimize pixel value alterations, thereby reducing the image distortion. After Mielikainen's foundational LSB matching approach, various methods [11–14] have emerged that enhance the technique's utility and application.

In 2006, Zhang and Wang [15] introduced a DH method using the EMD (exploiting modification direction) technique, which encodes secret data according to a $(2n + 1)$ arithmetic scheme into n cover pixels for transmission. This method involves selecting a pixel from the n cover pixels and subtly modifying its value—either by incrementing or decrementing by one—to embed the secret information, while the EMD technique is lauded for its data hiding efficiency, it's crucial to note that, unlike RDH methods, the original cover image cannot be restored after data extraction with the EMD approach, highlighting a significant distinction.The data hiding method based on Hamming coding [16], a coding method known as an error correction code, is known to be an effective method of hiding data in images.

Meanwhile, dual RDH [13,14,17–23], inspired by traditional secret image sharing methods [24], represents an advanced technique requiring two cover images for the DH process. In this method, secret data are concealed within both images. These altered images—now known as stego images—must then be combined to retrieve the embedded data. Over the past decade, this method has undergone intensive research and development, highlighting its promise for secure data transmission.

Since Chang et al. (2007) [17] introduced an RDH method that leverages the EMD technique, research into this and related methods [13,14,22,23] has significantly expanded. Additionally, some researchers have investigated dual RDH using the LSB matching technique [13,14,22,23] as an alternative approach. Unlike EMD, LSB matching aims at

aligning the LSBs of pixel values in two cover images for data embedding, offering a distinct balance between data capacity and image fidelity.

Chang et al. (2013) [21] proposed a DH method, in which only one pixel is changed by replacing the major and minor diagonals with horizontal and vertical lines. Similarly, Lee and Huang (2013) [25] introduced a method for hiding data by grouping two contiguous pixels from each of the two cover images, achieving reversibility by combining pairs of pixels in a dual stego image in a specific direction.

In 2015, Lu et al. [14] presented a novel RDH technique using two images and LSB matching, marking a significant advance in DH technology. This method introduces a new approach by combining two images to enhance security and data capacity. Following this innovation, Wang et al. [13] in 2017 published an improved version of the two-image-based reversible encryption technique, incorporating enhanced LSB matching. In this refined approach, duplicates of the cover image are created, and an advanced LSB matching method is applied to embed the secret message in both images, demonstrating a creative application of existing technologies for improved results. In 2022, Tseng et al. [23] made a significant contribution to the field by introducing an innovative reversible data encryption technique. Leveraging a novel LSB sorting technique combined with EMD, this method significantly expands and refines the strategies previously available in this field. A thorough analysis of this modified LSB matching technique has revealed theoretical similarities with the EMD method, enriching our understanding of its fundamental principles.

In this study, we introduce a groundbreaking RDH technique that combines the exploiting modification direction (EMD) method with an optimal least significant Bit (OLSB) replacement strategy, which is applied to two identical grayscale cover images. This approach represents a significant departure from traditional EMD methods, which typically embed about 1.10 bits of data per pixel in dual-pixel pairs. Our innovation does not only match the data embedding efficiency of irreversible EMD methods, but also significantly enhances the reversibility of RDH.

One of the most compelling features of our technique is its refined error minimization, which significantly reduces distortions in the marked images. This optimization ensures the visual quality of the output images remains pristine, establishing a new benchmark for RDH practices. Moreover, our method stands out by enabling the complete recovery of the original images without the need for embedding additional payload data—a breakthrough that addresses one of the major limitations faced by previous RDH methods.

Empirical evaluations have shown that our RDH method surpasses existing state-of-the-art techniques in several critical aspects. Notably, it achieves a high embedding rate (ER) while preserving the visual integrity of the stego images. With these advancements, our study presents a novel RDH solution that enhances security and efficiency for data hiding applications, thereby opening new avenues for future research and development in the field of secure digital communication.

The rest of this paper is structured as follows: Section 2 provides the foundational knowledge for our work. In Section 3, we explain the proposed dual RDH method that utilizes EMD and revised LSB matching. Section 4 presents our experimental results and compares them with the established methods. Finally, in Section 5, we draw conclusions and discuss avenues for future research.

2. Related Works

2.1. LSB Matching Revisited

Introduced by Mielikainen [10] in 2006, the LSB matching revisited technique represents a significant innovation in steganography, enabling the embedding of messages within monochrome images. By skillfully altering pixel pair values to discreetly modify the LSB, this technique ensures hidden messages are effectively embedded without compromising the image's visual fidelity. Its primary advantage lies in concealing information while maintaining the original appearance of the image, significantly reducing detection risks.

The method encodes covert messages by adjusting the LSBs of pixel values, minimizing perceptual differences between original and modified images. Such precision in pixel alteration is crucial for obscuring the embedded message, thus preserving the image's authenticity.

Message bits m_i and m_{i+1} are embedded using consecutive pixel values, x_i and x_{i+1}, with the steganographic image representing these pixels as y_i and y_{i+1}. Converting x_i to y_i involves encoding the message bit into the LSB, allowing it to seamlessly integrate with the pixel's binary structure.

Central to this technique is the binary function f, outlined in Equation (1), which determines the need for pixel value adjustments to embed the following message accurately:

$$f(x_i,\ x_{i+1}) = LSB\left(\left\lfloor \frac{x_i}{2} \right\rfloor + x_{i+1}\right) \tag{1}$$

This function f guides the embedding process, indicating how pixel pairs x_i and x_{i+1} are modified to encode the message bits m_i and m_{i+1}. If the LSB of x_i aligns with m_i, no modification is made, and y_i remains as x_i. Conversely, if f mandates an adjustment, x_i is incremented or decremented by one to correctly capture the message bit, thus changing y_i. Similarly, y_{i+1}'s value is adjusted based on $f(x_i - 1,\ x_{i+1})$ in relation to m_{i+1}.

Mielikainen's approach is further validated by its reduction in the average number of pixel adjustments needed for embedding messages. Experiments indicate that this method averages just 0.375 changes per pixel, a notable improvement from the previous standard of 0.500 changes with traditional LSB techniques. This advancement not only confirms the method's high efficacy, but also its concordance with theoretical models. Figure 1 explains the details of this LSB match process.

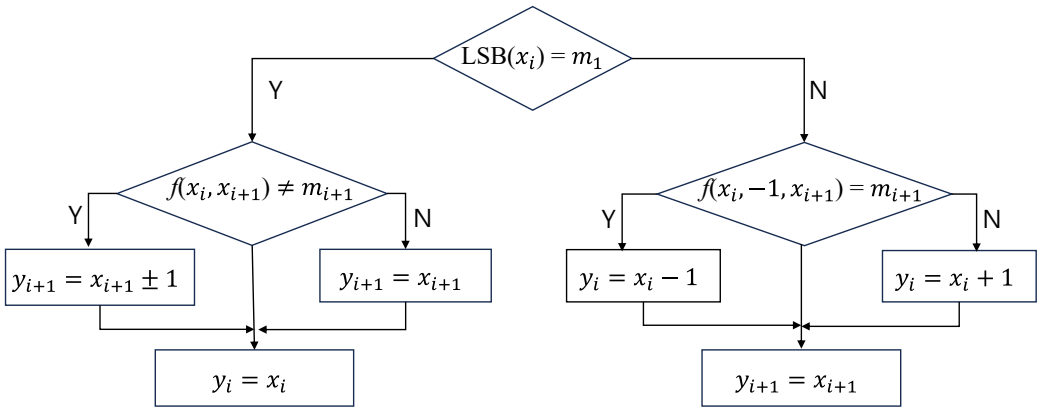


Figure 1. Schematic diagram of LSB matching revisited method [10,14].

