symmetry

MDPI

Article

A Novel Reversible Data Hiding Algorithm Based on Enhanced Reduced Difference Expansion

Thai-Son Nguyen *, Van-Thanh Huynh and Phuoc-Hung Vo

School of Engineering and Technology, Tra Vinh University, Tra Vinh 87110, Vietnam
* Correspondence: thaison@tvu.edu.vn; Tel.: +84-90-781-9045

Abstract: Reversible data hiding is a data-hiding technique which has the ability to recover the original version from stego-images after the secret information is extracted. In this paper, we propose a novel reversible data-hiding scheme based on an enhanced reduced difference-expansion technique. In the proposed scheme, the original image is divided into non-overlapping quad-blocks for embedding data. Then, to enhance the security, the secret bits are encrypted based on the encryption key and a symmetry-based strategy. To improve embedding capacity further, two adjacent encrypted bits are converted into a corresponding decimal digit. Difference expansion (DE) technique is applied to embed a decimal form instead of a binary version. Moreover, to maintain the good image quality, the enhanced reduced difference-expansion technique is used to reduce the original difference values so that it is suitable for decimal embedding. The experimental results demonstrated that the proposed scheme has achieved better performance in comparison with previous solutions.

Keywords: reversible data hiding; difference expansion; enhanced reduced difference expansion

check for updates

Citation: 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. https://doi.org/10.3390/sym14081726

Academic Editor: Yu-Chi Chen

Received: 11 July 2022
Accepted: 11 August 2022
Published: 18 August 2022

1. Introduction

With the rapid development of computer networks and multimedia technology, digital information is transmitted on the network environment more conveniently. However, such digital information faces many risks related to security issues. To solve these issues, many cryptography techniques i.e., DES, AES and RSA [1], have been proposed. Cryptography techniques encrypt the digital information from plaintext to cipher text, leading to an increase in attention from attackers. Another promising solution is data-hiding techniques that conceal the confidential data into cover data, i.e., text, images, audio.... In the data-hiding schemes, imperceptibility must be considered. This means that the attacker cannot detect the secret information in the marked data. The data-hiding schemes can be classified into two different categories, i.e., irreversible and reversible data-hiding schemes. For an irreversible data-hiding scheme, only secret data can be extracted, while the restoration of the cover data is unavailable. In contrast, a reversible data-hiding (RDH) scheme can extract the secret data and recover the original cover images in the extracting process. In recent years, RDH schemes have received much attention from the research community [2–5]. RDH schemes are suitable in some sensitive scenarios, such as military, medical and forensic fields, where any permanent distortion is unacceptable, and the exact recovery of the original cover data is required. RDH schemes for digital images can be classified into three different domains, including: frequency, compression, and spatial domains [6–18].

In the frequency domain [6–9], the cover image is first transformed into frequency coefficients via various transform functions, i.e., discrete Fourier transform (DFT), discrete cosine transform (DCT), and discrete wavelet transform (DWT). In 2018, Vo et al. [6] proposed a 2D HS-based RDH scheme. In their scheme, the suitable quantized DCT (QDCT) coefficients are determined for embedding the secret data. As a result, their embedding capacity and image quality are improved further. Later on, Vo et al. proposed another algorithm [7] in the frequency domain. In [7], they applied both DCT and singular-value decomposition (SVD) mechanisms to embed watermarks for digital image copyright.

Compared with RDH schemes in the spatial domain, RDH schemes in the frequency domain are more complex in terms of the execution. However, the RDH schemes in the frequency domain maintain greater robustness against various malicious attacks. In the compression domain, the cover images are compressed to preserve the room for containing the secret data. Many RDH solutions for compressed images have been proposed in [10–13]. These schemes obtained a high embedding capacity. However, they offered an increase in file size when containing the secret data.

In the spatial domain, the RDH schemes can be divided into two categories: histogram-shifting (HS) based and difference-expansion (DE) based. In the HS-based category, in 2006, Ni et al. proposed a HS-based RDH scheme [15]. Ni et al.'s scheme embedded the secret bits by modifying the pairs of peak point and zero point. In the HS-based RDH technique, the embedding capacity depends on the height of the peak point bin of the histogram. Therefore, in order to increase the embedding capacity, many algorithms [16–18] have tried to generate a sharper histogram. The HS-based RDH techniques obtained a high embedding capacity for smooth images. However, they suffered a low embedding capacity for texture images. In the DE-based category, the attention of several researchers was attracted [14,19–28]. In 2003, Tian [14] proposed the first DE-based scheme. In [14], two adjacent pixels in the cover image are grouped into a pair. Then, the difference in pixels in the pair is computed and expanded to carry one secret bit. Therefore, the maximum embedding capacity in [14] can be obtained up to 0.5 bpp. To increase the embedding capacity, Alattar [19] proposed a new DE-based RDH scheme. Instead of using two adjacent pixels as was done in [14], in Alattar's scheme the cover image is divided into non-overlapping blocks with a size of 2 × 2 pixels. With four pixels in each block, up to three difference values are determined and expanded for embedding three secret bits. As a result, the higher embedding capacity is obtained in Alattar's scheme, up to 0.75 bpp. However, by doing so, the original pixels will be twice changed for containing the secret data, causing much distortion in the stego-images. To overcome this shortcoming, several improved solutions were proposed in [20–25]. To further improve the performance of Alattar's scheme, Liu et al. [20] proposed a novel DE-based RDH scheme by using a reduced difference expansion (RDE) algorithm. In their scheme, to minimum the modification, the difference value between pixels of the pair is reduced before embedding the secret bits. Liu et al.'s scheme obtained the better quality of stego-images. Later on, to improve embedding capacity further, a hybrid RDH scheme based on DE and HS techniques was proposed by Kukreja et al. [25]. In Kukreja et al.'s scheme, the cover image is divided into non-overlapping blocks with the size of a × b pixels. In each block, a × (b−1) difference values are calculated from a × b pixels of the block. Then, the histogram of these difference values is constructed for embedding the secret data by HS technique. According to the properties of 2 × 2 blocks, several RDE-based RDH schemes are proposed in [21–24]. In such schemes, different techniques are used to determine the suitable difference values for embedding data. The image blocks are divided into three different groups, i.e., (1) expandable, (2) changeable, and (3) unchangeable groups. To avoid overflow/underflow problems, only expandable and changeable groups are modified to carry secret bits. For the blocks belonging to the expandable group, the difference values, larger than one, are reduced to embed the secret data by using the RDE technique. For the blocks belonging to the changeable group, the original difference values are directly modified to embed secret data by the DE algorithm. By applying the RDE technique, these RDE-based RDH schemes [20–28] achieved the better image quality of stego-images. However, they offered a low embedding capacity, because each pair of pixels is used to carry only one secret bit.

In the DE-based and RDE-based RDH schemes, only one secret bit is embedded into the difference of the pixel pair. In this paper, to improve the embedding capacity while maintaining the good image quality, a novel RDH scheme is proposed by using the ERDE technique. In the proposed scheme, two determined thresholds are used to classify difference values and to determine how these difference values are to be processed to maintain the image quality. Then, more secret bits are embedded into small difference values. For other difference values, they are reduced. Further, to increase the embedding capacity, small, reduced difference values are used to conceal the secret bits while the others are kept unchanged to guarantee the good image quality of the stego-images.

