electronics

Article

Secure Reversible Data Hiding Using Block-Wise Histogram Shifting

Samar Kamil [1], Monalisa Sahu [2], Raghunandan K. R. [3] and Aditya Kumar Sahu [4,*]

[1] Technical College Management, Baghdad 10047, Iraq
[2] Department of CSE, School of Engineering and Technology, GIET University, Gunupur 765022, Odisha, India
[3] Department of Computer Science and Engineering, NMAM Institute of Technology, NITTE (Deemed to be University), Nitte 574110, Karnataka, India
[4] Amrita School of Computing, Amrita Vishwa Vidyapeetham, Amaravati 522502, Andhra Pradesh, India
* Correspondence: s_adityakumar@av.amrita.edu or adityasahu.cse@gmail.com

Abstract: Reversible data hiding (RDH) techniques recover the original cover image after data extraction. Thus, they have gained popularity in e-healthcare, law forensics, and military applications. However, histogram shifting using a reversible data embedding technique suffers from low embedding capacity and high variability. This work proposes a technique in which the distribution obtained from the cover image determines the pixels that attain a peak or zero distribution. Afterward, adjacent histogram bins of the peak point are shifted, and data embedding is performed using the least significant bit (LSB) technique in the peak pixels. Furthermore, the robustness and embedding capacity are improved using the proposed dynamic block-wise reversible embedding strategy. Besides, the secret data are encrypted before embedding to further strengthen security. The experimental evaluation suggests that the proposed work attains superior stego images with a peak signal-to-noise ratio (PSNR) of more than 58 dB for 0.9 bits per pixel (BPP). Additionally, the results of the two-sample *t*-test and the Kolmogorov–Smirnov test reveal that the proposed work is resistant to attacks.

Keywords: reversible data hiding; histogram shifting; imperceptibility; embedding capacity

Citation: Kamil, S.; Sahu, M.; K. R., R.; Sahu, A.K. Secure Reversible Data Hiding Using Block-Wise Histogram Shifting. *Electronics* **2023**, *12*, 1222. https://doi.org/10.3390/electronics12051222

Academic Editors: Ruifan Li and Xin Ning

Received: 1 February 2023
Revised: 18 February 2023
Accepted: 22 February 2023
Published: 3 March 2023

1. Introduction

Reversible data hiding (RDH) techniques can restore the original cover media and the embedded information on the receiver end [1]. The least significant bit (LSB) strategy is a highly preferred data hiding technique [2]. This technique replaces the LSBs of the cover image pixels with data bits [3]. The stego image is processed to extract the secret data bits on the receiver side without recovering the original cover image [4]. Interestingly, there are several application areas, such as e-healthcare, law forensics, and military imagery, where original secret data and cover image recovery are crucial on the receiving end [5]. In [6], cover image pixels are processed to recover the cover image after secret data extraction. Various reversible data embedding techniques have been proposed, including difference expansion and its variants [7–10], histogram shifting [11–15], prediction-based technique [16], and vector quantized-based technique [17]. Of these, the histogram-based shifting technique has gained popularity due to its simplicity and ability to offer higher security. However, a significant setback for the histogram-based shifting technique is that secret data are embedded without taking care of the contrast of the cover image, which provides distortion in a large number of pixels and, thus, negatively impacts the visual quality. To overcome this challenge, a dynamic histogram shifting RDH technique is proposed based on the contrast of the cover image. In the peak value of the cover image histogram, left-side or right-side data embedding is done. Furthermore, to improve the embedding capacity, the image is divided into fixed blocks, and for each block, the histogram bins' peak values are determined for embedding capacity [18]. Researchers have suggested

various data scrambling techniques in the literature [19–22] using the XOR function and different keystreams.

The major contribution of this paper is to improve the security, embedding capacity, and visual quality using a dynamic block-wise reversible (DBWR) data embedding technique. Initially, the pixel histogram is drawn from the cover image. Next, the histogram processing determines the 256-bit key, after which the cover image is divided into four blocks. Each block's histogram bin is plotted, and the contrast of each block is determined. The contrast defines the frame's histogram properties, which are low contrast, high contrast, and normal contrast. Based on the predetermined contrast properties, it then identifies in which direction the peak value of the histogram should be adjusted. Thus, the minimum variability comes after the adjustment process. The secret data are embedded using a 1-bit LSB technique after all the needed conditions have been adaptively selected. The experimental results show that the proposed technique has improved the visual quality and embedding capacity considerably compared to existing techniques, namely Zong's technique [17] and Rajkumar's and Vasuki's technique [16].