2.2. Dual-Images RDH Techniques Using LSB Matching Method

In 2015, Lu et al. [14] introduced a sophisticated RDH method leveraging the LSB matching technique with two identical cover images. These images are represented as two sets, $X_1 = \{x_1^1,\ x_2^1,\ \ldots,\ x_n^1\}$ and $X_2 = \{x_1^2,\ x_2^2,\ \ldots,\ x_n^2\}$. By applying the LSB matching to the corresponding pixel values—$x_i^1,\ x_{i+1}^1$ in X_1 and $x_i^2,\ x_{i+1}^2$ in X_2—two new sets, X_1' and X_2', are produced, each containing the modified pixels.

More precisely, the pixel pair $(x_i^1,\ x_{i+1}^1)$ is used to hide the messages m_1 and m_2, and the corresponding pixel pair $(x_i^2,\ x_{i+1}^2)$ is used to hide the messages m_3 and m_4. This method can simultaneously hide two sets of data that first detect the location of a pixel change.

To restore the original pixel values, they calculate the average of the two marked pixels. Specifically, the calculated pixel values, p_i and p_{i+1}, are obtained by applying the floor function to the average of each corresponding pixel pair from the two sets. This process is illustrated in Equation (2), where the floor function truncates a real number to the nearest

smaller integer. This method ensures the restoration of the original pixel values to their nearest possible approximation.

$$\begin{cases} p_i = \lfloor (x_i^1 + x_i^2)/2 \rfloor, \\ p_{i+1} = \lfloor (x_{i+1}^1 + x_{i+1}^2)/2 \rfloor \end{cases} \tag{2}$$

When using the LSB matching technique, there are cases where the original pixel values cannot be recovered using the Equation (2). When the conditions $x_i \neq p_i$ or $x_{i+1} \neq p_{i+1}$ are satisfied, the original pixels— namely, x_i^1, x_{i+1}^1, x_i^2, and x_{i+1}^2—are modified to produce obfuscated pixels. These changes are made according to guidelines given in a predefined rules table. A summary of this table can be found in Table 1.

Table 1. Modified rule table.

Rule	Case	Pixel Value Modification				The Final Modified Pixel Values			
		x_i^1	x_{i+1}^1	x_i^2	x_{i+1}^2	x_i^1	x_{i+1}^1	x_i^2	x_{i+1}^2
1	3	0	0	−1	0	$x_i^1 + 2$	$x_{i+1}^1 + 1$	$x_i^2 - 1$	x_{i+1}^2
2	6	0	1	0	1	x_i^1	$x_{i+1}^1 + 1$	x_i^2	$x_{i+1}^2 - 1$
3	7	0	1	−1	0	$x_i^1 + 2$	x_{i+1}^1	$x_i^2 - 1$	x_{i+1}^2
4	9	−1	0	0	0	$x_i^1 - 1$	x_{i+1}^1	$x_i^2 + 2$	$x_{i+1}^2 + 1$
5	10	−1	0	0	1	$x_i^1 - 1$	x_{i+1}^1	$x_i^2 + 2$	x_{i+1}^2
6	11	−1	0	−1	0	$x_i^1 - 1$	$x_{i+1}^1 + 2$	$x_i^2 + 1$	$x_{i-1}^2 + 1$
7	16	1	0	1	0	$x_i^1 - 1$	$x_{i+1}^1 - 1$	$x_i^2 + 1$	$x_{i+1}^2 + 2$

2.3. The EMD Method and Applications Based on It

The proposed steganographic technique by Zhang [15] employs the $(2n + 1)$ number system for encoding secret numbers into groups of n pixels. In this scheme, altering a single pixel's value within each group by either increasing or decreasing by one hides the data, offering $2n$ correction methods. A secret message, represented as a binary data stream, is segmented into parts containing $L = \lfloor K \cdot log_2(2n + 1) \rfloor$ bits each, with these segments then expressed in base $(2n + 1)$ as K.

Utilizing the $(2n + 1)$ system, the method embeds a secret number across n pixels after a pseudorandom permutation of all hidden pixels, guided by a secret key. This reorganization results in pixel groups, each comprising n pixels labeled as $x_1, x_2, \ldots, x_n$. Zhang specifies the extraction function f—a weighted sum modulo $(2n + 1)$ based on the grayscale values of these pixels (Equation (3))—streamlining data embedding and retrieval.

$$f(x_1, x_2, \ldots, x_n) = \left[\sum_{i=1}^{n} (x_i \cdot i) \right] mod\ (2n + 1) \tag{3}$$

If the secret number (let us denote it as m) matches the output of the extraction function for the original pixel set, there is no need to change the pixel value. However, if m_i does not align with the extraction function's output, we compute the difference, denoted as s, between m_i and the extraction function output, utilizing modulo $(2n + 1)$. If s is less than or equal to n, then the value of the pixel at index s is incremented by one. Conversely, if s exceeds n, the value of the pixel at index $2n + 1 - s$ is decremented by one.

Consider, for instance, an original pixel group and secret message represented as $[136, 140]$ and $m = 2$. In this scenario, the computed value of the extraction function $f = [(136 \times 1 + 140 \times 2)]\ mod\ 5$ equals one, corresponding to a given secret number in the quintal system. To determine s, one calculates the difference between the secret number m and the output of f, applying modulo 5 for the operation. Hence, $s = m - f = (2 - 1) \bmod 5 = 1$. Should s be less than $n = 2$, the pixel value at the index corresponding to s is incremented by one. Consequently, this adjustment increases the first pixel's value by one, leading to an updated stego pixel group of $[137, 140]$. In cases where the intended secret number for embedding

is '0', s is determined as $(0-1) \bmod 5 = 4$. Given that s exceeds n, the procedure calls for decreasing the value of the pixel at index $2n+1-s = 2\times 2+1-4 = 1$, resulting in a modified stego pixel group of $[135, 140]$. On the receiving end, the extraction of the secret number is facilitated through the computation of the extraction function applied to the stego pixel group.

Qin et al. (2015) [18] performed the embedding process through the following two steps: the first step involved generating a displayed image using an EMD algorithm, and the second step involved generating a subsequent displayed image using an adaptive method, which referenced the first image. The quality of the resulting images was asymmetric, with the first image exhibiting a higher quality than the second.

Lin et al. (2019) [20] introduced a new dual-image-based RDH method leveraging the EMD matrix. This method identifies the four vertices of a 3×3 block and may shift two stego-pixel pairs to these vertices under certain conditions. Within this framework, two secret codes derived from a 5-ary numbering system are embedded within a pixel pair, typically referred to as a cover image. An EMD matrix facilitates these operations, resulting in two sets of modified pixel pairs, also termed stego-pixel pairs. Consequently, the secret data can be precisely extracted, and the original cover image fully restored during the data extraction and image reconstruction phases.

In 2022, Tseng et al. [23] introduced a RDH method based on the revised LSB method and the EMD method in dual images. It was found that the LSB matching revisited method could essentially be considered as a type of EMD method. Unlike conventional methods that typically utilize two pixels of the cover image at a time, this approach operates on a single pixel. The method involves duplicating this single pixel, embedding two secret bits into it, and then distributing these across two steganographic images. Essentially, this method represents an adaptation of the LSB matching revisited approach, involving the duplication of a single pixel value instead of utilizing it directly as input. Figure 2 illustrates the embedding phase of the proposed method.

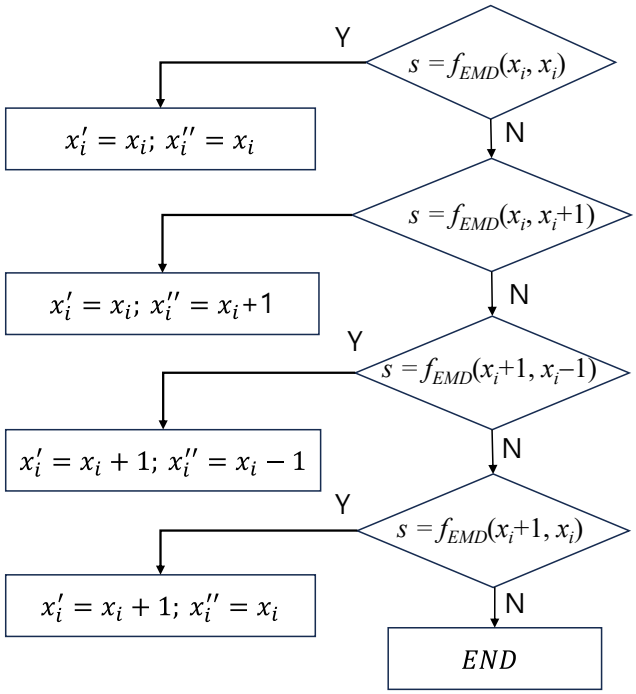


Figure 2. Schematic diagram of reversible modified LSB matching revisited method.

