


Article

Reversible Data Hiding Using an Improved Pixel Value Ordering and Complementary Strategy

Rajeev Kumar ¹, Neeraj Kumar ² and Ki-Hyun Jung ^{3,*} 

¹ Department of Computer Science and Engineering, Delhi Technological University, Delhi 110042, India

² Department of Electronics & Communication Engineering, Jamia Millia Islamia University, Delhi 110025, India

³ Department of Software Convergence, Andong National University, Andong 36729, Republic of Korea

* Correspondence: kingjung@anu.ac.kr; Tel.: +82-54-820-7968

Abstract: Reversible data hiding (RDH) schemes based on pixel value ordering have gained significant popularity due to their unique capability of providing high-quality marked images with a decent embedding capacity, while also enabling secret information extraction and the lossless recovery of the original images at the receiving side. However, the marked image quality may be distorted severely when the pixel value ordering (PVO) method is employed in a layer-wise manner to increase the embedding capacity. In this paper, a new high-capacity RDH scheme using a complementary strategy is introduced to overcome the limitation of the image quality in the case of layer-wise embedding. The proposed RDH scheme first divides the cover image into non-overlapping blocks of 2×2 pixels uniformly and then sorts the pixels of each block according to their intensity values. The secret data are then embedded into two layers. In the first layer, the minimum value of the block is decreased and the maximum value is increased by either 1 or 2 to embed the secret data bits. The second layer is used as a complement to the first layer and is in symmetry with the first layer. In the second layer, the proposed RDH scheme increases the minimum valued pixel and decreases the maximum valued pixel in order to minimize the distortion resulting from the first layer embedding and to embed an additional amount of the secret data. As a result, the proposed RDH scheme significantly increases the embedding capacity, which is clearly evident from the conducted experimental results.

Keywords: complementary strategy; IPVO; PVO-RDH; reversible data hiding



Citation: Kumar, R.; Kumar, N.; Jung, K.-H. Reversible Data Hiding Using an Improved Pixel Value Ordering and Complementary Strategy. *Symmetry* **2022**, *14*, 2477. <https://doi.org/10.3390/sym14122477>

Academic Editor: Jeng-Shyang Pan

Received: 23 September 2022

Accepted: 8 November 2022

Published: 22 November 2022

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



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

1. Introduction

The internet of things (IoT) is one of the trending technologies in the current technological era. It connects millions of physical devices through the internet network with a high speed and reliable data transfer to implement automatization. Various types of sensors attached to the IoT devices facilitate in the automatization as they collect and share environmental information in digital forms such as text, image, audio, video, and control and measurement signals. IoT networks deployed in the medical and defense fields [1] are sensitive to data integrity and protection. Hence, for the security reasons, digital content is pre-processed before it is shared the network. Pre-processing is performed using one of the two well-known techniques, i.e., encryption and steganography [2]. The encryption technique converts the digital content into a mysterious form using the popular symmetric and/or asymmetric key-based encryption methods. Mysterious content is unrecognizable for the intruders and is not decodable without the corresponding public/private key. However, in some circumstances, this may raise doubts about suspicious activity among outsiders, as the contents (though encoded) are visible to everyone, whereas the steganography technique reduces such risks by covertly embedding confidential messages in some trivial media, known as cover/host media, which can be of any type, such as text, image, audio, video, etc. At times, when both the cover media and embedding contents

are required in their original form at the receiving end, the reversible data hiding (RDH) technique is adopted. The RDH technique guarantees the reversibility of both the cover media and embedding contents at the receiving end [3].

In the early phase, RDH techniques were proposed based on their capacity for lossless compression [3–5] (which usually creates room inside the cover media by compressing its trivial elements to embed the secret message), but these techniques provide a very limited embedding capacity (EC). Thereafter, RDH techniques advanced in three major directions, which are difference expansion (DE) [6], histogram shifting [7,8] and prediction-error expansion (PEE) [9,10]. The difference expansion based the RDH scheme exploits inter-pixel differences to embed the data. In contrast, histogram-shifting-based RDH methods create a histogram of the image and then expand the peak bins while shifting the others. In 2007, Thodi et al. [9] presented a novel high EC with a least distortion RDH technique using prediction error expansion (PEE). The PEE strategy makes use of a predictor to predict a reference pixel based on the surrounding pixels and then modifies the reference pixel to embed the bits of the secret message based on the identified error between the reference pixel and the predicted value. To modify the pixel value, a prediction error histogram (PEH) is plotted, and its peak bins are utilized to embed the secret bits by expanding them and shifting the others to ensure the reversibility. The PEE seeks to embed data in all the pixels and makes only small changes in magnitude ($+1/-1$) per pixel. Thus, it improves both the EC and marked image quality.

A noteworthy improvement of PEE was introduced by Li et al. [10]. Li et al. proposed a pixel value ordering (PVO) technique which provides high-fidelity stego-images with a decent EC. The PVO technique divides the image into uniform-sized blocks and then sorts the pixels of each block. Next, the PVO generates prediction errors by taking the pixel intensity difference between the first and second pixels located at the extreme ends of the block. Thus, the prediction error histogram (PEH) generated from the difference between sorted pixels is usually sharper than the one produced by conventional PEE, which allows for embedding in one of the peak bins while shifting the other bins to ensure the reversibility. Thus, it provides high-fidelity stego-image. However, it has a limited EC, as only one of the peak bins is utilized for embedding the secret data. To overcome this limitation, Peng et al. introduced a value-added extension to PVO, which is popularly known as improved PVO (I-PVO) [11]. I-PVO computes the prediction errors in a different way, which considers the relative locations of the pixels inside the original block so that two peak bins, i.e., '0' and '1', can be expanded to increase the EC, and at the same time, the number of shifted pixels can be reduced to increase the quality of the stego-image. Thus, the IPVO method provides a higher data hiding capacity and stego-image of a better visual quality. Since reversible data hiding can be employed in layer-wise embedding to match the demand for a high capacity, the severity of the distortion of the stego-image is quite high in the case of two-layered IPVO. To address this concern, the proposed work introduces a new RDH scheme which embeds the secret data in two layers, where the second layer is complementary to the first layer. This means that modification performed in the first layer is nullified to a great extent in the second layer of embedding. Thus, the proposed RDH scheme significantly increases the data hiding capacity while maintaining the marked image quality. The rest of the paper is organized as follows. Section 2 discusses the related work. In Section 3, the proposed RDH scheme is explained in detail. The experimental results are discussed in Section 4. In Section 5, the conclusion of the work is provided.

2. Related Works

In this section, pixel-value-ordering-based RDH schemes are briefly reviewed. As discussed in Section 1, the PVO-based RDH scheme was first introduced by Li et al. in 2012 [10]. The PVO-RDH [10] provides high-fidelity stego-images with a decent embedding capacity. The work of [10] was extended by Peng et al. [11] in 2013, proposing an improved PVO-based RDH scheme with the aim of ensuring a higher embedding capacity with less distortion. The IPVO scheme makes use of '0' and '1' prediction errors (which are

usually the peak bins in the prediction error histograms (PEH)) to hide the secret data. Kumar et al. [12] extended the work of [11] to further increase the embedding capacity. For this purpose, Kumar et al. discussed a new IPVO-RDH scheme using the bin reservation strategy. The bin reservation strategy basically creates room to shift the minimum- and maximum-valued pixels to either of the sides, i.e., the left and right sides, so that a greater number of secret information bits can be embedded. However, this increase in the embedding capacity is achieved at the cost of the image distortion. The IPVO-RDH scheme [11] was further researched and improved in the study reported in [13]. In 2018, Jain and Kasana [13] proposed a new data hiding scheme that can embed the secret data into the already sorted blocks of the original cover image, unlike the method employed in [10], so that the embedding capacity can be increased by reducing the number of non-concealable image blocks. In 2019, Kumar et al. [14] introduced another new IPVO-based reversible data hiding scheme using the block extension strategy. The block extension strategy basically extends the smooth block size by two pixels so that the number of non-concealable pixels is reduced. Thus, the blocks of 2×2 pixels are extended to 2×3 pixels (in the case of extremely smooth blocks), and the embedding in the additional pixels is performed in a pixel-wise manner, as in [15], while the embedding in the original 2×2 block is performed in the manner described in [11]. In another noteworthy improvement, Weng et al. [16] introduced a novel PVO-RDH scheme which flexibly modifies the pixels in terms of the block-wise complexity. The scheme conceals the bits of secret information based on the block smoothness, which leads to the optimal utilization of the block redundancy. As a result, a significant enhancement in the embedding performance is achieved.