The rest of the paper is organized as follows; we briefly introduce previous related works in Section 2. Then, Section 3 elaborates the proposed scheme. To evaluate the performance of the proposed scheme, experimental results are given in Section 4. Our conclusions are drawn in Section 5.

2. Related Works

2.1. Difference Expansion Scheme

In 2003, a DE-based RDH scheme was first proposed by Tian [14]. In Tian's scheme, the cover image is grouped into pair of pixels (p_1, p_2). Then, the difference value d and the average value m of a pair of pixels are computed using Equation (1).

$$d = p_1 - p_2 \qquad m = \left\lfloor \frac{p_1 + p_2}{2} \right\rfloor \tag{1}$$

where $\lfloor . \rfloor$ is the floor function to round a number down to the nearest integer.

Then, the secret data s is embedded by applying the expansion technique in Equation (2).

$$\overline{d} = 2 \times d + s \tag{2}$$

where $\overline{d}$ is the result of embedding process, and s is the embedded secret bit.

Finally, the new stego-pixel pair is updated according to Equation (3).

$$\overline{p}_1 = m + \frac{\overline{d} + 1}{2} \qquad \overline{p}_2 = m - \left\lfloor \frac{\overline{d}}{2} \right\rfloor \tag{3}$$

where $\overline{p}_1$ and $\overline{p}_2$ are two stego pixels after the embedding process.

In Tian's scheme, two cover pixels are used to carry only one secret bit; therefore, their maximum embedding capacity is approximately 0.5 bpp.

2.2. Reduced Difference Expansion Scheme

In the DE-based RDH schemes, for embedding, the difference value is expanded to generate the space to embed secret data. It means that, in these schemes, the original value is modified at least twice, causing the low image quality. To improve the embedding capacity, Lui et al. [20] introduced the new DE-based algorithm. In their scheme, the difference value of each pixel pair is calculated as was done in [14,19]. Then, the original difference value is reduced according to Equation (4).

$$\overline{v}_i = \begin{cases} v_i - 2^{log_2|v_i|-1}, & if|v_i| > 1 \\ v_i, & \text{otherwise} \end{cases} \tag{4}$$

where v_i and $\overline{v}_i$ are original and reduced difference values, respectively. Then, each reduced difference value is used to hide one secret bit.

By using the RDE algorithm for embedding data, Liu et al.'s scheme improved the image quality of stego-images. However, their embedding capacity is still low, when it is equal to 0.5 bpp.

3. Proposed Algorithm

In this section, our DE-based RDH algorithm is presented in detail. To improve the embedding capacity and the image quality, the two following techniques are applied in the proposed scheme.

(1) Secret message encoding: For fair comparison, the generated secret data, based on the symmetry concept, means the secret bits should be random and the distribution of the secret data remains uniform. Then, two adjacent bits of the secret data are converted into decimal form.
(2) The ERDE technique: Each original difference value of the pixel pair is reduced before expanding for data embedding.

In the proposed scheme, the cover image is divided into 2 × 2 non-overlapping blocks. In each of these blocks, the smallest pixel is used as a base point to compute the difference values (DV). Next, the determined threshold T1 is used to classify which DV values are to be embedded or to be reduced. If the DV values are larger than T1, the ERDE technique is used to narrow the DV value for embedding data. Moreover, to maintain the tradeoff between the embedding capacity and the image quality in the data-embedding process, the second threshold T2 is used. If DVs of a block after reducing are smaller than T2, they are used for embedding secret bits. Otherwise, they are kept unchanged. The flowchart of our proposed scheme is presented in Figure 1.

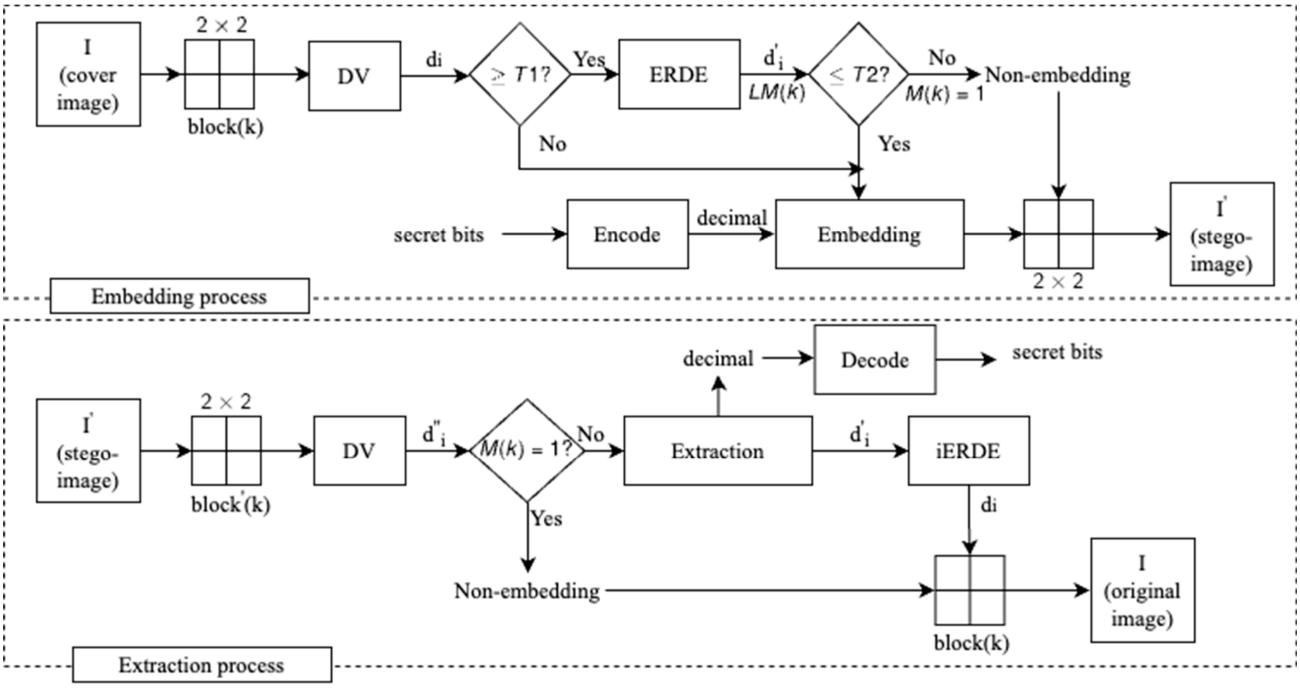


Figure 1. The flowchart of the proposed scheme.

The data embedding and extraction procedure are described in detail as follows:

3.1. The Data Embedding Procedure

To embed the message S into the cover image I, the eight following steps are used in the data-embedding algorithm:

Step 1. Encode the message S into an integer sequence B with L elements, $B = b_{i\in\{0\ldots L-1\}}$. Two adjacent bits in S is converted into the integer value b_i; therefore, $b_i \in (0,\ 1,\ 2,\ 3)$.