The rest of the paper is organized as follows: Section 2 explains the histogram shifting embedding technique and highlights its issues. Next, Section 3 illustrates the proposed data embedding and extraction process. The experimental results and comparative analysis are presented in Section 4. Finally, Section 5 concludes the work with promising future directions.

2. Related Work

Earlier histogram shifting-based RDH techniques use the peak point for data embedding in an image [23,24]. Rajkumar et al. [16] suggested an improved RDH technique that utilizes the Gaussian low-pass filter to pre-process host images. Here, the highest peak point of the histogram is chosen for embedding. The secret key provides an authentication process for the stego image. The experimental results show better perceptual quality and robustness. Zong et al.'s [17] RDH technique offers better imperceptibility. Using a low-pass filter, it first partitions the host image pixels into either low- or high-frequency components.

Furthermore, the gray levels of the low-frequency components are obtained using a randomly generated secret key [25]. Aziz et al. [26] proposed an RDH framework utilizing the difference in an image to improve the embedding capacity. Here, in addition to taking the difference of neighboring pixels, it also rearranges the image columns or rows to enhance the smoother regions. Then, a difference-based technique for embedding the data can be used for the transformed image. Some recent works [27–33] have extended more spaces to embed a large amount of data in images.

Pan et al. [34] proposed a novel scheme for reversible data hiding based on pixel value ordering (PVO) and dynamic pixel block partitionin a dynamic blocking strategy [35] used to divide the cover image. Fallahpour et al. [36] suggested an improved RDH technique using block-wise embedding and histogram shifting. Here, the peak and zero bins are determined. Next, adjacent bins of the peak are shifted. The data hiding is performed on the peak bins. The suggested technique is simple yet provides highly efficient reversible data hiding. Unfortunately, this technique still has some issues. For example, it has not been utilized correctly to explore the peak bin and the adjacent peak bin because if the peak bin value is even, then the right side of the peak bin is affected; otherwise, the left side of the peak bin is affected. In addition, the peak and zero values are obtained from the histogram for data embedding. However, for most cases, the zero values on the left and right sides of the peak bins are available. Therefore, if properly selected, the variation that occurs due to shifting can be reduced. The authors in [37] utilized a block-wise substitution-transposition technique to avoid bit errors. Next, a histogram shifting strategy is applied to hide the secret bits. Manikandan et al. [38] suggested that copyright protection of digital images can be achieved using fifth-generation (5G) wireless transmission. In [39–46], the authors suggested different RDH techniques that are used to enhance pairwise pixel value

ordering to improve the quality of the output image without reducing the capacity. A brief description of histogram shifting based on reversible data hiding is discussed below. Next, the proposed research gap, challenges, and objectives are highlighted.

2.1. Brief Description of the Histogram-Shifting Reversible Data Embedding Technique

An image's histogram represents the pictorial view of the number of pixels versus gray-level values. It is the relative (or absolute) frequency with which a gray level appears in the image. A gray image ranges from 0 to 255. In the histogram-shifting data embedding algorithm, the peak value of the histogram is determined, as shown in Figure 1. Here, the gray value 156 has the maximum pixels. Additionally, the gray value of zero pixels is found for histogram shifting, as shown in Figure 1. The gray values 25 and 235 have zero pixels. The histogram is shifted by one from the next available histogram bin to the peak for data embedding. The peak is utilized for hiding the bits with a deviation of ± 1 to the stego pixel from the original.