In addition to the aforementioned schemes, many other schemes, such as those described in [17,18], that use dynamic block size were introduced in the literature to improve the embedding performance of the schemes described in [10,11]. The scheme introduced by Di et al. [18] makes use of a quadtree for efficient embedding by PVO-RDH. The quadtree approach adaptively generates blocks of different sizes based on the correlations of image region, and then the secret data are optimally embedded. By introducing a new direction for efficient embedding, Zhao et al. [19] improved the PVO-RDH schemes using the adaptive threshold strategy for efficiently categorizing noisy blocks. The standard deviation is utilized to efficiently identify the noisy blocks, instead of the difference between the second and third pixels of the sorted blocks. The adaptive-threshold-based strategy helps to achieve a higher-quality stego-image [19,20].

Lee et al. [21] developed a “star-shaped” PVO-based reversible data hiding scheme. The scheme is different from other contemporary schemes, such as Li et al.’s method [10], as the proposed scheme takes a fixed 3×3 block to embed the secret data efficiently and utilizes the prevalent correlations between the pixel elements of the block for the preservation of the image quality and to ensure a high embedding capacity. Furthermore, it enables the sender/hider to perform multi-layer embedding, so that embedding capacity can be increased. He et al. [22] discussed a multi-pass PVO-based RDH scheme which takes a defined number of maximum- and minimum-valued pixels within the block as independent units to embed the secret data. The method increases the data hiding capacity using optimally combined embedding. Weng et al. [23] further extended the work on K-pass pixel value ordering to enhance the embedding performance. Weng et al.’s scheme exploits the traditionally excluded pixels to ensure a more accurate prediction of the local complexity, so that efficient embedding could be performed. Ou et al. [24] proposed a PVO-based data embedding technique in a two-dimensional space. The technique utilizes the correlations between the prediction errors in a block so that the redundancy of the block can be exploited effectively. The authors further discussed a dynamic selection method that can be used to treat different regions of the images differently based on their correlation level so as to enhance the embedding efficiency. He et al. [25] further extended this work by proposing a new RDH method based on optimally manipulating a 2D-PEH. The method flexibly predicts and modifies the maximum and minimum pixels, unlike those described in [10,11], to increase the embedding capacity. Kumar et al. [26] discussed a new enhanced

pairwise IPVO-based RDH scheme which embeds the secret data in not only a block-wise manner but also a pixel-wise manner, so that the pixels can be optimally utilized to embed the secret information. Additionally, the scheme embeds the secret data using the enhanced pairwise IPVO strategy in the case of block-wise embedding to limit the caused distortion. Furthermore, layer-wise embedding is also performed, which helps to further increase the embedding capacity. Thus, the scheme provides a high data hiding capacity with a sustained image quality. The work of [26] was further developed by Kaur et al. [27] in 2021 to further enhance the embedding performance. A comprehensive review of PVO-based RDH schemes can be further consulted in [28].

Based on the analysis of the aforementioned PVO-RDH schemes, it can be observed that none of the existing schemes aim to improve the IPVO scheme for layer-wise embedding. Thus, in this paper, a new RDH scheme using a complementary embedding strategy is proposed. The proposed scheme extended the work described in [11] to increase the embedding capacity. The detailed algorithm of the proposed complementary scheme is outlined in Section 4. The next section briefly reviews Peng et al.'s scheme.

3. The Proposed RDH Scheme

In this section, the proposed IPVO-based reversible data hiding scheme using a complementary embedding strategy is presented. Since it was proved in [11] that partitioning the image in 2×2 blocks provides the highest data hiding capacity, the proposed RDH scheme also partitions the host image into blocks of 2×2 pixels. The pixels of each block are first arranged in ascending order, and then the minimum- and maximum-valued pixels are prudently modified to conceal the secret information bits. The secret information embedding is performed in two layers, where the second layer is complementary to the first layer's work and is almost in symmetry with the first layer. The proposed scheme modifies the pixels in the second layer in such a way that the modification performed in the first layer can be minimized to a great extent. In the next subsections, the proposed embedding algorithm, and extraction and image recovery algorithm are described.

3.1. Embedding Algorithm

In this subsection, the detailed embedding algorithm as described at Algorithm 1 is presented.

Algorithm 1. Embedding Algorithm

1. Partition the host image (H) into blocks of 2×2 pixels (P_1, \dots, P_4) and arrange the pixels of each block in ascending order ($P_{\pi(1)}, P_{\pi(2)}, P_{\pi(3)}, P_{\pi(4)}$), where $P_{\pi(1)} \leq \dots \leq P_{\pi(4)}$, $\pi(i) < \pi(j)$ if $P_{\pi(i)} = P$ and $i < j$, as in [11].
 2. Design a location map (LM) to represent each image block (B_i) by either '0' or '1'. The blocks which have $P_{\pi(1)} < 2$, or $P_{\pi(4)} > 253$ are represented by '0' in the LM . All the other blocks are represented by '1'. LM is compressed using arithmetic encoding to obtain a compressed location map (CLM) of the length $LCLM$, where $LCLM$ represents the length of the compressed location map.
 3. Classify block (B_i) into three categories, namely the probable overflow/underflow, complex, and smooth, based on following ruleset:
If B_i is represented by '0' in LM , **then**
 B_i is assumed to be a probable overflow/underflow block, which is not considered for embedding S .
else B_i is represented by '1' in LM , **then**
compute noise level (NL_i) such that $NL_i = P_{\pi(3)} - P_{\pi(2)}$, and
if $NL_i > thr$, **then**
 B_i is assumed to be a complex block, which, again, is not considered for embedding S .
else B_i is assumed to be a smooth block, which is considered for embedding S .
end if
end if
-

4. In the case of smooth blocks:

Compute the prediction differences PD_{max} and PD_{min} using Equations (1) and (2), respectively, which are defined as follows:

$$PD_{max} = P_u - P_v \quad (1)$$

$$PD_{min} = P_s - P_t \quad (2)$$

where $u = \min(\pi(4), \pi(3))$, $v = \max(\pi(4), \pi(3))$, $s = \min(\pi(2), \pi(1))$, and $t = \max(\pi(2), \pi(1))$.