Step 2. Divide the cover image I into quad blocks of the size of 2 × 2 as shown in Figure 2. Each block is then converted into a vector, which is given as $p = (p_0,\ p_1,\ p_2,\ p_3)$.

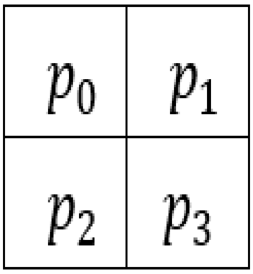


Figure 2. The block of quad pixels.

Step 3. Determine the minimum value by sorting the vector p in assending order. Obtain the vector $u_i = (u_0,\ u_1, u_2,\ u_3)$, with $u_0 \leq\ u_1 \leq u_2 \leq\ u_3$

Step 4. Compute the difference value d_i by using Equation (5).

$$\begin{cases} d_1 = u_1 - u_0 \\ d_2 = u_2 - u_0 \\ d_3 = u_3 - u_0 \end{cases} \tag{5}$$

where $u_0,\ u_1, u_2$ and u_3 are four pixels of the quad block, and d_i is the difference between two pixels.

Step 5. Enhance the reduced difference value: A threshold T1 is given to determine whether d_i should be reduced or not. In the proposed scheme, if the difference is less than a given threshold T1, we use the original difference for data embedding without reduction. Otherwise, if $d_i \geq$ T1, this difference value d_i is reduced by using the ERDE technique according to Equation (6). Otherwise, this original difference value is unchanged and moves to Step 6.

$$\overline{d}_i = \begin{cases} d_i - 2^{n-1},\ if\ 2^n \leq d_i \leq 2^n + 1 \\ d_i - \left(2^{n-1} + 2\right),\ if\ 2^n + 2 \leq d_i \leq 3 \times 2^{n-1} - 1 \\ d_i - 2^n,\ if\ 3 \times 2^{n-1} \leq d_i \leq 3 \times 2^{n-1} + 1 \\ d_i - (2^n + 2),\ if\ 3 \times 2^{n-1} + 2 \leq d_i \leq 4 \times 2^{n-1} - 1 \end{cases} \tag{6}$$

where d_i and $\overline{d}_i$ are the original and reduced difference values of two pixels, respectively, and $n = \lfloor log_2 d_i \rfloor$.

To effectively extract data and restore the original image, the location map LM is constructed according to Equation (7).

$$LM = \begin{cases} 0,\ \ if\ 2^n \leq d_i \leq 2^n + 1 \\ 1,\ \ if\ 2^n + 2 \leq d_i \leq 3 \times 2^{n-1} - 1 \\ 2,\ \ if\ 3 \times 2^{n-1} \leq d_i \leq 3 \times 2^{n-1} + 1 \\ 3,\ \ if\ 3 \times 2^{n-1} + 2 \leq d_i \leq 4 \times 2^{n-1} - 1 \end{cases} \tag{7}$$

where d_i is the original difference value of two pixels, and $n = \lfloor log_2 d_i \rfloor$.

Step 6. Data embedding: A threshold T2 is given to determine whether the reduced difference $\overline{d}_i$ is suitable to embed the secret data or not.

If $\overline{d}_i \ \leq$ T2, $\overline{d}_i$ is expanded to embed the secret value b_i according to Equation (8). Otherwise, $\overline{d}_i$ is non-embeddable and the coordinate of this block is recorded into the vector M by setting $M(\mathrm{k}) = 1$, where k is the k^{th} block.

$$\overline{\overline{d}}_i = 2^2 \times \overline{d}_i + b_i \tag{8}$$

where $\overline{\overline{d}}_i$ is the result of the difference value after te embedding process, and b_i is the secret data, and $b_i \in (0,\ 1,\ 2,\ 3)$

Step 7. The new vector $\overline{u}_i$ is updated by using Equation (9).

$$\begin{cases} \overline{u}_0 = u_0 \\ \overline{u}_1 = u_0 + \overset{=}{d}_1 \\ \overline{u}_2 = u_0 + \overset{=}{d}_2 \\ \overline{u}_3 = u_0 + \overset{=}{d}_3 \end{cases} \tag{9}$$

where $\overline{u}_0$, $\overline{u}_1$, $\overline{u}_2$ and $\overline{u}_3$ are four stego-pixels after data embedding.

After updating according to Equation (9), if the value of $\overline{u}_i$ is less than 0 or greater than 255, overflow/underflow problems have occurred. In this case, this block is also not suitable for data embedding. Then, the block should be unchanged, and the coordinate of the block is recorded in the vector M in the same way as in Step 6. Otherwise, the new vector $\overline{u}_i$ is converted into the corresponding positions of 2 × 2 blocks.

Step 8. Repeat the above steps until the whole secret bits are embedded. Then, the stego-image I' is obtained. Subsequently, the extra information LM and M is compressed and sent to the receiver via a secure channel.

3.2. The Data Extraction Procedure

The extraction procedure on the contrary does simply the reverse of the embedding procedure. First, the extra information LM and M, which is received from the sender, is used for extracting. The extraction and recovery process is present in the steps below.

Step 1. Divide the stego-image I' into quad blocks with the size of 2 × 2. Each block is converted into the vector $\overline{u}_i$ as Steps 2 and 3 in the embedding procedure. Then, compute the difference value $\overset{=}{d}_i$ of the pixel pairs by using Equation (5).

Step 2. Extract the data B: The integer value b_i is extracted by using Equation (10).

$$b_i = \overset{=}{d}_i \; mod \; 2^2 \tag{10}$$

where *mod* is the function to return the remainder after a number is divided by a divisor.

Step 3. Restore the difference value $\overset{=}{d}_i$ in Equation (11).

$$\overline{d}_i = \left\lfloor \frac{\overset{=}{d}_i}{2^2} \right\rfloor \tag{11}$$

where $\overline{d}_i$ is the reconstructed difference value.

Step 4. If $M(k) = 1$, the k^{th} block is a non-embeddable block. Otherwise, the secret data is extracted, and this block is reconstructed as below.

According to the location map LM, the difference value d_i is recovered by using the iERDE technique in Equation (12); otherwise, d_i is equal to $\overline{d}_i$.

$$d_i = \begin{cases} \overline{d}_i + 2^n, \; if \text{ LM} = 0 \\ \overline{d}_i + 2^n + 2, \; if \text{ LM} = 1 \\ \overline{d}_i + 2^{n+1}, \; if \text{ LM} = 2 \\ \overline{d}_i + 2^{n+1} + 2, \; if \text{ LM} = 3 \end{cases} \tag{12}$$

where $n = \left\lfloor log_2 \overline{d}_i \right\rfloor$, and d_i is the difference after restoration to the original difference.

Step 5. Restore the original vector u_i by using Equation (13).

$$\begin{cases} u_0 = \overline{u}_0 \\ u_1 = \overline{u}_0 + d_1 \\ u_2 = \overline{u}_0 + d_2 \\ u_3 = \overline{u}_0 + d_3 \end{cases} \tag{13}$$

where $u_0,\ u_1, u_2$ and u_3 are four restored pixels of the quad block.