The f_{EMD} extraction function (Equation (4)) for the LSB matching revisited method can be defined as follows:

$$f_{EMD}(x_i, x_{i+1}) = LSB(x_i) * 2 + LSB(\lfloor x_i/2 \rfloor + x_{i+1}) \quad (4)$$

Suppose there is an instance where a single pixel value from the original cover image is two. In the data embedding process, this results in an initial pixel pair of $(2,2)$. For a secret message $s = 1$ and a corresponding $f_{EMD}(2,2) = 1$, the steganographic pixel pair remains $(2,2)$, indicating no change. If $s = 0$, the method evaluates two candidate pairs, $(2,1)$ and $(2,3)$. The pair $(2,1)$ is deemed not viable as it does not allow for the restoration of the original pixel value of two through the recovery formula $x_i = \lfloor (x_i' + x_i'')/2 \rfloor$. Consequently, the pair $(2,3)$ is selected as the stego-pair.

3. Proposed Method

In this section, we present an enhanced dual RDH method, integrating the EMD technique with the LSB replacement strategy to boost performance. Our new method uses two images instead of one to hide data, which is different from the traditional EMD and LSB methods that use a single image. This two-image approach avoids the problem of the original image being permanently altered and un-recoverable. By employing a pair of cover images, our approach not only provides more effective data concealment but also assures the receiver can retrieve and reconstruct the original images, enhancing secure data management.

This technique significantly boosts security and upholds data integrity by requiring two images to fully recover hidden data, effectively mitigating the risks associated with a single image compromise. It guarantees the original data cannot be recovered from just one image, thus reinforcing communication security. Additionally, it preserves the quality of the cover images throughout the data embedding process by discreetly altering a single pixel in each pixel pair, which keeps the changes invisible and maintains the images' natural look.

Using two pixels for pair-wise data hiding, our method can conceal a quinary integer, equivalent to 2.32 bits of information, translating to a data hiding efficiency of 1.16 bits per pixel. This level of efficiency, validated by traditional EMD methods, is retained in our approach, providing a robust and aesthetically unaltered data hiding solution that fulfills complex data protection needs.

Figure 3 illustrates the flow of the enhanced dual RDH process. The sender creates two cover images from the original image and utilizes the RDH technique to embed secret data into each, resulting in two stego images. The receiver employs these images to extract the hidden information and reconstruct the original image through a data extraction and image recovery process. This diagram effectively demonstrates how the proposed method enhances security and maintains data integrity while securely transmitting information.

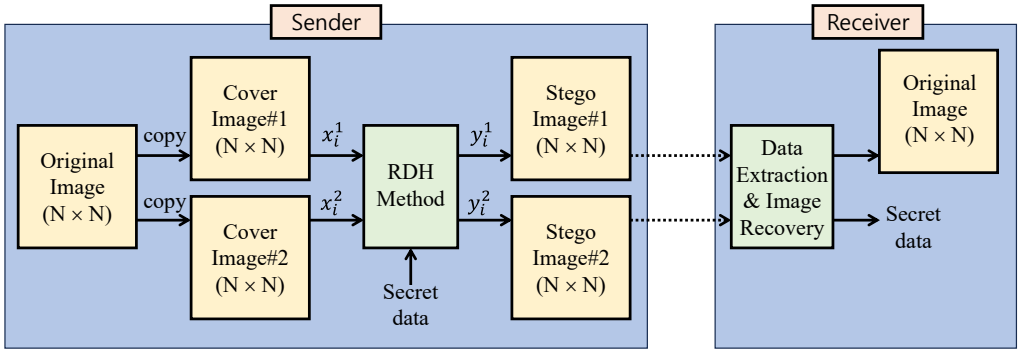


Figure 3. Schematic diagram for the proposed model.

Sections 3.1 and 3.2 provide detailed explanations of the data hiding process and the data extraction and original image restoration process, respectively.

3.1. Data Embedding Procedure

The process involves two cover images, I_1 and I_2, in Figure 3 as duplicates of the original image I. Applying the modified EMD method to pixels $x_i^1 \in I_1$ and $x_i^2 \in I_2$, the 5-ary stream data are concealed. This process is presented in detail in the following steps:

Input: Two cover images I_1 and I_2; 5-ary secret data $m = (m_1, m_2, \ldots, m_n)$.
Output: Two stego images, ΔI_1 and ΔI_2.

Step 1: For cover images I_1 and I_2 of size $N \times N$, comprising pixels $x_i^1 \in I_1$ and $x_i^2 \in I_2$, respectively. The index i indicates the sequence of each pixel;

Step 2: Select a pixel x_i^1 from the first cover image I_1, and its counterpart x_i^2 from the second cover image I_2. Furthermore, determine the crucial data represented by m_i;

Step 3: Compute the extraction function f (using Equation (5)) with the pixel pairs x_i^1 and x_i^2. If the 5-ary number m_i aligns with the function's outcome, no modification is needed. Otherwise, adjust the pixel values of the two pixels to embed the 5-ary number;

$$f(x_1, x_2) = \sum_{i=1}^{N \times N} ([x_i^1 \cdot 1 + x_i^2 \cdot 2]) \; mod \; 5 \tag{5}$$

Step 4: Call Algorithm 1's function Embed(x_i^1, x_i^2, m_i). The Embed receives x_i^1, x_i^2, and m_i as parameters and performs the data hiding process. When data hiding is complete, y_i^1 and y_i^2 are returned;

Step 5: Replace the original pixel values in I_1 and I_2 with the new stego pixel values y_i^1 and y_i^2 from the embedding function in Algorithm 1. Increment the index variable i after this substitution;

Step 6: Proceed with the embedding process by increasing the index i. If i is less than the total number of pixels $(N \times N)$, repeat the previous steps until the full image is processed, resulting in the creation of the stego images ΔI_1 and ΔI_2.

Algorithm 1 provides a detailed description of the key process in our proposed RDH method using pseudocode. Lines 3–4 present the key steps used in the algorithm, while lines 5–17 present our proposed approach, which is simple to implement yet highly effective. Our method provides an efficient way to hide data within the cover image while ensuring data integrity. To eliminate ambiguity in image decoding, it is assumed that the order information of two stego images is specified in the header of the image.

The header of each stego image contains metadata pertaining to the image. This metadata encompasses not only basic details like the image's size, format, and color depth but also supports the inclusion of additional information for specific application requirements. In this study, the sequence information of stego images is captured as an extra field within the image header's metadata, ensuring these images are processed and interpreted in their intended order. Consequently, algorithms or systems utilizing stego images can consult the image header to determine the sequence of images, which is critical for accurately performing data extraction and restoration processes.

The methods introduced by Lu et al. (2015) [14] and Tseng et al. (2022) [23] start by altering a single pixel within each pair as part of the data hiding process. However, there are cases where extracting the hidden bit from the altered pixel pair is unfeasible, necessitating a subsequent modification of the pixel pair. This approach can introduce increased distortion in pixel pairs and elevate time complexity. In contrast, our proposed method seeks to address these challenges head-on, striving to reduce image distortion attributable to the modification of additional pixels. Through the application of EMD and optimal LSB techniques, our method achieves noteworthy enhancements in the algorithm's efficiency.