Embed the bits (b) from S into the maximum-valued pixel $P_{\pi(4)}$ and minimum-valued pixel $P_{\pi(1)}$ using Equations (3) and (4), respectively, which are defined as follows:

$$P'_{\pi(4)} = \begin{cases} P_{\pi(4)} + (b + 1), & \text{if } PD_{max} = 1, \\ P_{\pi(4)} + 2, & \text{if } PD_{max} > 1, \\ P_{\pi(4)} + (b + 1), & \text{if } PD_{max} = 0, \\ P_{\pi(4)} + 2, & \text{if } PD_{max} < 0 \end{cases} \quad (3)$$

$$P'_{\pi(1)} = \begin{cases} P_{\pi(1)} - (b + 1), & \text{if } PD_{min} = 1, \\ P_{\pi(1)} - 2, & \text{if } PD_{min} > 1, \\ P_{\pi(1)} - (b + 1), & \text{if } PD_{min} = 0, \\ P_{\pi(1)} - 2, & \text{if } PD_{min} < 0 \end{cases} \quad (4)$$

Compute the new prediction differences PD'_{max} and PD'_{min} between the newly obtained first maximum ($P'_{\pi(4)}$) and second maximum pixels ($P_{\pi(3)}$) and the first minimum ($P'_{\pi(1)}$) and second minimum pixels ($P_{\pi(2)}$) using Equations (1) and (2), respectively.

Embed the bits (b) from S into the newly obtained maximum-valued pixel $P'_{\pi(4)}$ and newly obtained minimum-valued pixel $P'_{\pi(1)}$ using Equations (5) and (6), respectively, which are defined as follows.

$$P''_{\pi(4)} = \begin{cases} P'_{\pi(4)} - b, & \text{if } PD'_{max} = -3 \text{ or } 3, \\ P'_{\pi(4)}, & \text{if } PD'_{max} > 3, \\ P'_{\pi(4)}, & \text{if } PD'_{max} < -3, \\ P'_{\pi(4)} - 1, & \text{else} \end{cases} \quad (5)$$

$$P''_{\pi(1)} = \begin{cases} P'_{\pi(1)} + b, & \text{if } PD'_{min} = -3 \text{ or } 3, \\ P'_{\pi(1)}, & \text{if } PD'_{min} > 3, \\ P'_{\pi(1)}, & \text{if } PD'_{min} < -3, \\ P'_{\pi(1)} + 1, & \text{else} \end{cases} \quad (6)$$

The process of secret information embedding is halted in a case where the all the bits from S are embedded or the last information carrying block B_{end} is reached.

5. Concatenate all the auxiliary information, such as the length of the compressed location map (LCLM), compressed location map (CLM), thr , and B_{end} , which is required for blind decoding to obtain a list Aux .
6. Extract and conceal the least significant bit (LSB) of the first $LAux$ pixels (where $LAux$ represents the length of Aux) in the remaining blocks using Step 4. Then, use the simple LSB substitution method to substitute the LSB of first $LAux$ pixels with the bits of Aux .

Thus, all the bits of the secret information bitstream (S) are concealed, and a stego-image H' is obtained. Next, an illustrative example of the proposed complementary embedding method is discussed.

3.2. Illustrative Example of Embedding Algorithm

In this subsection, an illustrative example of the embedding process of the proposed complementary embedding method is discussed in detail using Figure 1. Here, a host image block of 2×2 pixels $(P_1, P_2, P_3, P_4) = (105, 104, 100, 99)$ is considered. The pixels of the block are then arranged in ascending order, such as $(P_{\pi(1)}, P_{\pi(2)}, P_{\pi(3)}, P_{\pi(4)}) = (99, 100,$

104, 105). It should be noted that the example does not take the location map and noise level threshold into consideration, so that the focus can be maintained purely on the embedding procedure. Next, two prediction differences (PD_{max} and PD_{min}) are computed, such that $PD_{max} = (105 - 104) = 1$ and $PD_{min} = (100 - 99) = 1$. Suppose that three bits of secret data ("100") are to be embedded into the block. The values of PD_{min} and PD_{max} , are both 1, meaning the values $P_{\pi(1)} = 99$ and $P_{\pi(4)} = 105$ will be decreased and increased by $(b + 1)$, respectively. Thus, the minimum and maximum pixels after the first layer of data embedding become $(99 - (1 + 1)) = 97$ and $(105 + (0 + 1)) = 106$. For the second layer of data embedding, two different values, namely (PD'_{max} and PD'_{min}), are calculated using the new maximum and minimum pixels, such that $PD'_{max} = (106 - 104) = 2$ and $PD'_{min} = (100 - 97) = 3$. In the second layer, the information is embedded only when the difference is equal to -3 or 3 in Step 5d of the embedding algorithm. In this example, PD'_{min} is 3, which means that a new minimum value after the embedding of the secret data bit, i.e., '0', will be $P''_{\pi(1)} = (97 + 0) = 97$. The maximum pixel will not be used for the secret data embedding, as PD'_{max} is 2, but its value will be decreased by 1, so that the host image can be restored. Thus, the final stego-block is $(105, 104, 100, 97)$.

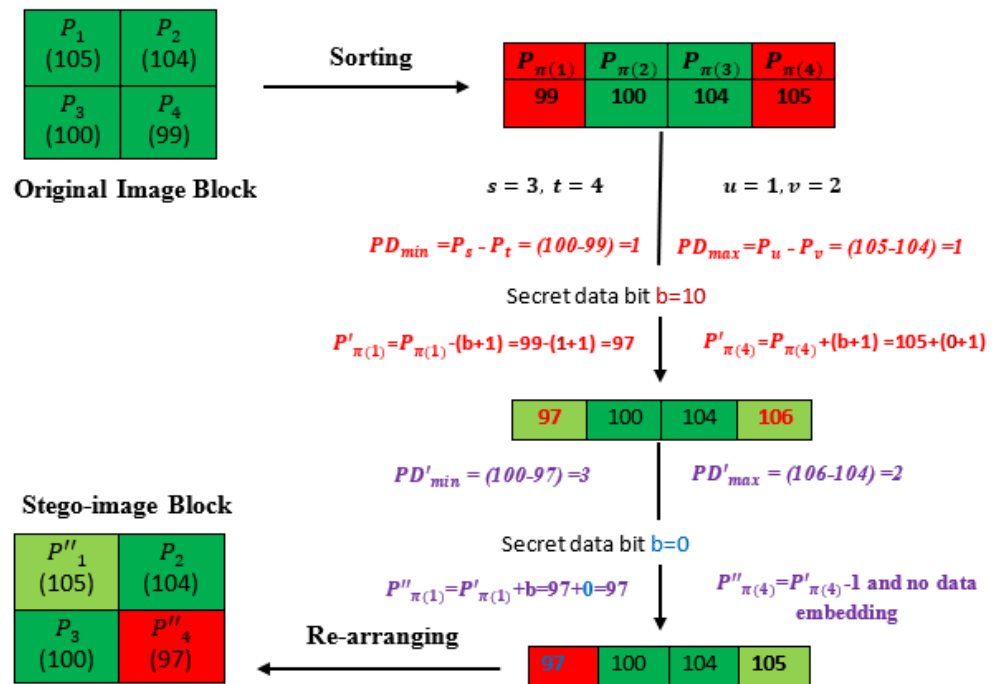


Figure 1. An illustrative example of the proposed embedding procedure.

3.3. Extraction and Image Recovery Algorithm

In this subsection, the proposed extraction and image recovery algorithm as Algorithm 2 is presented.