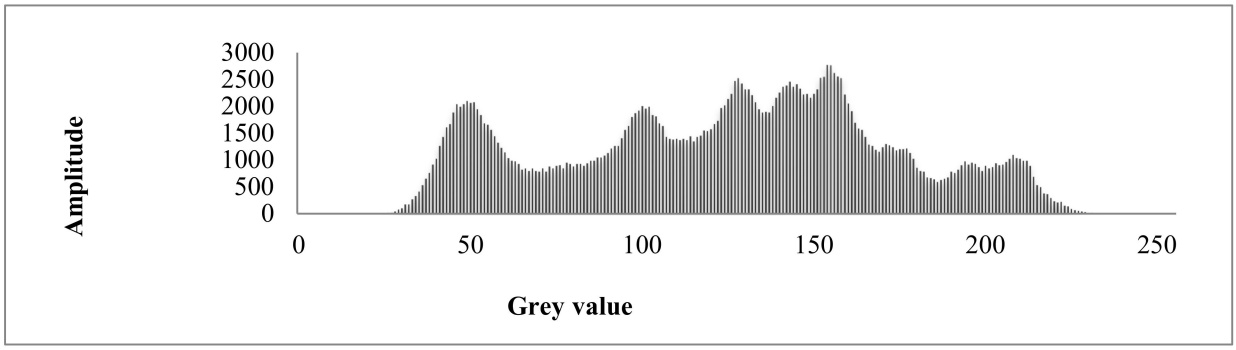


Figure 1. Sample histogram for a pepper image.

2.2. Research Gaps, Objectives, and Contributions

The primary motivation behind the proposed work is to improve existing histogram-shifting RDH techniques. This can be achieved by addressing the following two issues: (1) improper selection of the peak pixel value, and (2) proper selection of the zero-pixel value. The next section discusses the issues just mentioned.

(1) Improper selection of the peak pixel value: In the current histogram-shifting RDH technique, the adjacent pixels of the peak pixel value are shifted by one to embed the secret data in the peak pixel value. Thus, if the peak pixel value is odd, then data hiding is performed using the LSB technique. However, this affects the left adjacent pixel of the peak, and the right adjacent pixel of the peak will then be affected. Therefore, either the peak pixel or the adjacent pixel selection is required for data embedding. The peak or adjacent pixel selection is improved using the proposed technique.

(2) Proper selection of the zero-pixel value: In the current histogram-shifting reversible data hiding technique, the peak pixel and zero-pixel value on the histogram are determined, and data embedding is performed. The variability in the cover image is directly proportional to the distance between the peak and the zero value on the histogram value. Thus, to reduce the distance, in the proposed technique, the zero value on both sides of the peak is determined; then, for the side where the distance is less, the adjacent pixel is shifted. For example, Figure 1 shows the histogram of the cover image, and it has two zero-pixel values (25 and 235) and one peak value (156). The distance between the peak and the zero-pixel value on the right side of the peak is less compared to the zero-pixel value on the left side of the peak. Besides the above two issues, some more issues are found in existing techniques as presented below:

1. Although existing histogram shifting-based techniques offer better embedding capacity, they still produce high variability and are prone to attacks.

2. Although the pixel-value-ordering (PVO) algorithm provides low variability and higher embedding capacity, it requires a long iteration time.

Therefore, to avoid the abovementioned issues, the current work proposes a data-hiding approach that provides better imperceptibility, better embedding capacity, lesser time complexity, and higher security as the secret message is encrypted with a 256-bit key. In our work, the exposure value of the histogram is obtained, and it suggests whether the histogram has low, normal, or high contrast. If the histogram has low contrast, then most of the bins of the histogram lie on the left side (near the zero value), the normal contrast lies in the center, and the high contrast is on the right side (near the 255 value). Next, based on the exposure value, it finds the shifting direction. For example, if the cover image has low contrast, right shifting gives less variability. On the other side, if the image is in high contrast, left shifting gives less variability. Based on the left or right shifting, the peak and zero-bin values in that direction are determined.

Furthermore, the peak value or adjacent bin value is selected for key hiding based on the shifting. The proposed work has an edge over Fallahpour et al. [36] concerning less variability. The following are the primary objectives of the proposed work:

1. The proposed work provides a facility of error correction codes that are added to the encrypted data before data embedding to achieve robustness against attacks.

2. The proposed histogram-shifting technique is tested using various statistical tests, such as the two-sample *t*-test, the Kolmogorov–Smirnov Test, and peak signal-to-noise ratio (PSNR) and SSIM imperceptibility measures. The results of the above measures are in favor of the proposed work.