Algorithm 1 Enhanced EMD with optimal LSB (OLSB) method

procedure EMBED(x_i^1, x_i^2, m_i) ▷ Input: Pixel pairs (x_i^1, x_i^2) from I_1 and I_2, and 5-ary data m_i.
  $y \leftarrow [x_i^1, x_i^2]$; ▷ Initialize y as a vector of the pixel pairs.
  $f \leftarrow (x_i^1 \cdot 1 + x_i^2 \cdot 2)\ mod\ 5$; ▷ Compute f for modulo operation.
  $s \leftarrow m_i - f$; ▷ Determine difference s for data embedding adjustment.
  if $s = 0$ **then**
    no change needed; ▷ No adjustment required for $s = 0$.
  else if $s = 1$ **then**
    $y_1 \leftarrow y_1 + 1$; ▷ Increment first pixel value for $s = 1$.
  else if $s = 2$ **then**
    $y_2 \leftarrow y_2 + 1$; ▷ Increment second pixel value for $s = 2$.
  else if $s = 3$ **then**
    $y_1 \leftarrow y_1 - 1$; ▷ Decrement first pixel to encode $s = 3$.
    $y_2 \leftarrow y_2 + 1$; ▷ Increment second pixel to balance embedding.
  else if $s = 4$ **then**
    $y_1 \leftarrow y_1 + 1$; ▷ Increment first pixel to encode $s = 4$.
    $y_2 \leftarrow y_2 - 1$; ▷ Decrement second pixel to balance embedding.
  end if
  return y ▷ Output the modified pixel pair as stego pixels.
end procedure

3.2. Extraction and Recovering Procedure

Upon successfully receiving the two marked images, ΔI_1 and ΔI_2, sent by the sender, the receiver can proceed to apply the following data extraction and recovery methods step by step. This enables the extraction of the secret data sent by the sender and the recovery of the original image as follows:

Input: Two stego images, ΔI_1 and ΔI_2.
Output: An original image, I and recovered secret data, m'.

Step 1: For the two stego images, ΔI_1 and ΔI_2, each of size $N \times N$, identify the stego pixels $y_i^1 \in \Delta I_1$ and $y_i^2 \in \Delta I_2$. Use the index i to indicate the sequence of each pixel pair;

Step 2: Select a pair of corresponding stego pixels, y_i^1 and y_i^2. Calculate the extraction function f for these pixels using Equation (5);

Step 3: For every pair of stego pixels, y_i^1 and y_i^2, compute and extract the secret message s utilizing the function f. Store the extracted secret message s_i in the vector m_i' to compile the recovered secret data;

Step 4: To restore the original pixel value x_i from the stego pixels y_i^1 and y_i^2, apply Equation (6) as follows:

$$p_i = \left\lfloor \frac{(y_i^1 + y_i^2)}{2} \right\rfloor \tag{6}$$

This step calculates the value of p_i by averaging the values of the two stego pixels and applying the floor function to round down to the nearest integer. The resulting value of p_i represents the i^{th} original pixel in the recovered image I. This process is expressed in detail in pseudocode in Algorithm 2. In other words, the function ExtractRecover(y_i^1, y_i^2) of Algorithm 2 is called. The ExtractRecover function receives y_i^1 and y_i^2 as parameters and extracts data and restores the original pixels. When this process is completed, the data m_i' hidden in the two pixels and the restored pixel p_i are returned;

Step 5: Allocate p_i to the i^{th} pixel of the reconstructed image I. Continue this method for every pixel pair in the stego images until the full original image is restored.

By methodically applying these steps to the stego images, the method accurately reconstructs the original image and securely extracts the hidden message. This procedure

highlights the reversible nature of our steganography method, demonstrating its efficiency and reliability in data recovery.

Algorithm 2 Data extraction and original image recovery

procedure EXTRACTRECOVER(y_i^1, y_i^2) ▷ Input: Stego pixel pairs (y_i^1, y_i^2) from ΔI_1 and ΔI_2.
  Initialize vector m_i' to store recovered 5-ary data.
  Initialize vector p to store original pixel values.
  for each pixel pair (y_i^1, y_i^2) **do**
    $f \leftarrow (y_i^1 \cdot 1 + y_i^2 \cdot 2)\ mod\ 5$; ▷ Compute f for modulo operation.
    $s \leftarrow$ Extracted secret data based on f.
    Append s to vector m_i'.
    $p_i \leftarrow \left\lfloor \frac{(y_i^1 + y_i^2)}{2} \right\rfloor$; ▷ Recover original pixel value.
    Append p_i to vector p.
  end for
  return m_i', p ▷ Output the recovered 5-ary data and original pixel values.
end procedure

This algorithm outlines the procedure for extracting hidden data and reconstructing the original image from two stego images. The process begins by iterating through each pair of stego pixels, (y_i^1, y_i^2), in the modified images ΔI_1 and ΔI_2. For each pixel pair, the algorithm calculates f using the specified modulo operation, then extracts the secret data s relying on f, and subsequently appends this data to the vector m_i' to compile the recovered secret data. Additionally, it derives the original pixel value p_i by averaging the two stego pixel values and applying the floor function to round the result to an integer value. This value is then appended to the vector I. Ultimately, the algorithm yields the compiled recovered 5-ary data and the original pixel values, thereby illustrating the reversible nature of the steganography technique.

3.3. Underflow and Overflow Management

In the embedding phase of our steganographic method, special attention is given to managing pixel values at the extremities, particularly those with values between 0 and 255. This precaution is crucial for preventing underflow and overflow scenarios that could jeopardize the accuracy of data extraction and thus affect the integrity of the pixel values.

Underflow is defined as when an operation attempts to decrease a pixel's value below 0, while overflow occurs when an attempt is made to increase a pixel's value above 255. These conditions can result in erroneous data extraction, as pixel values are supposed to remain within the range from 0 to 255. To address these risks, pixel pairs with extreme values—either (0, 0) or (255, 255)—are intentionally excluded from the data embedding and extraction processes. This approach enhances the system's reliability by avoiding misinterpretations of embedded data and ensuring both the accuracy of the hidden message and the integrity of the pixel values.

The initial collection of pixel pairs used for data hiding is $\{(0,\ 0), (1,\ 1), \ldots, (255,\ 255)\}$, with each pair comprising pixels of identical values. To circumvent potential complications arising from utilizing extremities (0, 0) and (255, 255), like generating computed pixel pairs beyond the permissible range, these specific pairs are omitted from the data hiding process. Consequently, the revised set of pixel pairs for use becomes $\{(1,\ 1), (2,\ 2),\ \ldots,\ (254,\ 254)\}$, thereby reducing ambiguity and errors in the data hiding and extraction processes.

Consider a scenario with a pixel pair of (1, 1) and a data range from 0 to 4; the resulting selection of pixel pairs includes $\{(1,\ 2), (1,\ 0), (0,\ 1), (1,\ 1), (2,\ 1)\}$. Through careful selection, potential decoding challenges are averted, leading to a more secure and efficient steganographic procedure. By excluding pixels with extreme values and appropriately adjusting the pixel pairs, decoding issues are effectively mitigated, enhancing the steganography system's reliability and efficiency.

3.4. Examples

Consider a scenario in which we have two original pixels with values ($x_i^1 = 30$ and $x_i^2 = 30$), and the secret bits to be embedded are represented by $m_i = (100)_2 = 4_5$ in binary and quinary (base-5) systems, respectively. The first step in the embedding process involves assigning the original pixel pair $[x_i^1, x_i^2]$ to a vector denoted as y. Next, we calculate the variables f and s. The formula $f = [30 \cdot 1 + 30 \cdot 2] \bmod 5 = 0$ determines f, which represents a weighted sum of the pixel values modulo 5. Subsequently, we compute s as $s = m_i - f = 4 - 0 = 4$, indicating the difference between the secret message value and f. For $s = 4$, the pixel values are adjusted according to Algorithm 1, which suggests modifying the original pixel values to embed the secret bits, yielding $y \leftarrow [y_1 + 1, y_2 - 1] = [31, 29]$. Hence, the updated stego pixel pair encapsulating the secret bit becomes $y = [31, 29]$.