Algorithm 2. Extraction and Image Recovery Algorithm

1. Read the LSBs of some pre-defined pixels to obtain the length of the auxiliary information Aux . Next, extract and process the entire auxiliary information by reading the LSBs of the next $LAux$ pixels.
 2. Partition the stego-image (H') into blocks of 2×2 pixels (P''_1, \dots, P''_4) and arrange the pixels of each block in ascending order ($P_{\pi(1)}, P_{\pi(2)}, P_{\pi(3)}, P_{\pi(4)}$), where $P_{\pi(1)} \leq \dots \leq P_{\pi(4)}, \pi(i) < \pi(j)$ if $P_{\pi(i)} = P_{\pi(j)}$ and $i < j$, as in [11].
-

3. Classify the block (B_i) starting from the (B_{end+1}) into three categories, namely the probable overflow/underflow, complex, and smooth, based on the following ruleset:
 - if** B_i is represented by '0' in LM , **then**
 the B_i is assumed to be a probable overflow/underflow block, which does not have any secret information bits.
 - else** B_i is represented by '1' in the LM , **then**
 compute the noise level (NL_i) such that $NL_i = P_{\pi(3)} - P_{\pi(2)}$, and
 if the $NL_i > thr$, **then**
 B_i is assumed to be a complex block, which, again, does not have any secret information bits.
 - else** B_i is assumed to be a smooth block, and proceed to the next step.
 - End if**

4. **if** B_i is a smooth one, **then**

Compute the two prediction differences PD''_{max} and PD''_{min} between the first maximum ($P''_{\pi(4)}$) and second maximum pixels ($P_{\pi(3)}$) and the first minimum ($P''_{\pi(1)}$) and second minimum pixels ($P_{\pi(2)}$) using Equations (1) and (2), respectively.

Extract the concealed bits of secret information and restore the pixel values using following the ruleset:

if $PD''_{max} == -3$ or $PD''_{max} == 3$, **then**
 $b = '0'$ and $P'_{\pi(4)} = P''_{\pi(4)}$.
else if $PD''_{max} == -2$ or $PD''_{max} == 2$, **then**
 $b = '1'$ and $P'_{\pi(4)} = P''_{\pi(4)} + 1$.
else if $PD''_{max} < -3$ or $PD''_{max} > 3$, **then**
 $P'_{\pi(4)} = P''_{\pi(4)}$, and there is no hidden data.
else $P'_{\pi(4)} = P''_{\pi(4)} + 1$.
end if

if $PD''_{min} == -3$ or $PD''_{min} == 3$, **then**
 $b = '0'$ and $P'_{\pi(1)} = P''_{\pi(1)}$.
else if $PD''_{min} == -2$ or $PD''_{min} == 2$, **then**
 $b = '1'$ and $P'_{\pi(1)} = P''_{\pi(1)} - 1$.
else if $PD''_{min} < -3$ or $PD''_{min} > 3$, **then**
 $P'_{\pi(1)} = P''_{\pi(1)}$, and there is no hidden data.
else $P'_{\pi(1)} = P''_{\pi(1)} - 1$.
end if

Compute the two prediction differences PD'_{max} and PD'_{min} between the first maximum ($P'_{\pi(4)}$) and second maximum pixels ($P_{\pi(3)}$) and the first minimum ($P'_{\pi(1)}$) and second minimum pixels ($P_{\pi(2)}$) using Equations (1) and (2), respectively.

Extract the concealed bits of secret information and restore the pixel values using the following ruleset:

if $PD'_{max} == -2$ or $PD'_{max} == 3$, **then**
 $b = '1'$ and $P_{\pi(4)} = P'_{\pi(4)} - 2$.
else if $PD'_{max} == -1$ or $PD'_{max} == 2$, **then**
 $b = '0'$ and $P_{\pi(4)} = P'_{\pi(4)} - 1$.
else if $PD'_{max} < -2$ or $PD'_{max} > 3$, **then**
 $P_{\pi(4)} = P'_{\pi(4)} - 2$, and there is no hidden data.
else $P_{\pi(4)} = P'_{\pi(4)}$.
end if

if $PD'_{min} == -2$ or $PD'_{min} == 3$, **then**
 $b = '1'$ and $P_{\pi(1)} = P'_{\pi(1)} + 2$.
else if $PD'_{min} == -1$ or $PD'_{min} == 2$, **then**
 $b = '0'$ and $P_{\pi(1)} = P'_{\pi(1)} + 1$.
else if $PD'_{min} < -2$ or $PD'_{min} > 3$, **then**
 $P_{\pi(1)} = P'_{\pi(1)} - 2$, and there is no hidden data.
else $P_{\pi(1)} = P'_{\pi(1)}$.
end if

end if

The step is repeated until the $LAux$ bits are retrieved by processing the blocks of the image.

5. Substitute the LSB of the first $LAux$ pixels with the bits obtained from Step 4. Next, iteratively execute Step 2 to Step 4 until the block (B_{end}) is detected, so that the complete hidden bitstream of the secret information (S) and the host image (H) can be obtained.

3.4. Illustrative Example of the Extraction and Image Recovery Algorithm

In this subsection, an illustrative example of the extraction and image recovery process of the proposed complementary method is discussed in detail using Figure 2. Here, a stego-image block of 2×2 pixels ($P''_1, P''_2, P''_3, P''_4$) = (105, 104, 100, 97) is considered. The pixels of the block are then arranged in ascending order, such as ($P''_{\pi(1)}, P''_{\pi(2)}, P''_{\pi(3)}, P''_{\pi(4)}$) = (97, 100, 104, 105). Next, the two prediction differences PD''_{max} and PD''_{min} are computed, such that $PD''_{max} = (105 - 104) = 1$ and $PD''_{min} = (100 - 97) = 3$. It should be noted that the secret information is assumed to be embedded if the difference belongs to either -3 or 3 or -2 or 2 , as per the Step 5b of the algorithm, in the first layer. In this example, $PD''_{min} = (100 - 97) = 3$, meaning there are '0' bits concealed in $P''_{\pi(1)}$, and nothing is hidden in $P''_{\pi(4)}$, as per the given rules of the extraction algorithm. Then, the pixel values after the extraction of the secret data, as per the given rules of the algorithm, can be recovered. The new values are $P'_{\pi(1)} = P''_{\pi(1)} = 97$ and $P'_{\pi(2)} = P''_{\pi(2)} + 1 = 105 + 1 = 106$. For the second layer of the data extraction and image recovery, two new prediction differences, PD'_{max} and PD'_{min} , are computed such that $PD'_{max} = (106 - 104) = 2$ and $PD'_{min} = (100 - 97) = 3$. It should be noted that the secret information is assumed to be embedded if the difference is either -2 or 3 or -1 or 2 , as per the Step 5d of the algorithm, in the second layer. Here, PD'_{min} is 3, meaning there is '1' bit concealed, and the original pixel value can be restored such that $P_{\pi(1)} = P'_{\pi(1)} + 2 = 97 + 2 = 99$. In the case of the PD'_{max} , the concealed bit of the secret information is '0', and the original pixel value can be restored such that $P_{\pi(4)} = P'_{\pi(4)} - 1 = 106 - 1 = 105$. Thus, the original host image block (105, 104, 100, 99) after the extraction of the secret information '100', is received.