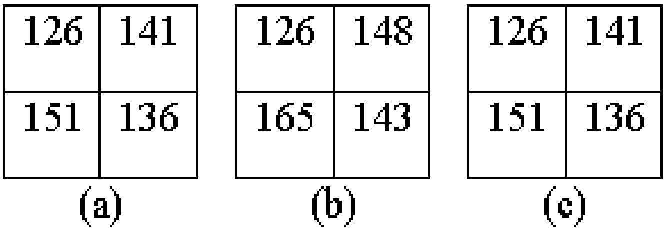
Then, the vector u_{i} is converted into the corresponding positions in the current block.

Step 6. Repeat the above steps until the whole blocks are processed completely. The original image is obtained. Then, each extracted value b_i is converted into two secret bits. The message S is conducted by concatenating two bits into the original string.

3.3. Example of the Proposed Scheme

3.3.1. An Example of the Embedding Process

Assume that the quad block of the grayscale image *I* is shown in Figure 3a. Allow two thresholds, T1 = 2 and T2 = 10; the example of the embedding process is presented as follows:



126	141
151	136

(a)

126	148
165	143

(b)

126	141
151	136

(c)

Figure 3. An example of a quad block for data embedding and extraction process. (**a**) Before embedding; (**b**) After embedding; (**c**) After extraction.

Step 1. Encode the message: Assume that the binary secret bits, $S =$ ′011011′, is embedded. Then, it is encoded into the integer values $B =$ ′1 2 3′

Step 2. Transform the block into the vector $p = (126,\ 141,\ 151,\ 136)$

Step 3. Sort the vector p in an ascending order to obtain vector $u = (126,\ 136,\ 141,\ 151)$

Step 4. Compute the difference values d_i by using Equation (5).

$$\begin{cases} d_1 = 136 - 126 = 10 \\ d_2 = 141 - 126 = 15 \\ d_3 = 151 - 126 = 25 \end{cases}$$

Step 5. The given threshold T1 $= 2$, so $d_{\mathrm{i}} \geq$ T1. Then, reduce the difference value d_i by using Equation (6).

$$n = \lfloor log_2 d_{\mathrm{i}} \rfloor = \lfloor log_2 10 \rfloor = 3,\ then,\ 2^3 \leq 10 \leq 2^3 + 1$$
$$\overline{d}_1 = d_i - (2^{n-1} + 2) = 10 - (2^{3-1} + 2) = 4$$
$$LM = 1$$
$$n = \lfloor log_2 d_{\mathrm{i}} \rfloor = \lfloor log_2 15 \rfloor = 3,\ then,\ 3 \times 2^{3-1} + 2 \leq 15 \leq 4 \times 2^{3-1} - 1$$
$$\overline{d}_2 = d_i - (2^n + 2) = 15 - (2^3 + 2) = 5$$
$$LM = 3$$
$$n = \lfloor log_2 d_{\mathrm{i}} \rfloor = \lfloor log_2 25 \rfloor = 4,\ then,\ 3 \times 2^{4-1} \leq 25 \leq 3 \times 2^{4-1} + 1$$
$$\overline{d}_3 = d_i - 2^n = 25 - 2^4 = 9LM = 2$$

Step 6. Embed the data: If $\overline{d}_i \leq$ T2, then $\overline{d}_i$ are expanded to embed the secret data by using Equation (8).

$$\overline{\overline{d}}_1 = 2^2 \times \overline{d}_1 + b_1 = 2^2 \times 4 + 1 = 17$$
$$\overline{\overline{d}}_2 = 2^2 \times \overline{d}_2 + b_2 = 2^2 \times 5 + 2 = 22\overline{\overline{d}}_3 = 2^2 \times \overline{d}_3 + b_3 = 2^2 \times 9 + 3 = 39$$

Step 7. Update the new vector $\overline{u}_i$ using Equation (9)

$$\begin{cases} \overline{u}_0 = u_0 = 126 \\ \overline{u}_1 = u_0 + \bar{\bar{d}}_1 = 126 + 17 = 143 \\ \overline{u}_2 = u_0 + \bar{\bar{d}}_2 = 126 + 22 = 148 \\ \overline{u}_3 = u_0 + \bar{\bar{d}}_3 = 126 + 39 = 165 \end{cases}$$

Step 8. Reverse the convert vector $\overline{u}_i$ into the correct corresponding positions of the stego-block as shown in Figure 3b.

3.3.2. An Example of the Extraction Process

Step 1. First, the stego-block is transformed into the vector $\overline{p}$. Next, sort the vector p in ascending order to obtain the vector $\overline{u} = (126,\ 143,\ 148,\ 165)$. Then, calculate the difference values $\bar{\bar{d}}_i$ by using Equation (5).

$$\begin{cases} \bar{\bar{d}}_1 = 143 - 126 = 17 \\ \bar{\bar{d}}_2 = 148 - 126 = 22 \\ \bar{\bar{d}}_3 = 165 - 126 = 39 \end{cases}$$

Step 2. Extract the embedded data B. The integer values b_i are extracted in Equation (10).

$$\begin{gathered} b_1 = \bar{\bar{d}}_1 \ mod\ 2^2 = 17\ mod\ 4 = 1 \\ b_2 = \bar{\bar{d}}_2 \ mod\ 2^2 = 22\ mod\ 4 = 2 \\ b_3 = \bar{\bar{d}}_3 \ mod\ 2^2 = 39\ mod\ 4 = 3 \end{gathered}$$

Convert a sequence of the integer values $B = {}'1\ 2\ 3'$ into the original secret bits $S = {}'011011'$

Step 3. Restore the difference values $\overline{d}_i$ by using Equation (11)

$$\overline{d}_1 = \left\lfloor \frac{\bar{\bar{d}}_1}{2^2} \right\rfloor = \left\lfloor \frac{17}{2^2} \right\rfloor = 4\overline{d}_2 = \left\lfloor \frac{\bar{\bar{d}}_2}{2^2} \right\rfloor = \left\lfloor \frac{22}{2^2} \right\rfloor = 5\overline{d}_3 = \left\lfloor \frac{\bar{\bar{d}}_3}{2^2} \right\rfloor = \left\lfloor \frac{39}{2^2} \right\rfloor = 9$$

Step 4. Calculate the original difference values d_i by using Equation (12).

$$\begin{gathered} n = \left\lfloor log_2 \overline{d}_1 \right\rfloor = \lfloor log_2 4 \rfloor = 2 \\ \text{LM} = 1 \\ d_1 = \overline{d}_1 + 2^n + 2 = 4 + 2^2 + 2 = 10 \\ n = \left\lfloor log_2 \overline{d}_2 \right\rfloor = \lfloor log_2 5 \rfloor = 2 \\ \text{LM} = 3 \\ d_2 = \overline{d}_i + 2^{n+1} + 2 = 5 + 2^{2+1} + 2 = 15 \\ n = \left\lfloor log_2 \overline{d}_3 \right\rfloor = \lfloor log_2 9 \rfloor = 3 \\ \text{LM} = 2 \\ d_3 = \overline{d}_i + 2^{n+1} = 9 + 2^{3+1} = 25 \end{gathered}$$

Step 5. Restore the original vector u_{i} using Equation (13).

$$\begin{cases} u_0 = \overline{u}_0 = 126 \\ u_1 = \overline{u}_0 + d_1 = 126 + 10 = 136 \\ u_2 = \overline{u}_0 + d_2 = 126 + 15 = 141 \\ u_3 = \overline{u}_0 + d_3 = 126 + 25 = 151 \end{cases}$$

Finally, convert the vector u_{i} into correctly corresponding positions of the original block as shown in Figure 3c.