3. Proposed Technique

The proposed RDH-based histogram-shifting technique provides adequate embedding capacity, lesser variability, and enhanced security. The work is diagrammatically represented in Figure 2. Initially, the cover image is partitioned into blocks. After that, each block's pixels are processed, and a histogram is plotted. Next, the peak and zero bins on the histogram are determined. Based on the peak and zero-bin values, the adjacent bins of the peak value are shifted toward a zero value. The secret data are obtained and split into 1-bit form. The peak bin's LSB bit matches the secret data bit. If the bits are matched, then the counter value is incremented, or else no change in the counter value is made. The whole process is repeated for all peak bins. The counter value is compared with the threshold value (T). The threshold value is determined using Equation (1).

If the counter value is greater than the threshold value, then data are hidden in the flipped form or in the original form. The whole process is repeated for all blocks. At last, the blocks are concatenated to reconstruct the stego image. The peak value, zero-bin value, and secret data hidden in the flipped or original form need to communicate with the receiver to recover the original secret data. The pseudocode for the proposed algorithm is shown below (Algorithm 1). On the receiver side, the stego image is divided into blocks. After that, the peak, zero-bin, and secret data order information are considered for each block. Next, data are extracted from the peak and its adjacent pixel value. Finally, after retrieving the secret data, the histogram bins are shifted toward the peak value to recover the original cover image. The proposed technique to improve visual quality is discussed in this section. Cover image pixel variability is reduced by selecting the appropriate zero-pixel value on the histogram to achieve this goal. In the proposed technique, the terminologies are used as follows: the image is I, the contrast value is C, the peak is P, the right zero is RZ, the left zero is LZ, and the histogram bins are h(n). The total number of bins in the histogram is L, histogram shifting is Hs, and data hiding is DH. The histogram distribution tells the image contrast and is calculated using Equation (2).