During the extraction phase, to retrieve the hidden secret bit from the stego pixel pair, we recalculate f as $f = [(31 \cdot 1 + 29 \cdot 2)] \bmod 5 = 4$. The alignment of f with the message value $m_i = 4$ ensures the accurate extraction of the secret bit, which, when converted back to binary, yields $m_i = (100)_2$. Lastly, to restore the original pixel values from the stego pixel pair $y = [31, 29]$, we apply an averaging technique as outlined in Equation (6). This approach accurately reconstructs the original cover pixel value $x_i^1 = 30$, demonstrating the reversible nature of this steganography method.

4. Experimental Results

In this study, we have meticulously conducted a comprehensive comparative analysis to highlight the performance distinctions between our innovative RDH approach and various established methodologies. At the heart of our evaluation framework is a set of nine carefully selected grayscale images, each with a resolution of 512×512 pixels, as illustrated in Figure 4.

Sourced from the esteemed USC-SIPI image database [26], these images form the empirical foundation for our experimental analysis. To anchor our evaluation in rigorous quantitative metrics, we utilize the following two critical performance indicators: embedding capacity (EC) and peak signal-to-noise ratio (PSNR) [16]. Furthermore, PSNR acts as a well-known measure of image quality after data embedding. As defined in Equation (7), PSNR provides a mathematical framework for assessing how well the quality is preserved during the steganographic process, enabling an in-depth investigation into any potential degradation of image quality caused by the data hiding techniques under evaluation.

$$PSNR = 10log_{10}\frac{255^2}{MSE} \tag{7}$$

These metrics are vital for a detailed comparison of the efficacy of our proposed solution against established techniques in the domain. EC measures the number of secret bits that can be seamlessly integrated into a cover image without compromising its visual perception. This analysis aims to shed light on the relative advantages and possible limitations of our method, laying a strong foundation for ongoing innovation and enhancement in the realms of digital image processing and secure data embedding.

More precisely, PSNR is defined by an equation that quantifies the relationship between the maximum possible power of a signal and the impact of noise that compromises its integrity upon reproduction.

To measure PSNR, the mean square error (MSE) (Equation (8)) is utilized, indicating the average squared deviation in intensity levels between the compressed and the original (or reference) image.

$$MSE(x, y) = \frac{1}{N \times N}\sum_{i=1}^{N^2}(x_i - y_i)^2 \tag{8}$$

High image quality is indicated when the MSE of the compressed image is low, which suggests only a minor deviation from the original. MSE is determined by comparing the

following two images: the original, denoted as x, and the distorted or compressed version, represented as y.

Figure 4. Test grayscale images (512 × 512): (**a**) Baboon, (**b**) Barbara, (**c**) Boat, (**d**) Goldhill, (**e**) Airplane, (**f**) Lena, (**g**) Peppers, (**h**) Tiffany, and (**i**) Zelda.

Table 2 presents a comparison of the data hiding performance of our proposed methods with that of existing methods, including Lee & Huang (2013) [25], Lu et al. (2015) [14], Sahu & Swain (2019) [22], Lin et al. (2019) [20], and Tseng & Leng (2022) [23]. Among these comparisons, Lee & Huang (2013) and Lin et al. (2019) report a performance of 1.07 bits per pixel (bpp), showing comparable outcomes. However, our analysis finds no significant overall difference in performance among the existing methods. Noteworthy is that Lin et al. (2019) [20] employ an EMD-based method, whereas Tseng & Leng (2022) [23] utilize a LSB matching revisited approach. Our proposed method exhibits superior performance, achieving 1.10 bpp, thus surpassing the bpp values reported by the previously mentioned methods.

Table 2. Comparison of maximum embedding ratio with different schemes.

Images	Lee & Huang [25]	Lu et al. [14]	Sahu & Swain [22]	Lin et al. [20]	Tseng & Leng [23]	Proposed
Lena	1.07	1.0	1.0	1.07	1.0	1.10
Baboon	1.07	0.9	1.0	1.07	0.9	1.10
Pepper	1.07	0.9	1.0	1.07	0.9	1.10
Boat	1.07	0.9	1.0	1.07	1.0	1.10
Airplane	1.07	0.9	1.0	1.07	1.0	1.10
Goldhill	1.07	0.9	1.0	1.07	1.0	1.10
Barbara	1.07	0.9	1.0	1.07	1.0	1.10
Tiffany	1.07	0.9	1.0	1.07	1.0	1.10
Zelda	1.07	1.0	1.0	1.07	1.0	1.10
Average	1.07	0.92	1.0	1.07	0.97	1.10

To assess the performance of data quality and embedding capacity (EC), we conducted simulations on both the existing methods and our proposed method using randomly generated data on selected cover images. The results are showcased in Table 3, where the superiority of our proposed method is highlighted.

Table 3. Comparison with existing dual-image-based scheme in terms of PSNR and EC(bpp) after maximum data.

Image	Methods		Chang et al. [17]	Lu et al. [14]	Sahu et al. [22]	Tseng et al. [23]	Proposed
Lena	PSNR	ΔI_1	45.19	49.12	51.17	51.14	50.34
		ΔI_2	45.20	49.13	49.41	51.13	51.13
	EC (bits)		524,288	524,288	524,288	524,288	576,565
Baboon	PSNR	ΔI_1	45.18	47.95	51.16	51.14	50.34
		ΔI_2	45.19	49.15	49.41	51.14	51.13
	EC (bits)		522,888	522,996	524,288	524,210	576,203
Pepper	PSNR	ΔI_1	45.21	49.11	51.14	51.14	50.35
		ΔI_2	45.21	49.08	49.72	51.14	51.13
	EC (bits)		523,356	524,192	524,288	524,240	576,659
Boat	PSNR	ΔI_1	45.20	49.00	51.18	51.14	50.35
		ΔI_2	45.21	49.07	49.41	51.14	51.15
	EC (bits)		524,208	524,208	524,288	524,288	576,521
Airplane	PSNR	ΔI_1	45.11	49.39	51.13	51.13	50.34
		ΔI_2	45.11	49.03	49.73	51.13	51.13
	EC (bits)		524,208	524,288	524,288	524,288	576,558
Goldhill	PSNR	ΔI_1	45.2	49.17	51.12	51.13	50.35
		ΔI_2	45.17	49.09	49.72	51.12	51.15
	EC (bits)		524,288	524,288	524,288	524,288	576,399
Barbara	PSNR	ΔI_1	45.2	49.14	51.12	51.13	50.34
		ΔI_2	45.21	49.11	49.73	51.13	51.12
	EC (bits)		524,288	524,288	524,288	524,288	577,040
Tiffany	PSNR	ΔI_1	45.18	49.38	51.15	51.16	50.35
		ΔI_2	45.19	49.06	49.73	51.16	51.16
	EC (bits)		524,288	524,288	524,288	524,288	576,947
Zelda	PSNR	ΔI_1	45.66	49.14	51.14	51.14	50.36
		ΔI_2	45.20	49.09	49.71	51.14	51.14
	EC (bits)		524,288	524,288	524,288	524,288	576,705

In this study, we focus on the performance evaluation of data hiding techniques, specifically assessing the effectiveness of various methods (Chang et al. (2007) [17], Lu et al. (2015) [14], Sahu et al. (2019) [22], Tseng et al. [23]), including the approach we propose, in

embedding data within the 'Lena' image to its maximum capacity. The metric employed to gauge the data hiding performance is the peak signal-to-noise ratio (PSNR), a widely recognized standard for quantifying the quality of stego images—images into which data has been embedded—in comparison to the original images.

Dual RDH involves the process of concealing data within two distinct cover images for each evaluated method, denoted as I_1 and I_2. This methodology allows for a comparative analysis of the methods by evaluating the PSNR and embedding capacity (EC) bits of the stego images ΔI_1 and ΔI_2, the outcomes of the embedding process.