4. Experimental Results

In this section, we present the experimental results of the proposed scheme. These results are experimented on ten common grayscale images. All the images are 512 × 512 with different complexity including Lena, Baboon, Peppers, Barbara, Airplane, Boat, Lake, Livingroom, Pirate and Woman, as shown in Figure 4. The experimental environment is MATLAB R2014a running on Microsoft Windows 10 Professional 64-bits, and the processor platform is an Intel(R) Core (TM) i7-8700U CPU (12MB Cache, 3.20 GHz), 8 GB of RAM DDR4 memory.

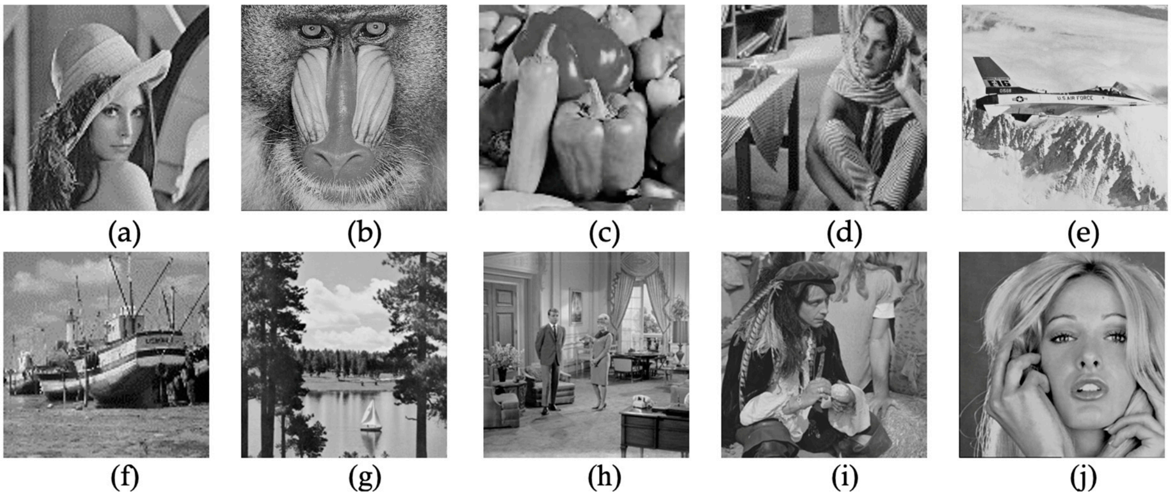


Figure 4. Experimental image dataset. (**a**) Lena; (**b**) Baboon; (**c**) Peppers; (**d**) Barbara; (**e**) Airplane; (**f**) Boat; (**g**) Lake; (**h**) Livingroom; (**i**) Pirate; (**j**) Woman.

The proposed scheme achieves high performance in terms of the embedding capacity and the visual quality. In this scheme, the message in binary form is first converted into decimal form, then one decimal is embedded into each difference value. Due to one decimal value being equal to two bits, the bit rate of the proposed scheme would certainly improve twice compared to previous schemes. This is becauese only one secret bit is embedded into the pixel pair in previous schemes. In their scheme, the expansion of difference values for embedding decimal values may lead to a negative impact on the image quality and there will also be overflow/underflow problems. To solve this problem, we proposed a new algorithm to reduce the original difference value using an improved ERDE technique. In the proposed ERDE technique, the difference value is minimum modified to embed the secret decimal value. It means the large amounts of secret bits can be embedded while maintaining good imperceptibility and avoiding the overflow/underflow problems.

To compare the image quality, the peak signal-to-noise ratio (PSNR) is used to calculate the visual similarity between a cover image and a stego-image. The PSNR is calculated as Equation (14).

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

where MSE is the mean squared error representing the difference between the cover image and stego-image and is calculated as Equation (15).

$$MSE = \frac{1}{m \times n}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(p_{i,j} - \overline{p}_{i,j}\right)^2 \tag{15}$$

with m and n as the height and width of the image, respectively, and $p_{i,j}$ and $\overline{p}_{i,j}$ refer to the pixels coordinate at the ith row and jth column of the cover image and stego-image, respectively.

Beside the PSNR, the embedding capacity (EC) and bit per pixel (bpp) are also common factors to evaluate the performance of the RDH schemes. The EC is the number of bits which are embedded inside the cover image. The bpp is determined based on the rate of bits which is embedded into one pixel.

To improve the PSNR value, we applied the proposed ERDE algorithm with an optimal reduced threshold T1. In our experiment, with T1 equal to 2, the ERDE scheme achieves the best performance. In the proposed scheme, the difference values are first reduced by ERDE technique, and then two bits are encoded into decimal and embedded into one reduced value. This leads to the proposed scheme to improve the embedding capacity while maintaining a good visual image. Additionally, to prevent the overflow/underflow problems, the embedding threshold T2 is used to decide whether a block is embeddable or non-embeddable. The block is embeddable if the difference value of this block is smaller than or equal to T2; otherwise, this block is ignored. Depending on the length of the secret data, the value of T2 is selected accordingly. A large value of T2 means more data to be embedded and more distortion in the cover image. Moreover, if T2 is too large, overflow/underflow problems may occur. In the experiment, we try to test several T2 with values of 2, 4, 6, 8, 10. Table 1 shows overflow/underflow blocks of common images with T2 = 10 and T2 = 12.

Table 1. The number of block overflows/underflows with T2 = 10 and T2 = 12.

	T2 = 10		**T2 = 12**	
Image	**EC**	**Overflow/Underflow**	**EC**	**Overflow/Underflow**
Airplane	344,418	0	353,694	0
Baboon	191,622	0	219,486	0
Barbara	271,452	0	288,108	90
Boat	323,526	0	341,418	43
Lena	357,756	0	367,344	1
Peppers	352,740	0	364,590	0
Lake	308,364	0	327,192	7
Livingroom	311,316	13	330,630	18
Pirate	328,236	0	344,916	0
Woman	330,234	0	345,768	0

To evaluate how the threshold T2 impacts on PSNR and EC, the Figure 5 shows the embedding capacity and the image quality of the Lena image with different values of T2. We see that when T2 is increased, the number of embedded bits significantly increases. However, the quality of the stego-image Lena decreases.

To evaluate the performance of the proposed scheme, the comparison of the embedding capacity and image quality between the proposed scheme and previous schemes, including Arham et al.'s scheme [22], Ntahobari & Ahamd's scheme [23] and Maniriho et al.'s scheme [28], are shown in Table 2. It can be seen in Table 2, with T2 = 12, that the proposed scheme achieves higher embedding capacity than T2 = 10. However, the overflow/underflow problems will occur in some images with T2 = 12. In the proposed scheme, the best result of EC and PSNR is obtained when the value of T2 is in the range of [2, 10].