$$T = \frac{Maximum(Peak\ Bin)}{2} \quad (1)$$

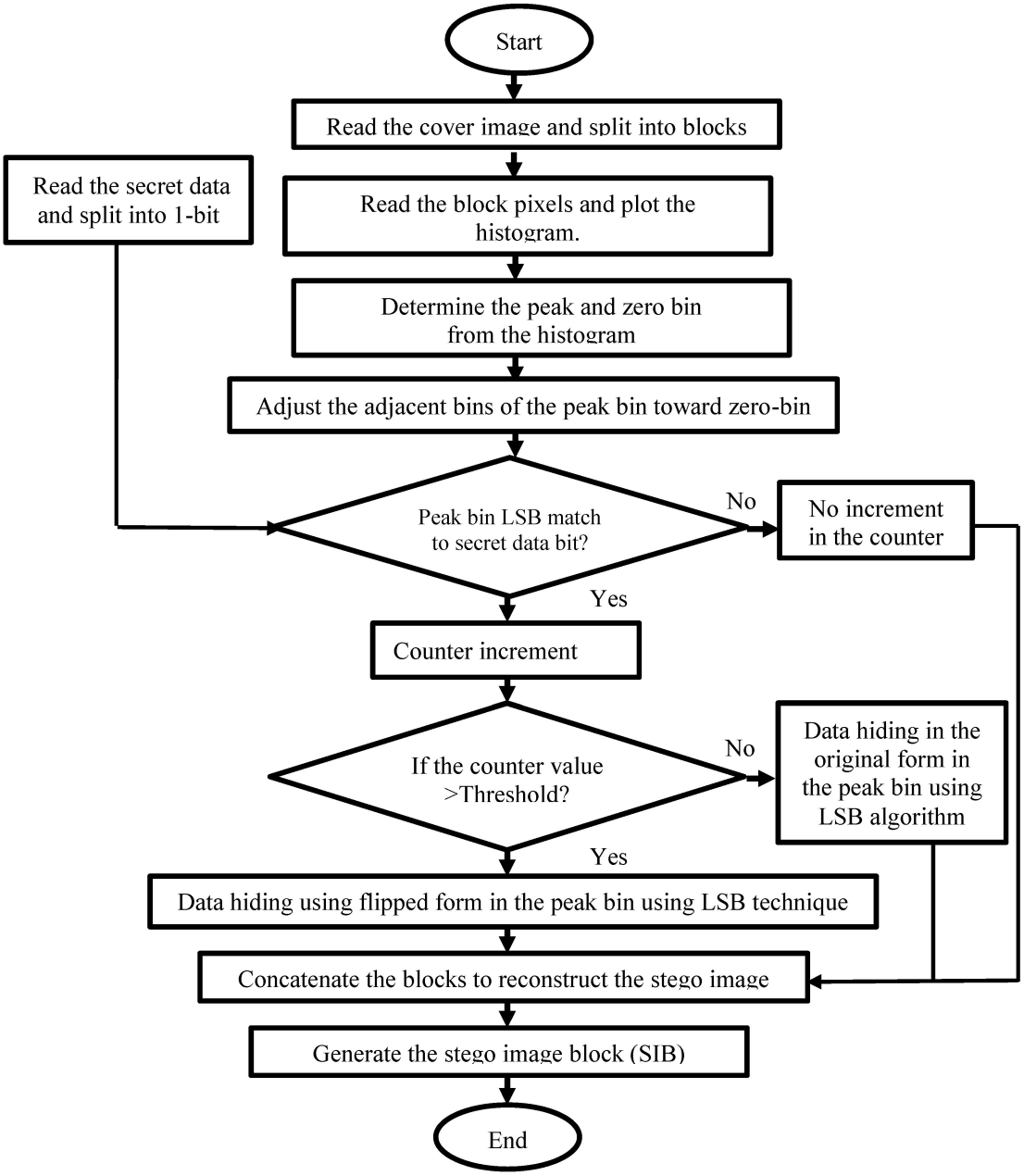


Figure 2. Flowchart for the proposed data embedding technique.

$$C = \frac{1}{L}\frac{\sum_{n=1}^{L} h(n) * n}{\sum_{n=1}^{L} h(n)} \tag{2}$$

Practically, the contrast range varies from 0 to 1. Then, the image histogram shifting is classified into low contrast, normal contrast, or high contrast based on Equation (2), Figure 3a–c show an example of histogram shifting in possible cases. If the image is in in low contrast, the histogram bins are distributed on the left side (near 0) of the histogram. For high contrast, the distribution is on the right side of the histogram (near 255). The adjustment of histogram bins using the proposed technique is represented in Equation (3).

Algorithm 1: Pseudocode for the proposed algorithm

```
Input: Cover image block, secret data, counter
Output: Stego image block
Step 1: Read the image and split it into blocks.
Step 2: Plot the histogram (h) for the blocks.
Step 3: Determine the peak and zero-bin from the histogram.
[peak_index] = max(h) and [zero_index] = min(h)
Step 4: Adjusts the adjacent pixel values
        For i = 1:row
                For j = 1:col
                        If(CI(i,j) > P)
                           CI(i,j) = CI(i,j) + 1
                        Else
                           CI(i,j) = CI(i,j)
                        Endif
        End
End
Step 5: Read the secret data and split it into 1-bit each.
Step 6: If peak bin LSB bit match with the secret, then k = 1, counter = 0;
For i = 1:row
                For j = 1:col
                        If(peak_index(i,j) ≠ secret data(1,k))
                           counter = counter + 1
                           k = k + 1
                        Endif
        End
End
Step 7: If counter > threshold
                For i = 1:length(secret data)
                        If(secret data(1,i) = 0)
                           secret data(1,i) = 1
                        else
                           secret data(1,i) = 1
                        Endif
         End
        Else
        secret data = secret data
      End
Step 8: Data embedding is done.
```

$$H_S = \begin{cases} C - RZ < C - LZ & \text{under contrast} & h(n)\text{adjustment towards right} \\ C - RZ = C - LZ & \text{normal contrast} & h(n)\textit{adjustment either left or right depending on distribution} \\ C - LZ < C - RZ & \text{over contrast} & h(n)\text{adjustment towards left} \end{cases} \quad (3)$$

In low-contrast images, the histogram is shifted toward the right side. For high-contrast images, it is shifted toward the left side. Moreover, if the contrast is normal, the histogram bins are distributed in the middle of the histogram. Next, the histogram bins' intensity distribution on the left side and right side of the peak value is determined, and the side where the pixel distribution is less than the zero points is selected, as shown in Figure 4.