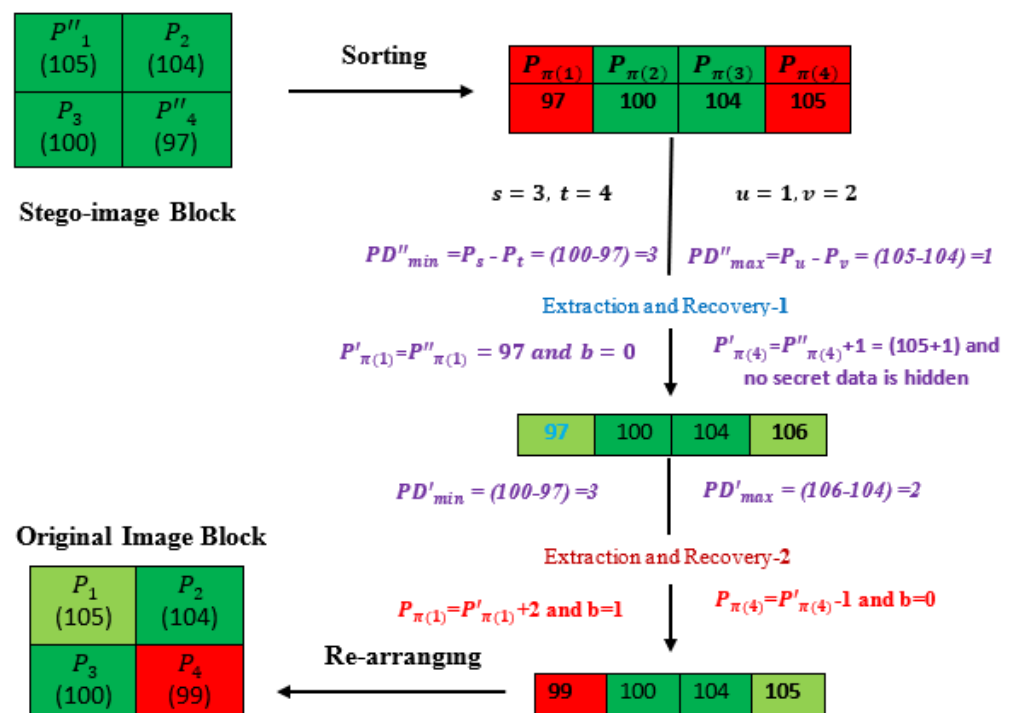


Figure 2. An illustrative example of the proposed extraction and image recovery procedure.

4. Experimental Results and Discussion

This section discusses the experimental performance analysis of our proposed complementary RDH scheme in comparison with the related existing schemes, such as that

of He et al. [25], Weng et al. (K-Pass) [23], that of Weng et al. (DIPVO) [16], Peng et al. (Two-layered) [11] and Di et al.'s method [18]. Peng et al.'s two-layered method is basically a two-time implementation on a given image. The performance of Peng et al.'s two-layered method is evaluated here mainly to enable a comprehensive analysis comparing it with the proposed method, which also makes use of two-layer embedding. However, the second layer embedding of the proposed scheme is basically a complement to the first layer embedding. To cover address the state of the art of pixel-value-ordering-based hiding methods, the results are comparatively evaluated against the results of some of the recently published methods, such as He et al.'s and Di et al.'s methods, along with the parent method, i.e., Peng et al.'s method. The experimental results of Peng et al. [11] and Peng et al.'s two-layered method are taken for the 2×2 pixels blocks, as it was observed from the literature that the maximum embedding capacity is achieved at a block size of 2×2 pixels. The implementation is performed using MATLAB running on an Intel (R) Core (TM) i5 processor, 3.20 GHz, with a 4 GB RAM hardware platform. The secret data stream used in our experiment was generated using a random function

The implementation of the complementary RDH scheme along with Peng et al.'s two-layered scheme was performed in MATLAB for experimental purposes. The experimental results of He et al. [25] and Di et al.'s method [18], the Weng et al. (K-Pass) [23] and Weng et al. (DIPVO) [16] method, were taken from their articles. The experiments were performed using standard images, as shown in Figure 3. The performance metrics used for evaluating the existing and the complementary RDH schemes were the embedding capacity and peak signal-to-noise ratio (PSNR). The marked images which were obtained after embedding the secret information through the proposed schemes are shown in Figure 4.

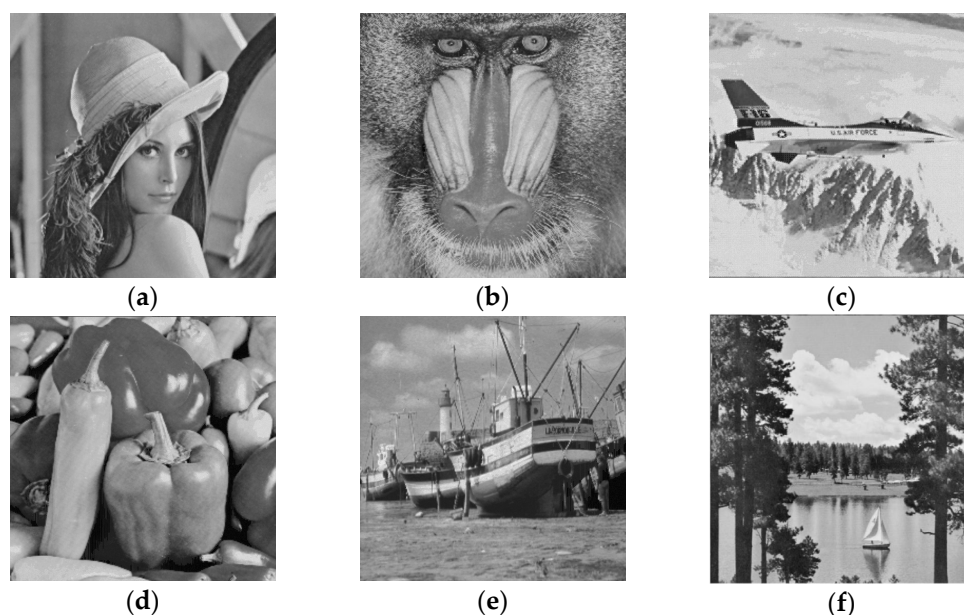


Figure 3. Cover images sized 512×512 pixels. (a) Lena. (b) Baboon. (c) Airplane. (d) Peppers. (e) Fishing boat. (f) Sail boat.

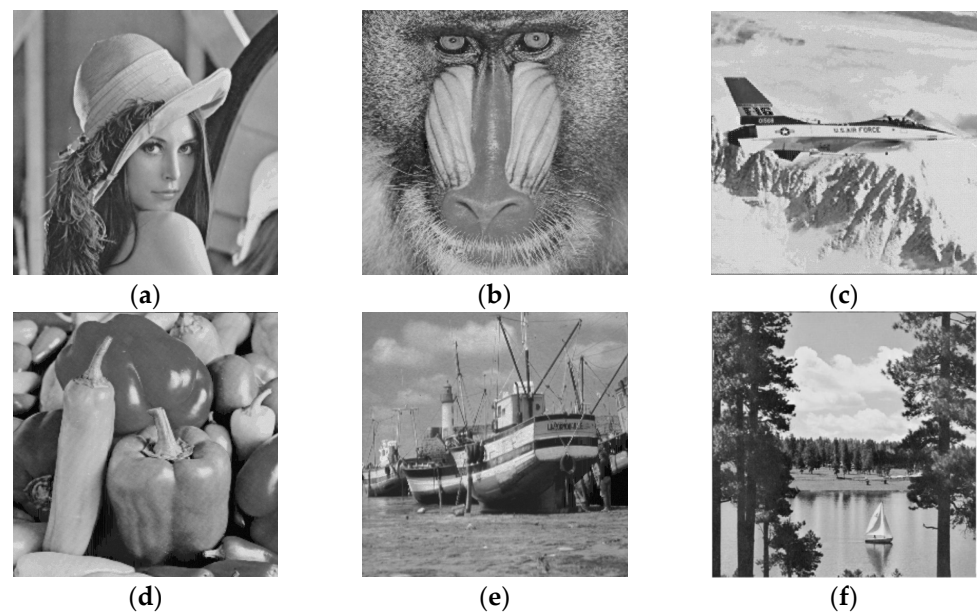


Figure 4. Stego-images sized 512×512 pixels. (a) Lena. (b) Baboon. (c) Airplane. (d) Peppers. (e) Fishing boat. (f) Sail boat.