In the proposed scheme, each difference value can embed two bits after applying the ERDE technique. As a result, our average embedding capacity of all test images is up to 311,966 bits, whereas the EC of Arham et al. [22], Ntahobari & Ahamd scheme [23], and Maniriho et al.'s scheme [28] is 177,924 bits, 185,284 bits and 242,146 bits, respectively. Although the EC increased by 68%, the proposed scheme also achieves a better visual image than that of Ntahobari & Ahamd's scheme, which reached 33.43 dB and 31.95 dB, respectively. From Table 2, the PSNR value of the proposed scheme slightly decreased compared to Arham et al.'s scheme with maximum data embedding. However, when two schemes are embedded the same embedding capacity, the PSNR value of the proposed scheme is always better than that of Arham et al.'s scheme.

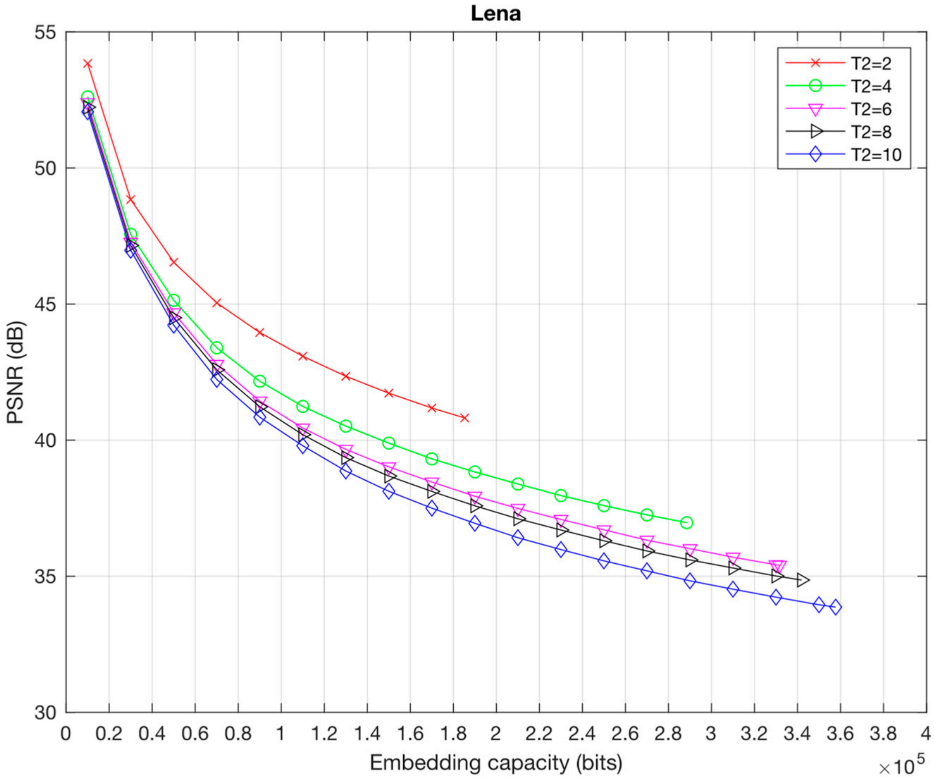
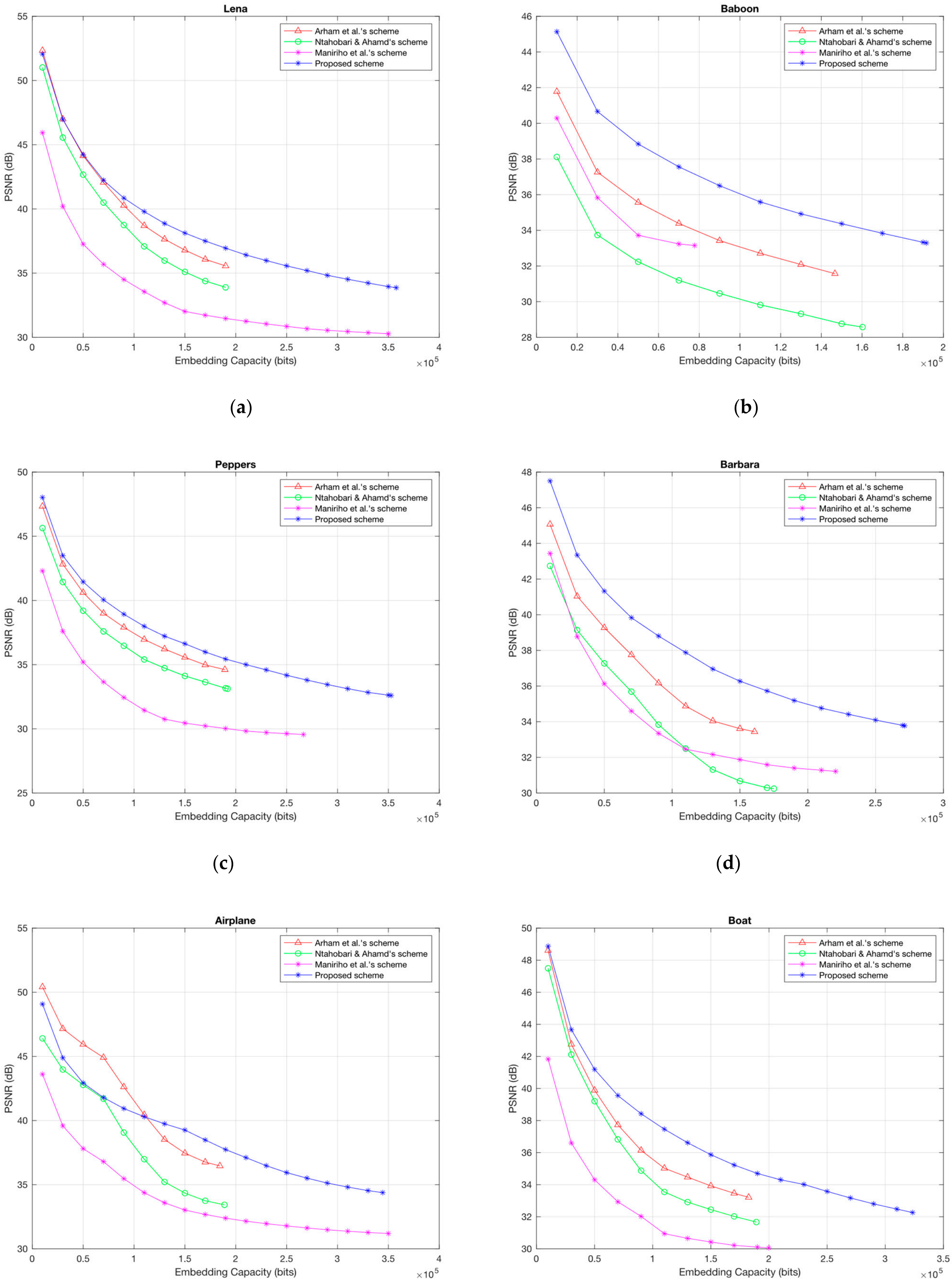


Figure 5. The EC and PSNR comparison of Lena image with different T2.