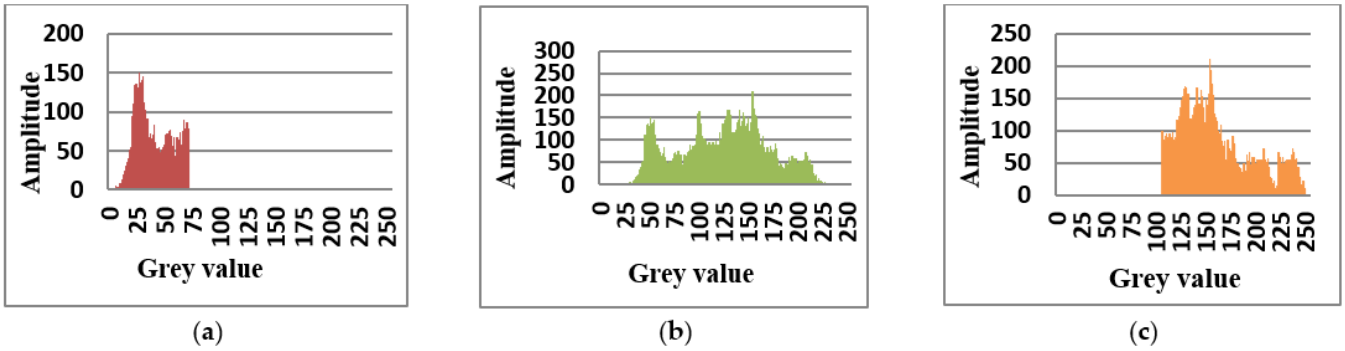


Figure 3. (**a**) low contrast, (**b**) normal contrast, and (**c**) high contrast.

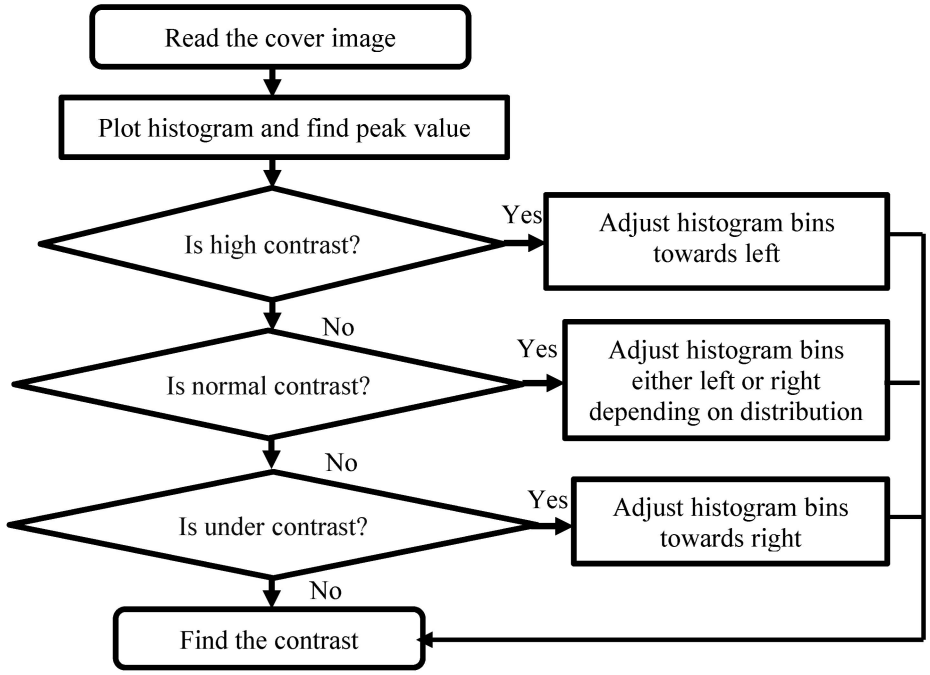


Figure 4. Flow chart for determining contrast and adjustment.

During the embedding phase, the peak value or its adjacent value is selected because the peak value and its adjacent value contain the same approximate distribution. Furthermore, the histogram bins are adjusted toward zero points for secret data embedding, improving the image's visual quality. On the other side, if the zero-point histogram bin is unavailable, then the histogram bin that has a minimum number of pixels is selected, and zero points are created for secret data embedding.