The results of our experiments highlight that our proposed method is uniquely capable of embedding data at the maximum capacity, setting it apart from other techniques that exhibited relatively similar data hiding performances. Specifically, the method by Chang et al. (2007) [17] exhibited a PSNR of approximately 45 dB, while Lu et al. (2015) [14] reported an improvement with a PSNR around 49 dB. The technique proposed by Sahu et al. (2019) [22] resulted in a PSNR of 51 dB for ΔI_1 and 49 dB for ΔI_2, averaging approximately 50 dB. The approach by Tseng et al. [23] demonstrated a remarkable consistency in image quality, achieving an average PSNR of 51 dB across both images.

Our proposed method showcased a PSNR of 50 dB for ΔI_1 and 51 dB for ΔI_2, indicating a slight variation in the quality of the two images. Although the average image quality is slightly lower compared to the method proposed by Tseng et al., the superior data hiding capacity of our approach markedly proves its overall excellence. This comprehensive assessment emphasizes the potential of our method in striking a delicate balance between embedding capacity and image integrity, rendering it a compelling choice for applications necessitating robust and efficient data hiding solutions.

Figures 5 and 6 visually demonstrate the change in image quality (PSNR) for the displayed images ΔI_1 and ΔI_2 when various embedding ratios (ERs) are applied to the original image 'Lena'. The ER values were methodically determined by documenting the PSNR measurements in increments of 0.1, with a range from 0.1 to 1.1.

Figure 5 presents the PSNR data for ΔI_1. With the exception of the method proposed by Lu et al. (2015) [14], all instances achieved a PSNR quality above 60 dB at 0.1 bpp. Although our proposed method does not achieve the highest performance, it demonstrates the ability to embed more data than the methods proposed by Tseng et al. (2022) [23] and Sahu et al. (2019) [22]. Notably, these methods are limited to hiding up to 1.0 bpp, while our strategy increases this capacity to 1.10 bpp and also exhibits remarkable PSNR performance.

Figure 6 indicates that our proposed method achieves the highest PSNR across the entire range of embedding ratios compared to the existing methods. The observed slight difference in PSNR between ΔI_1 and ΔI_2 stems from the characteristics of our proposed method, a trait shared by the existing methods.

In Figure 6, the methods introduced by Tseng et al. (2022) [23] and Sahu et al. (2019) [22] exhibit lower PSNR performance over the entire bpp range when compared to our method, exemplifying such properties; therefore, this trait is not an exclusive limitation of our proposed method. As a result, our proposed method has been demonstrated to enhance bpp performance while maintaining a high PSNR level.

The comparative analysis in Figures 5 and 6 validates the non-destructive nature of the RDH approach, and showcases the adaptability and efficiency of our method. We have achieved an optimal balance between embedding capacity and image quality, significantly advancing the field of steganography and digital image processing. In this study, we adopt a dynamic modification strategy through a RDH technique, aimed at offering a flexible adjustment between embedding capacity and image quality, as indicated by PSNR.

This approach offers precise control over the degree of data embedding and makes it possible to adapt the amount of information hidden in the image to the respective requirements.

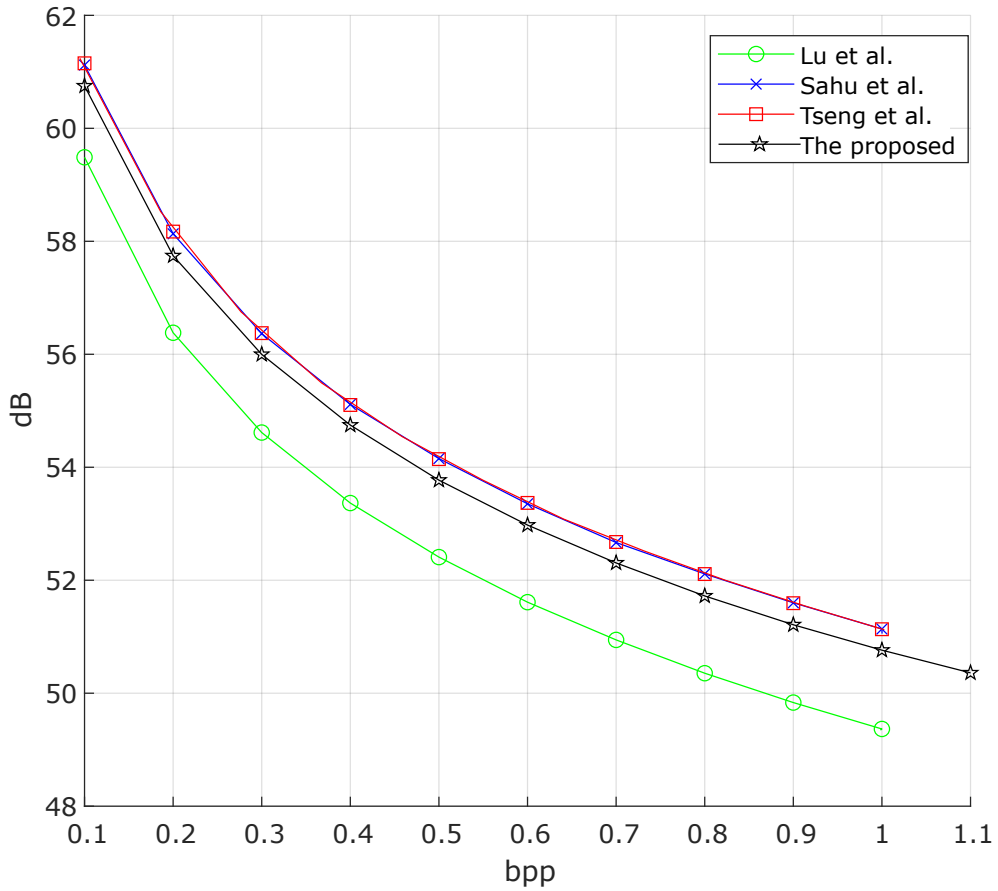


Figure 5. Comparative PSNR of SI_1 with different ERs for Lena image in different schemes [14,22,23].