Table 2. The EC (bit) and PSNR (dB) comparison between the proposed and previous schemes.

Images	**Arham et al. [22]**		**Ntahobari & Ahamd [23]**		**Maniriho et al. [28]**		**Proposed (T2 = 10)**			
	EC	**PSNR**	**EC**	**PSNR**	**EC**	**PSNR**	**EC**	**PSNR**	**EC**	**PSNR**
Airplane	184,359	36.46	188,886	33.43	371,124	31.11	184,359	37.94	344,418	34.38
Baboon	146,682	31.57	160,272	28.58	77,709	33.15	146,682	34.45	191,622	33.29
Barbara	160,749	33.44	175,044	30.25	220,575	31.22	160,749	35.97	271,452	33.77
Boat	182,475	33.21	189,123	31.67	199,782	30.06	182,475	34.86	323,526	32.26
Lena	190,743	35.55	194,070	33.80	356,856	30.25	190,743	36.93	357,756	33.87
Peppers	189,306	34.61	191,976	33.13	266,493	29.56	189,306	35.46	352,740	32.60
Lake	179,448	36.24	186,552	34.02	214,215	33.61	179,448	38.12	308,364	35.74
Livingroom	178,416	33.39	187,404	30.74	208,800	30.27	178,416	35.02	311,316	32.54
Pirate	184,083	33.80	190,401	31.83	263,034	30.48	184,083	35.46	328,236	32.97
Woman	182,982	34.06	189,108	32.04	242,868	29.86	182,982	35.25	330,234	32.91
Average	177,924	34.23	185,284	31.95	242,146	30.96	177,924	35.95	311,966	33.43

To demonstrate the outstanding effectiveness of the proposed scheme, the PSNR comparison in dB between the proposed scheme and previous schemes is shown in Figure 6a–j. From the graph, we can see that in most cases, the proposed scheme is better than the other schemes with the same embedding capacity rate. Moreover, the proposed scheme can obtain a much higher maximum EC than previous schemes. For example, the EC of the proposed scheme for the Lena image is greater than 350,000 bits. However, for Arham et al.'s scheme [22] and Ntahobari & Ahamd's scheme [23], the EC is only around 190,000 bits and 194,000 bits, respectively.

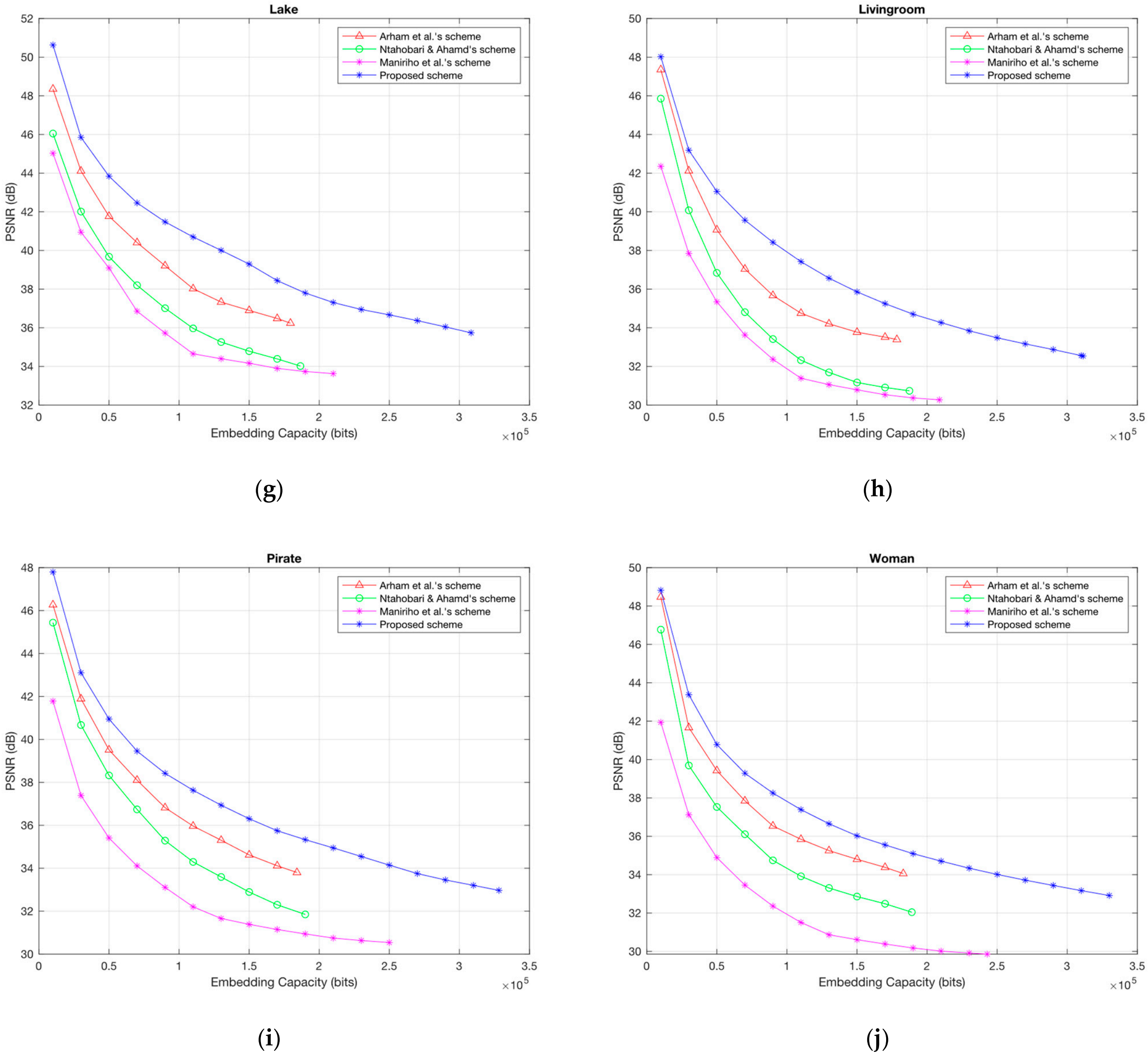


(**a**) (**b**)

(**c**) (**d**)

(**e**) (**f**)

Figure 6. *Cont.*



(**g**)

(**h**)

(**i**)

(**j**)

Figure 6. The PSNR comparison between the proposed scheme and three previous schemes. (**a**) Lena; (**b**) Baboon; (**c**) Peppers; (**d**) Barbara; (**e**) Airplane; (**f**) Boat; (**g**) Lake; (**h**) Livingroom; (**i**) Pirate; (**j**) Woman.

5. Conclusions

In this paper, we propose a new RDH scheme based on enhanced reduced difference expansion of a quad-block. In the proposed scheme, the ERDE technique is used to reduce the original difference value and the secret data are encoded into decimal values for embedding. Experimental results show that the proposed scheme achieves high performance in terms of the embedding capacity and the image quality in comparison with previous works. Moreover, by using the ERDE technique, the proposed scheme could avoid the overflow/underflow problems. In addition, the proposed scheme ensures reversibility and can be applied to special fields such as medical, military, and digital forensics.