The experimental results and comparison of the proposed complementary RDH scheme with the existing ones, such as that of He et al. [25], Weng et al. (K-Pass) [23], that of Weng et al. (DIPVO) [16], Peng et al.'s [11] two-layered method and Di et al.'s method [18] are illustrated. Figure 5 illustrates the embedding performance of the different existing methods in comparison with the proposed complementary RDH scheme. In our experiments, the noise level thresholds '65' and '4' were considered for the baboon, and the remaining test images, respectively, as far as Peng et al. and Peng et al.'s two-layered method and the proposed scheme are concerned. For the illustrative comparison, we varied the embedding capacity from 5000 bits to its maximum value for all the aforementioned schemes. The figure shows that the performance of the complementary RDH scheme has a low PSNR in comparison to the other popular methods, including those of He et al. [25], Weng et al. [16], Peng et al. [11] and Di et al. [18] and the improved K-pass [23]. The main reason for this inferiority is the use of two-layer data embedding, as all of these methods employ only one-layer embedding, which causes a maximum ± 1 change in the pixel value, whereas the proposed scheme employs two-layer embedding, which causes a ± 2 change in the pixel value. Therefore, the methods such as those of He et al. [25], Weng et al. [16], Peng et al. [11] and Di et al. [18] and Weng et al. (K-Pass) [23] achieve a higher PSNR, comparatively. However, the complementary RDH scheme provides superior results in terms of the data embedding capacity in comparison to the existing aforementioned schemes. Furthermore, the quality of the stego-image is also maintained, since second layer-embedding is used to recover the pixel values to some extent. Moreover, it has a significantly higher PSNR and data hiding capacity for all the test images (except the airplane) than Peng et al.'s two-layered method, which is the closest method in terms of the style of the secret data embedding.

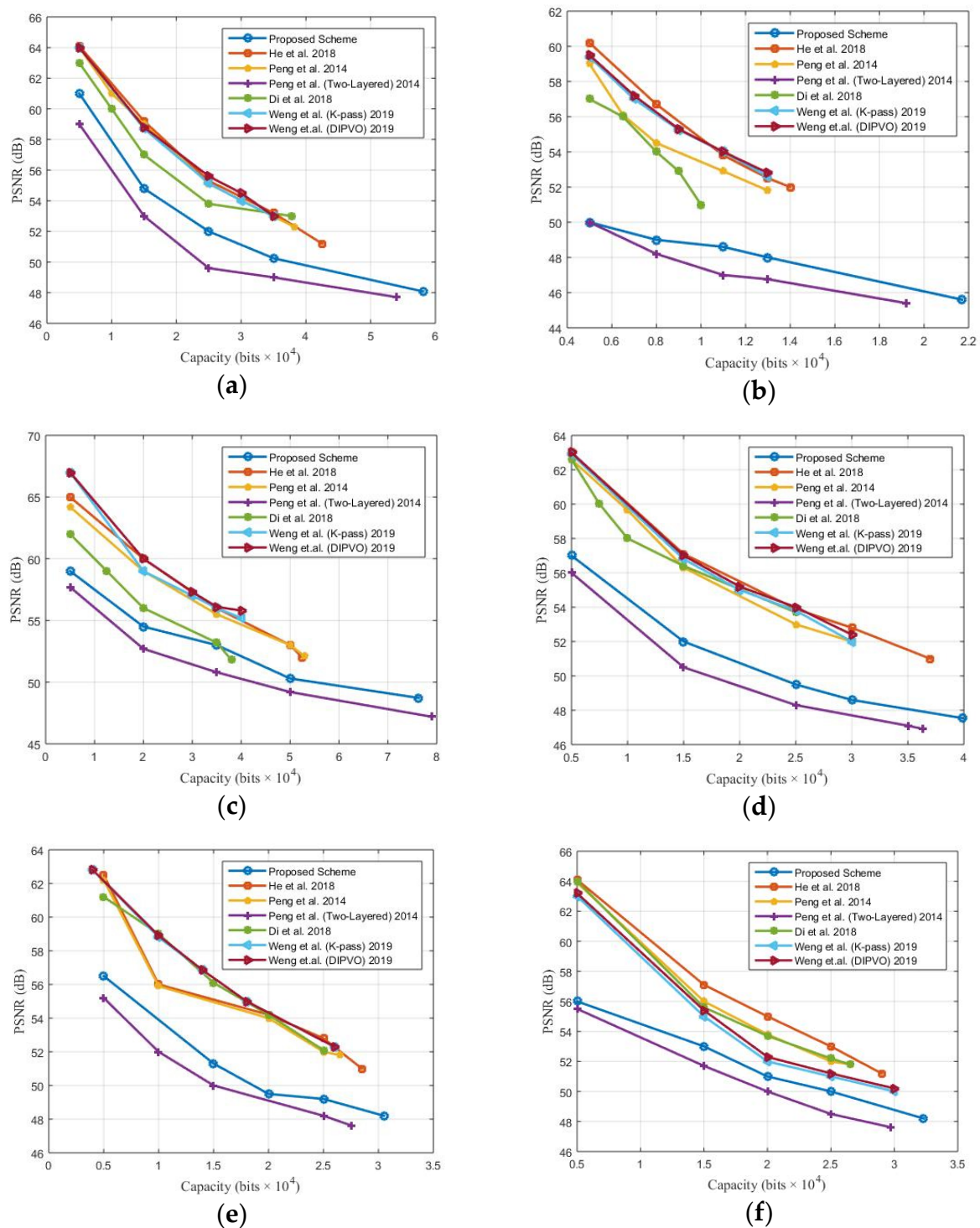


Figure 5. Performance comparisons of PSNR vs. embedding capacity of the proposed scheme with He et al. [25], Peng et al.'s [11], Peng et al. (Two-layered), Di et al.'s method [18], Weng et al. (K-Pass) [23], and Weng et al. (DIPVO) [16]. (a) Lena. (b) Baboon. (c) Airplane. (d) Peppers. (e) Fishing boat. (f) Sail boat.

To succinctly evaluate the performance of the proposed RDH scheme with respect to Peng et al.'s two-layered method at different thresholds (noise level), two cover images, namely the Lena and baboon images, were used, as these represent the extreme directions of digital images as far as standard images are concerned.

Not all the results for all the images are presented due to their similar nature. The experimental results (as shown in Figure 6) were captured by varying the noise level threshold in the ranges of 2 to 20 and 20 to 80 in the case of Lena and the baboon, respectively. It was observed in the experimental analysis that the embedding capacity is usually directly proportional to the noise level threshold, whereas the PSNR is indirectly proportional. The proposed complementary RDH scheme performs significantly better than the Peng et al.'s two-layered method using the same parameters, as evident from Figure 6. Thus, it can easily be stated that the proposed RDH scheme successfully improves the working of the PVO-based RDH schemes as far as the layer-wise embedding is concerned.