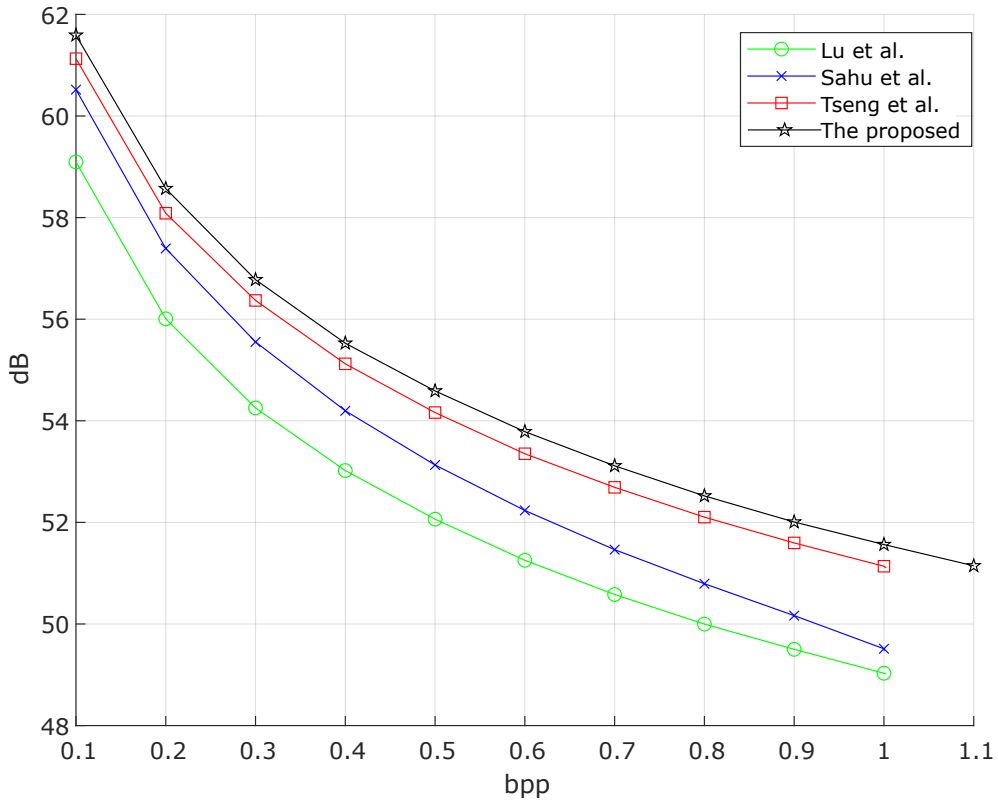
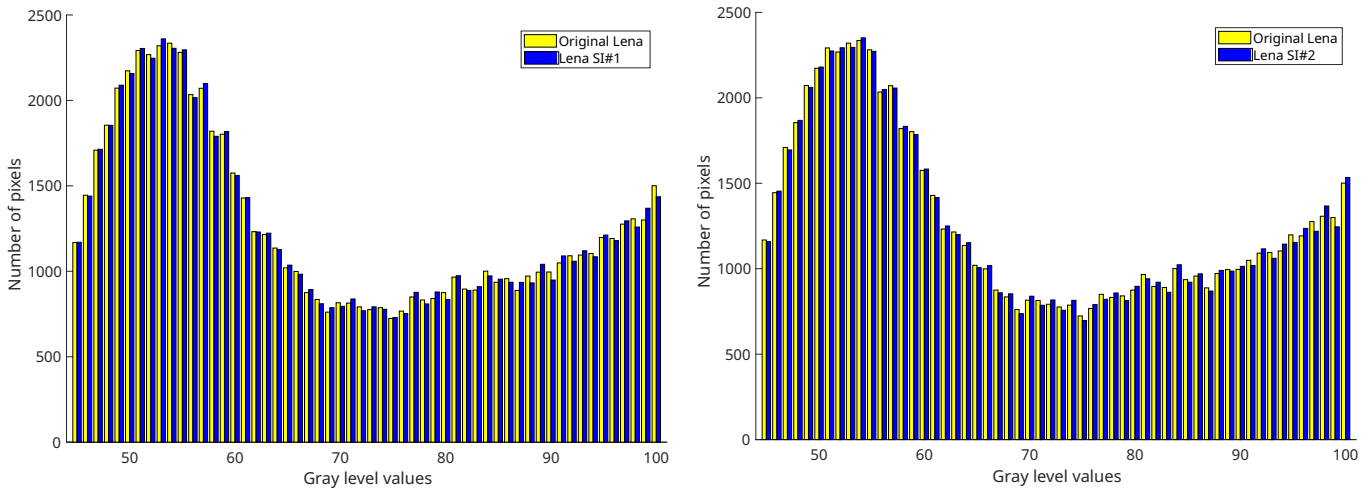


Figure 6. Comparative PSNR of SI_2 with different ERs for Lena image in different schemes [14,22,23].

Figure 7 expands on the traditional visual analysis by presenting detailed histograms comparing the original image of Lena with the two displayed images ΔI_1 and ΔI_2. This deliberate arrangement facilitates a direct visual comparison and provides a clear benchmark for evaluating the effectiveness of our data hiding methods. In particular, Figure 7a highlights the subtle differences between the histograms of the original image and that displayed in ΔI_1 . Similarly, Figure 7b provides a comprehensive comparison between the original image and that displayed in ΔI_2 , with both marked Lena images containing 50,000 hidden bits. As depicted in Figure 7a,b, the histogram of the displayed image closely matches the histogram of the original image with only minor deviations.

This observation validates the non-intrusive nature of our data hiding technique and clearly differentiates our approach from conventional data hiding methods. Our method, which efficiently conceals data while preserving the integrity of the original image's histogram, signifies a substantial advancement in the field of secure data embedding techniques. We underscore the adaptability of our method across a broad spectrum of applications in digital media security, prepared to lead innovation and enhance the safeguarding of digital communications. As we delve deeper into the realms of data hiding and digital image processing, we anticipate developing even more secure and efficient solutions in the future.

We elaborate on the methodology employed to augment the resilience of digital shadows against regular singular (RS) analysis attacks. Within the scope of RS analysis, a shadow is partitioned into the following three distinct subsets: the Regular subset (denoted as R_M or R_{-M}), the Singular subset (S_M or S_{-M}), and the Unaltered subset U. The terms R_M and S_M (or R_{-M} and S_{-M}) quantitatively denote the percentage of Regular and Singular subsets, which are masked by M or its complement $-M$, respectively.



(**a**) Histogram of left marked image

(**b**) Histogram of right marked image

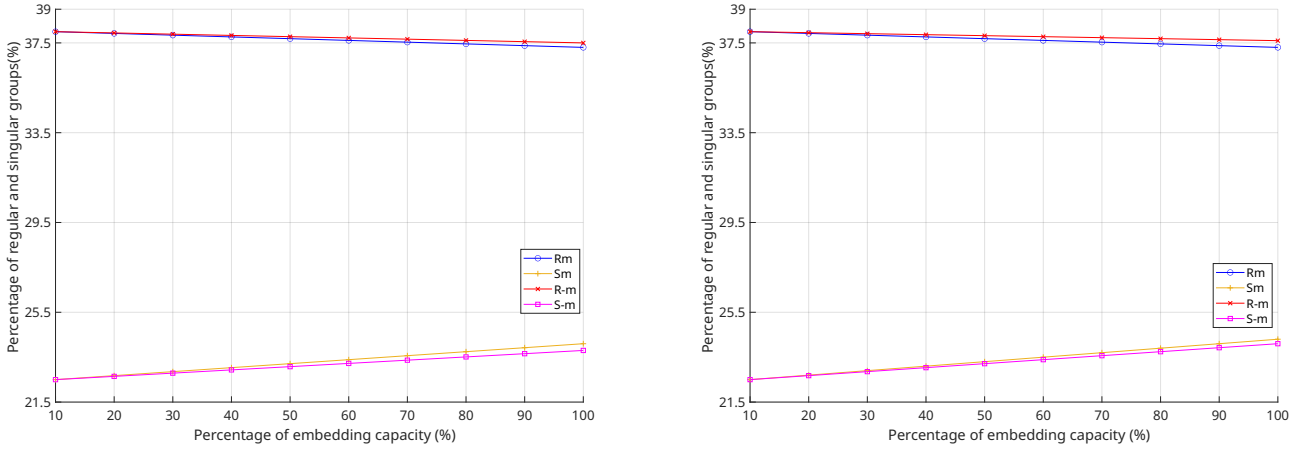
Figure 7. Comparison of histograms of the original Lena image and the two marked images.

The experimental framework is designed to group pixels into quartets and apply a mask M, which is defined by the matrix $[0, 1, 1, 0]$. This mask plays a crucial role in distinguishing between the Regular and Singular subsets. For a configuration to be considered as valid within the RS analysis paradigm, the interrelation between the Regular and Singular subsets must adhere to the constraints as outlined by Equations (9) and (10).

$$R_M + S_M \leq 1 \text{ and } R_{-M} + S_{-M} \leq 1 \tag{9}$$

$$R_M \cong R_{-M} \text{ and } S_M \cong S_{-M} \tag{10}$$

Figure 8 provides a visual accompaniment to the RS analysis for each shadow derived from the benchmark images 'Lena'.



(**a**) The RS chart of ΔI_1 (**b**) The RS chart of ΔI_2

Figure 8. The RS analysis for two stego images, ΔI_1 and ΔI_2, of Lena.