Author Contributions: Conceptualization, T.-S.N. and V.-T.H.; methodology, T.-S.N.; software, V.-T.H.; validation, T.-S.N., V.-T.H. and P.-H.V.; formal analysis, V.-T.H.; investigation, T.-S.N.; resources, T.-S.N.; data curation, V.-T.H.; writing—original draft preparation, V.-T.H.; writing—review and editing, T.-S.N. and P.-H.V.; visualization, V.-T.H.; supervision, T.-S.N.; project administration, T.-S.N.; funding acquisition, T.-S.N. All authors have read and agreed to the published version of the manuscript.

Funding: This study was fully supported by the Tra Vinh University under grant contract number 211/HĐ.HĐKH—ĐHTV.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data available on request.

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

References

1. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
2. Jung, K.-H. A Survey of Reversible Data Hiding Methods in Dual Images. *IETE Tech. Rev.* **2016**, *33*, 441–452. [CrossRef]
3. Arai, E.; Imaizumi, S. High-Capacity Reversible Data Hiding in Encrypted Images with Flexible Restoration. *J. Imaging* **2022**, *8*, 176. [CrossRef] [PubMed]
4. Chang, C.-C.; Su, G.-D.; Lin, C.-C.; Li, Y.-H. Position-Aware Guided Hiding Data Scheme with Reversibility and Adaptivity for Dual Images. *Symmetry* **2022**, *14*, 509. [CrossRef]
5. Yu, C.; Zhang, X.; Li, G.; Zhan, S.; Tang, Z. Reversible data hiding with adaptive difference recovery for encrypted images. *Inf. Sci.* **2022**, *584*, 89–110. [CrossRef]
6. Vo, P.-H.; Nguyen, T.-S.; Huynh, V.-T.; Do, T.-N. A novel reversible data hiding scheme with two-dimensional histogram shifting mechanism. *Multimed. Tools Appl.* **2018**, *77*, 28777–28797. [CrossRef]
7. Vo, P.H.; Nguyen, T.S.; Huynh, V.T.; Do, T.N. A robust hybrid watermarking scheme based on DCT and SVD for copyright protection of stereo images. In Proceedings of the 2017 4th NAFOSTED Conference on Information and Computer Science, Hanoi, Vietnam, 24–25 November 2017; pp. 331–335.
8. Nguyen, T.-S. Fragile watermarking for image authentication based on DWT-SVD-DCT techniques. *Multimed. Tools Appl.* **2021**, *80*, 25107–25119. [CrossRef]
9. Nguyen, T.-S.; Chang, C.-C.; Yang, X.-Q. A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain. *AEU—Int. J. Electron. Commun.* **2016**, *70*, 1055–1061. [CrossRef]
10. Di, F.; Zhang, M.; Huang, F.; Liu, J.; Kong, Y. Reversible data hiding in JPEG images based on zero coefficients and distortion cost function. *Multimed. Tools Appl.* **2019**, *78*, 34541–34561. [CrossRef]
11. Xie, X.-Z.; Lin, C.-C.; Chang, C.-C. A reversible data hiding scheme for JPEG images by doubling small quantized AC coefficients. *Multimed. Tools Appl.* **2019**, *78*, 11443–11462. [CrossRef]
12. Liu, Y.; Chang, C.-C. Reversible data hiding for JPEG images employing all quantized non-zero AC coefficients. *Displays* **2018**, *51*, 51–56. [CrossRef]
13. Hou, D.; Wang, H.; Zhang, W.; Yu, N. Reversible data hiding in JPEG image based on DCT frequency and block selection. *Signal Process.* **2018**, *148*, 41–47. [CrossRef]
14. Tian, J. Reversible data embedding using a difference expansion. *IEEE Trans. Circuits Syst. Video Technol.* **2003**, *13*, 890–896. [CrossRef]
15. Ni, Z.; Shi, Y.; Ansari, N.; Su, W. Reversible data hiding. *IEEE Trans. Circuits Syst. Video Technol.* **2006**, *16*, 354–362. [CrossRef]
16. Fu, D.-S.; Jing, Z.-J.; Zhao, S.-G.; Fan, J. Reversible data hiding based on prediction-error histogram shifting and EMD mechanism. *AEU—Int. J. Electron. Commun.* **2014**, *68*, 933–943. [CrossRef]
17. Rad, R.M.; Wong, K.; Guo, J.-M. Reversible data hiding by adaptive group modification on histogram of prediction errors. *Signal Process.* **2016**, *125*, 315–328. [CrossRef]
18. Pan, Z.; Hu, S.; Ma, X.; Wang, L. Reversible data hiding based on local histogram shifting with multilayer embedding. *J. Vis. Commun. Image Represent.* **2015**, *31*, 64–74. [CrossRef]
19. Alattar, A.M. Reversible watermark using difference expansion of quads. In Proceedings of the 2004 IEEE International Conference on Acoustics, Speech, and Signal Processing, Montreal, QC, Canada, 17–21 May 2004; Volume 3, p. iii-377.
20. Liu, C.-L.; Lou, D.-C.; Lee, C.-C. Reversible Data Embedding Using Reduced Difference Expansion. In Proceedings of the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007), Kaohsiung, Taiwan, 26–28 November 2007; Volume 1, pp. 433–436.
21. Ahmad, T.; Holil, M.; Wibisono, W.; Muslim, I.R. An improved Quad and RDE-based medical data hiding method. In Proceedings of the 2013 IEEE International Conference on Computational Intelligence and Cybernetics (CYBERNETICSCOM), Yogyakarta, Indonesia, 3–4 December 2013; pp. 141–145.
22. Arham, A.; Nugroho, H.A.; Adji, T.B. Multiple layer data hiding scheme based on difference expansion of quad. *Signal Process.* **2017**, *137*, 52–62. [CrossRef]
23. Ntahobari, M.; Ahmad, T. Protecting Data by Improving Quality of Stego Image based on Enhanced Reduced difference Expansion. *Int. J. Electr. Comput. Eng.* **2018**, *8*, 2468–2476. [CrossRef]
24. Syahlan, Z.; Ahmad, T. Reversible data hiding method by extending reduced difference expansion. *Int. J. Adv. Intell. Inform.* **2019**, *5*, 101–112. [CrossRef]

25. Kukreja, S.; Kasana, S.S.; Kasana, G. Histogram based multilevel reversible data hiding scheme using simple and absolute difference images. *Multimed. Tools Appl.* **2019**, *78*, 6139–6162. [CrossRef]
26. Al-Qershi, O.M.; Khoo, B.E. High capacity data hiding schemes for medical images based on difference expansion. *J. Syst. Softw.* **2011**, *84*, 105–112. [CrossRef]
27. Al-Qershi, O.M.; Ee Khoo, B. Two-dimensional difference expansion (2D-DE) scheme with a characteristics-based threshold. *Signal Process.* **2013**, *93*, 154–162. [CrossRef]
28. Maniriho, P.; Mahoro, L.J.; Bizimana, Z.; Niyigaba, E.; Ahmad, T. Reversible difference expansion multi-layer data hiding technique for medical images. *Int. J. Adv. Intell. Inform.* **2021**, *7*, 1–11. [CrossRef]