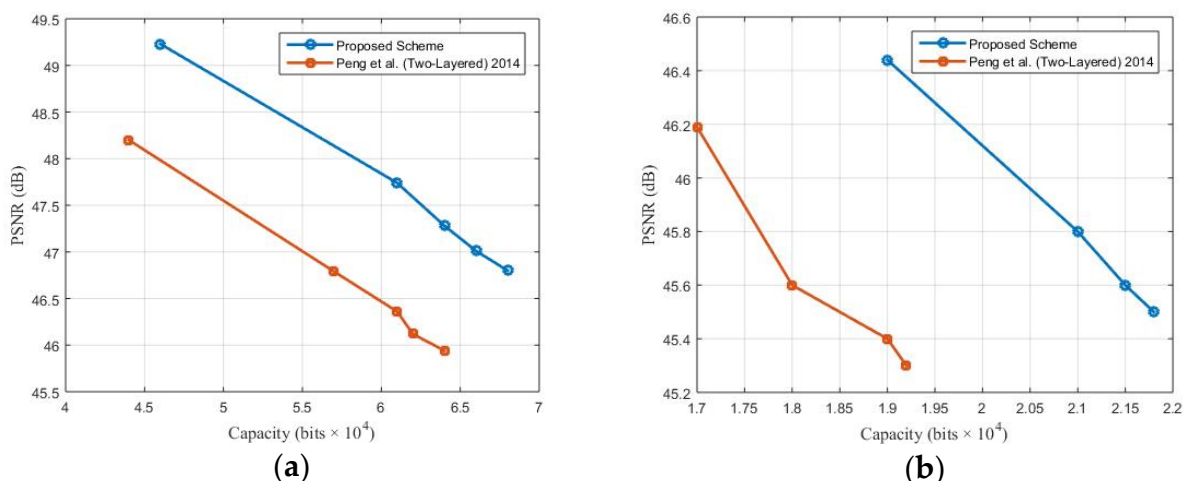


Figure 6. Comparative analysis of the embedding performance at different thresholds of the proposed scheme with the Peng et al. (Two-layered) [11]. (a) Lena. (b) Baboon.

4.1. Histogram Attack

A histogram analysis of each of the test images was performed to verify the performance of the proposed method against histogram attacks. The performance analysis was accomplished by comparing the histograms of the original images with the stego-images (after embedding the 30,000 bits, as shown in Figure 3), as seen in Figure 7. It is clear that neither the original image histograms nor their associated stego-histograms images underwent any discernible modification. For the exceptions of the baboon and peppers, the histograms also reveal that the majority of the test images lacked pixels valued at 0 or 255, which could result in an overflow or underflow issue and would be displayed clearly. Even in the case of the baboon and peppers, there are very few of these pixels. Thus, it is evident that the compressed location map can be represented by a small number of bits, indicating that the embedding capacity would barely be affected by the supplementary information.

4.2. Statistical Attack

The created stego-images conceal sensitive information using the proposed scheme to safeguard the original information. The marked pixels in stego-images include the original information that we embedded.

The cover image and stego-image correlation coefficients (CC) and standard deviations (SD) are displayed in Table 1 for the sake of comparison, taking into account $thr = 5$ for all the test images. The CC is closer to one, and the difference in SD is closer to zero, which indicates a good concealment according to the data. Thus, the proposed approach is more resistant to a number of attacks. Furthermore, it is possible to correctly recover the original image from the stego-images and obtain the hidden information without any data loss. Due to the scheme's innocence, it is able to thwart potential malevolent attacks.

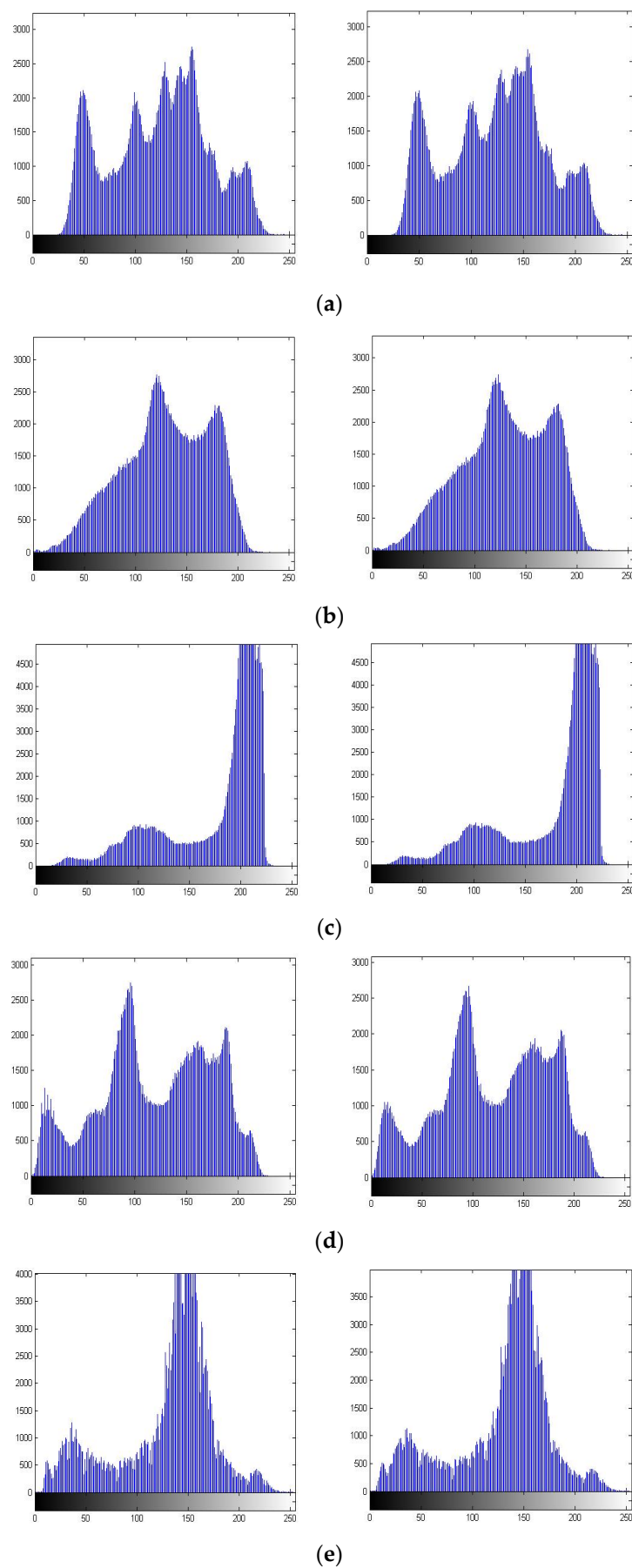


Figure 7. Cont.

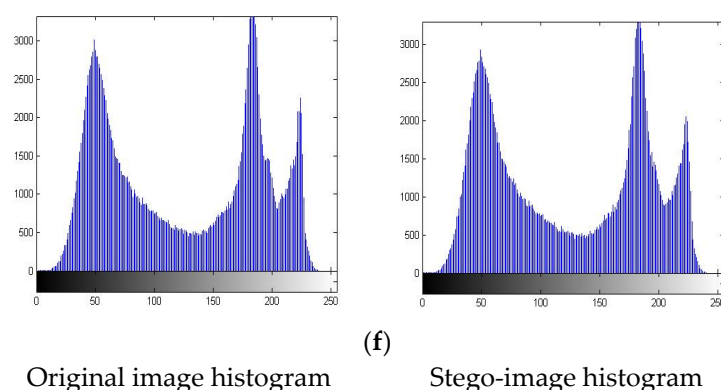


Figure 7. Histogram distribution of the original and stego-images. (a) Lena. (b) Baboon. (c) Airplane. (d) Peppers. (e) Fishing boat. (f) Sail boat.

Table 1. Standard deviations (SD) and correlation coefficients (CC) of cover images and stego-images.

Test Image	CC	SD (Cover Image)	SD' (Stego-Image)	Difference (SD'-SD)
Lena	0.9998	47.8557	47.8942	0.0382
Baboon	0.9999	42.3135	42.3845	0.0710
Airplane	0.9999	46.4120	46.4341	0.0220
Peppers	0.9999	53.8794	53.9227	0.0433
Fishing Boat	0.9998	46.6772	46.7309	0.0537
Sail-Boat	0.9999	65.5815	65.6142	0.0328

5. Conclusions

In this paper, a new RDH scheme using the complementary embedding strategy has been proposed. The proposed scheme aimed to preserve the marked image quality in the case of layer-wise embedding. For a high image quality, a cover image was first partitioned uniformly into non-overlapping blocks, and then the secret data were able to be concealed in the maximum and minimum pixel values only in the two layers. In the first layer, the minimum and maximum pixels were decreased and increased by either by '1' or '2', respectively. In the second layer, the minimum pixel value was increased by '0' or '1' and the maximum pixel value was decreased by '0' or '1' to embed the secret data. As a result, the ordering of the pixel values was preserved to ensure the reversibility in the block. The experimental results provided an evidence of the superior embedding capacity of the scheme, with a good PSNR, compared to the previous related works. The proposed scheme could hide 68,000 bits on 46.7 dB and 21,000 bits on 45.5 dB in the Lena and baboon images respectively.