The RS analysis ensures that the following conditions are met: Firstly, $R_M + S_M \leq 1$: The sum of the regular and singular pixels under the influence of mask M should be less than or equal to one. This condition suggests that after the mask's application, the overall alteration to the image is minimized to reduce the likelihood of detection. Secondly, $R_M \approx R_{-M}$ and $S_M \approx S_{-M}$: The regular and singular pixels affected by the mask M should closely correspond to those affected by the inverse mask $-M$. This balance ensures the message's uniform distribution throughout the image, thereby preventing concentrations in any specific area that could facilitate detection. By adhering to these conditions, RS analysis enables the careful encoding of a message in an image while preserving its visual integrity. The approach effectively balances concealing information with the risk of image quality degradation due to alterations.

Given that the two marked images produced by our proposed method adhere to the RS analysis conditions, we have demonstrated our ability to maintain an optimal balance between the visual integrity of the image and the modifications required for image quality and data hiding.

5. Conclusions

In this study, we developed and evaluated an optimized strategy for reversible data hiding (RDH) utilizing an enhanced exploiting modification direction (EMD) method, which significantly improved the efficacy of the data hiding technique. By integrating the foundational principles of EMD with the benefits of reversibility, we achieved an exceptional data hiding rate of approximately 1.10 bits per pixel while also preserving the images' high visual fidelity. Moreover, we greatly reduced the visual and technical anomalies in stego images, safeguarding the integrity and quality of the concealed data. A distinguishing characteristic of our methodology is its ability to enable the flawless restoration of the original image without the need for any supplementary payload, marking a significant advancement over the existing RDH practices. The efficacy of our proposed technique was verified through empirical testing, involving rigorous comparisons with several cutting-edge methods. Looking ahead, we aim to further refine our approach, ensuring it remains theoretically sound, practically viable, and provides an all-encompassing solution for RDH endeavors in digital imaging.

The robustness of data hiding techniques in noisy environments is a critical research topic. This aspect is particularly useful for assessing resistance to various distortions that may occur due to external attacks or during the data transmission process. Therefore,

future research should aim to evaluate the robustness of the method presented in this study against noise, while also exploring solutions to overcome related limitations.

Author Contributions: Each author discussed the details of the manuscript. C.K. designed and wrote the manuscript. C.K. implemented the proposed technique and provided the experimental results. K.-H.J. and L.L. reviewed and revised the article. L.C.Q. drafted and revised the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Brain Pool program funded by the Ministry of Science and ICT through the National Research Foundation of Korea (2019H1D3A1A01101687) and Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2021R1I1A3049788) (K.-H.J.). This research was supported by the National Natural Science Foundation of China (61866028), Technology Innovation Guidance Program Project (Special Project of Technology Cooperation, Science and Technology Department of Jiangxi Province) (20212BDH81003) (L.L.).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Acknowledgments: We thank the anonymous reviewers for their valuable suggestions that improved the quality of this article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

DH	Data Hiding
RDH	Reversible Data Hiding
Dual RDH	Dual Reversible Data Hiding
EMD	Exploiting Modification Direction
I_1	Cover image (CI) 1
I_2	Cover image (CI) 2
ΔI_1	Stego image (SI) 1
ΔI_2	Stego image (SI) 2
x_i^1	a pixel of I_1, i.e., $x_i^1 \in I_1$
x_i^2	a pixel of I_2, i.e., $x_i^2 \in I_2$
$m = (m_1, m_2, \ldots, m_n)$	5-ary secret data
$N \times N$	Image Size
$f(x_1, x_2)$	Extraction function, $\sum_{i=1}^{N \times N}([x_i^1 \cdot 1 + x_i^2 \cdot 2])\ mod\ 5$
y_i^1	a pixel composed of SI 1
y_i^2	a pixel composed of SI 2
$y[]$	Vector for y
p_i	Average of the two pixels, y_i^1 and y_i^2
$s(= f)$	Extracted secret data

References

1. Petitcolas, F.A.; Anderson, R.J.; Kuhn, M.G. Information hiding—A survey. *Proc. IEEE* **1999**, *87*, 1062–1078. [CrossRef]
2. Provos, N.; Honeyman, P. Hide and seek: An introduction to steganography. *IEEE Secur. Priv.* **2003**, *1*, 32–44. [CrossRef]
3. Johnson, N.F.; Jajodia, S. Exploring steganography: Seeing the unseen. *Computer* **1998**, *31*, 26–34. [CrossRef]
4. Cheddad, A.; Condell, J.; Curran, K.; Kevitt, P.M. Digital image steganography: Survey and analysis of current methods. *Signal Process.* **2010**, *90*, 727–752. [CrossRef]
5. Tian, J. Reversible data embedding using a difference expansion. *IEEE Trans. Circuits Syst. Video Technol.* **2003**, *13*, 890–896. [CrossRef]
6. Ni, Z.; Shi, Y.Q.; Ansari, N.; Su, W. Reversible data hiding. *IEEE Trans. Circuits Syst. Video Technol.* **2006**, *16*, 354–362.
7. Weng, S.; Zhao, Y.; Pan, J.S.; Ni, R. Reversible data hiding based on a histogram modification mechanism: An overview. *J. Vis. Commun. Image Represent.* **2017**, *46*, 152–164.

8. 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]
9. Chan, C.K.; Cheng, L.M. Hiding data in images by simple LSB substitution. *Pattern Recognit.* **2004**, *37*, 469–474. [CrossRef]
10. Mielikainen, J. LSB matching revisited. *IEEE Signal Process. Lett.* **2006**, *13*, 285–287. [CrossRef]
11. Hiary, H.; Sabri, K.E.; Mohammed, M.S. A hybrid steganography system based on LSB matching and replacement. *Int. J. Adv. Comput. Sci. Appl.* **2016**, *7*, 374–380. [CrossRef]
12. Luo, W.; Huang, F.; Huang, J. Edge adaptive image steganography based on LSB matching revisited. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 201–214.
13. Wang, Y.L.; Shen, J.J.; Hwang, M.S. An improved dual image-based reversible hiding technique using LSB matching. *Int. J. Netw. Secur.* **2017**, *19*, 858–862.
14. 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]
15. Zhang, X.; Wang, S. Efficient steganographic embedding by exploiting modification direction. *IEEE Commun. Lett.* **2006**, *10*, 781–783. [CrossRef]
16. Yang, C.N.; Chou, Y.S.; Liu, Y.; Kim, C. Exploiting error control in matrix coding-based data. *J. Real-Time Image Process.* **2019**, *16*, 577–588. [CrossRef]
17. Chang, C.C.; Kieu, T.D.; Chou, Y.C. Reversible data hiding scheme using two steganographic images. In Proceedings of the IEEE Region 10 International Conference (TENCON), Taipei, Taiwan, 30 October–2 November 2007; pp. 1–4.
18. 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]
19. Chen, X.F.; Guo, W.L. Reversible data hiding scheme based on fully exploiting the orientation combinations of dual stego-images. *Int. J. Netw. Secur.* **2019**, *22*, 126–135.
20. Lin, J.Y.; Chen, Y.; Chang, C.C.; Hu, Y.C. Dual-image-based reversible data hiding scheme with integrity verification using exploiting modification direction. *Multimed. Tools Appl.* **2019**, *78*, 25855–25872. [CrossRef]
21. 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 3rd International Conference on Information, Communications and Signal Processing, Tainan, Taiwan, 10–13 December 2013; pp. 1–5.
22. Sahu, A.K.; Swain, G. Dual stego-imaging based reversible data hiding using improved LSB matching. *Int. J. Intell. Eng. Syst.* **2019**, *12*, 63–73. [CrossRef]
23. Tseng, H.W.; Leng, H.S. A reversible modified least significant bit (LSB) matching revisited method. *Signal Process. Image Commun.* **2022**, *101*, 116556. [CrossRef]
24. Lin, C.C.; Tsai, W.H. Secret image sharing with steganography and authentication. *J. Syst. Softw.* **2003**,*73*, 405–414. [CrossRef]
25. 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]
26. Image Databases. Available online: https://www.imageprocessingplace.com/root_files_V3/image_databases.htm (accessed on 5 January 2023).