Author Contributions: Conceptualization, R.K. and N.K.; methodology, K.-H.J. and N.K.; visualization, R.K.; writing—original draft, R.K. and N.K.; writing—review and editing, R.K. and K.-H.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Education (2021R1I1A3049788), and Brain Pool program, funded by the Ministry of Science and ICT through the National Research Foundation of Korea (2019H1D3A1A01101687, 2021H1D3A2A01099390).

Data Availability Statement: Data is available on the request to any of the author.

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

References

1. Singh, Y.; Singh, S.; Kumar, R. A distributed energy-efficient target tracking protocol for three level heterogeneous sensor networks. *Int. J. Comput. Appl.* **2012**, *51*, 0975–8887. [\[CrossRef\]](#)
2. Kumar, R.; Saini, K.K.; Chand, S. A new steganography technique using snake scan ordering strategy. *Int. J. Image* **2013**, *6*, 25–32. [\[CrossRef\]](#)
3. Kumar, R.; Chand, S. A reversible high capacity data hiding scheme using pixel value adjusting feature. *Multimed. Tools Appl.* **2016**, *75*, 241–259. [\[CrossRef\]](#)
4. Kumar, R.; Chand, S. A reversible data hiding scheme using pixel location. *Int. Arab J. Info. Tech.* **2018**, *15*, 763–768.
5. Malik, A.; Singh, S.; Kumar, R. Recovery based high capacity reversible data hiding scheme using even-odd embedding. *Multimed. Tools Appl.* **2018**, *77*, 15803–15827S. [\[CrossRef\]](#)
6. Tian, J. Reversible data embedding using a difference expansion. *IEEE Trans. Circuits Syst. Video Technol.* **2003**, *13*, 890–896. [\[CrossRef\]](#)
7. Kumar, R.; Chand, S.; Singh, S. An Improved Histogram-Shifting-Imitated Reversible Data Hiding based on HVS Characteristics. *Multimed. Tools Appl.* **2018**, *77*, 13445–13457. [\[CrossRef\]](#)
8. Kumar, R.; Chand, S. A novel high capacity reversible data hiding scheme based on pixel intensity segmentation. *Multimed. Tools Appl.* **2017**, *76*, 979–996. [\[CrossRef\]](#)
9. Thodi, D.M.; Rodriguez, J.J. Expansion embedding techniques for reversible watermarking. *IEEE Trans. Image Process.* **2007**, *16*, 721–730. [\[CrossRef\]](#)
10. Li, X.; Li, J.; Li, B.; Yang, B. High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion. *Signal Process.* **2013**, *93*, 198–205. [\[CrossRef\]](#)
11. Peng, F.; Li, X.L.; Yang, B. Improved PVO-based Reversible Data Hiding. *Digit. Signal Process.* **2014**, *25*, 255–265. [\[CrossRef\]](#)
12. Kumar, R.; Kumar, N.; Jung, K.H. I-PVO based high capacity reversible data hiding using bin reservation strategy. *Multimed. Tools Appl.* **2020**, *79*, 22635–22651. [\[CrossRef\]](#)
13. Kumar, N.; Kasana, S.S. High-capacity reversible data hiding using modified pixel value ordering approach. *J. Circuits Syst. Comput.* **2018**, *17*, 175–185.
14. Kumar, R.; Kim, D.S.; Lim, S.; Jung, K.H. High-Fidelity Reversible Data Hiding Using Block Extension Strategy. In Proceedings of the 34th International Technical Conference on Circuits/Systems, Jeju, Republic of Korea, 23–26 June 2019; Volume 19, pp. 1–4.
15. Qu, X.; Kim, H.J. Pixel-based pixel value ordering predictor for high-fidelity reversible data hiding. *Signal Process.* **2015**, *111*, 249–260. [\[CrossRef\]](#)
16. Weng, S.; Shi, Y.; Hong, W.; Yao, Y. Dynamic improved pixel value ordering reversible data hiding. *Inf. Sci.* **2019**, *489*, 136–154. [\[CrossRef\]](#)
17. Wang, X.; Ding, J.; Pei, Q. A novel reversible image data hiding scheme based on pixel value ordering and dynamic pixel block partition. *Inf. Sci.* **2015**, *310*, 16–35. [\[CrossRef\]](#)
18. Di, F.; Zhang, M.; Liao, X.; Liu, J. High-fidelity reversible data hiding by quadtree-based pixel value ordering. *Multimed. Tools Appl.* **2018**, *78*, 7125–7141. [\[CrossRef\]](#)
19. Zhao, W.; Yang, B.; Gong, S. A higher efficient reversible data hiding scheme based on pixel value ordering. *J. Inf. Hiding Multimed. Signal Process.* **2018**, *9*, 918–928.
20. Lu, T.C.; Tseng, C.Y.; Huang, S.W.; Vo, T.N. Pixel-value-ordering based reversible information hiding scheme with self-adaptive threshold strategy. *Symmetry* **2018**, *10*, 764. [\[CrossRef\]](#)
21. Lee, C.F.; Shen, J.J.; Kao, Y.C. High-Capacity Reversible Data Hiding Based on Star-Shaped PVO Method. In Proceedings of the 14th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Sendai, Japan, 26–28 November 2018; Volume 109.
22. He, W.; Zhou, K.; Cai, J.; Wang, L.; Xiong, G. Reversible data hiding using multi-pass pixel value ordering and prediction-error expansion. *J. Vis. Commun. Image Represent.* **2017**, *49*, 351–360. [\[CrossRef\]](#)
23. Weng, S.; Chen, Y.; Ou, B.; Chang, C.; Zhang, C. Improved K-Pass Pixel Value Ordering Based Data Hiding. *IEEE Access* **2019**, *7*, 34570–34582. [\[CrossRef\]](#)
24. Ou, B.; Li, X.; Wang, J. High-fidelity reversible data hiding based on pixel-value-ordering and pairwise prediction-error expansion. *J. Vis. Commun. Image Represent.* **2016**, *39*, 12–23. [\[CrossRef\]](#)
25. He, W.; Xiong, G.; Weng, S.; Cai, J.; Wang, Y. Reversible data hiding using multi-pass pixel-value-ordering and pairwise prediction-error expansion. *Inf. Sci.* **2018**, *467*, 784–799. [\[CrossRef\]](#)
26. Kumar, R.; Jung, K.H. Enhanced pairwise IPVO-based reversible data hiding scheme using rhombus context. *Inf. Sci.* **2020**, *536*, 101–119. [\[CrossRef\]](#)
27. Kaur, G.; Singh, S.; Rani, R.; Kumar, R.; Malik, A. High-quality reversible data hiding scheme using sorting and enhanced pairwise PEE. *IET Image Process.* **2022**, *16*, 1096–1110. [\[CrossRef\]](#)
28. Kaur, G.; Singh, S.; Rani, R.; Kumar, R. A comprehensive study of reversible data hiding (RDH) schemes based on pixel value ordering (PVO). *Arch. Comput. Methods Eng.* **2021**, *28*, 3517–3568. [\[CrossRef\]](#)