The block diagram of data embedding and extraction is shown in Figure 5a,b. In the proposed technique, the cover image is taken, and the histogram is plotted. Afterward, the histogram is processed to generate a 256-bit random key from Equation (4). The complete flow for the key generation is shown in Figure 6. Here, h_i denotes the histogram bins.

$$Random\_key_i = \frac{h_i}{2} \qquad 0 < \mathrm{I} < 255 \tag{4}$$

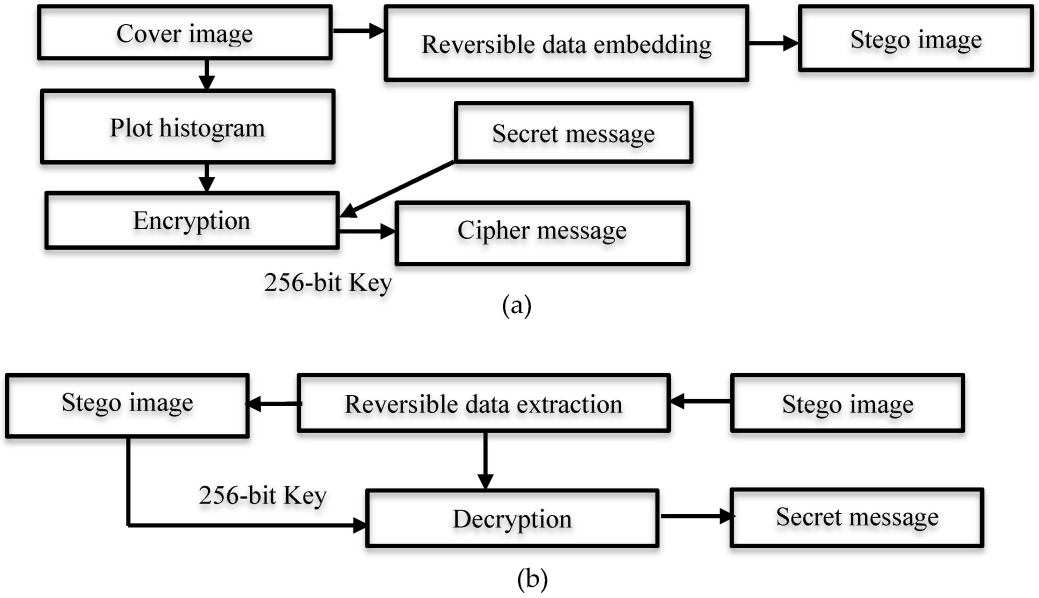


Figure 5. (**a**) Block diagram for data embedding, and (**b**) block diagram for data extraction.

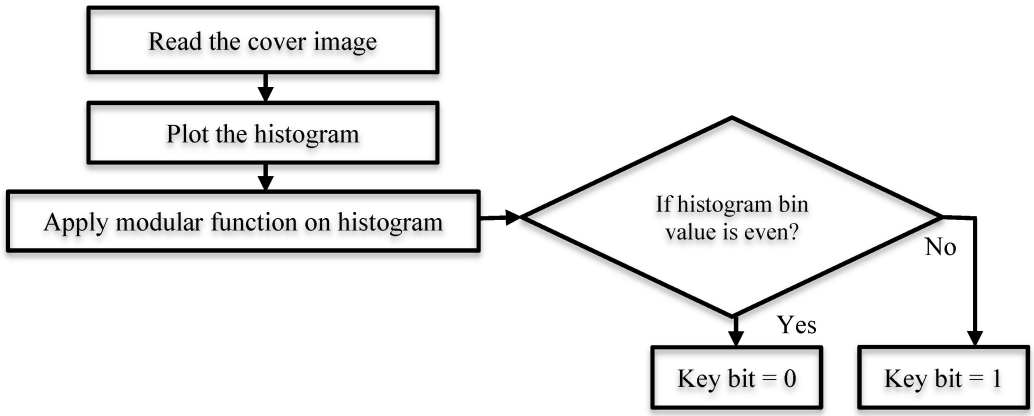


Figure 6. Flow diagram of key generation.

Next, the secret message and the 256-bit key are given as input to the encryption module to generate the ciphertext. Then, the image is grouped into blocks, and for each block, a histogram is found to determine the contrast. The contrast of each block tells whether the block is either low contrast, high contrast, or normally distributed. Furthermore, the peak value of the histogram is determined in each block. Next, based on the contrast, the histogram bins are adjusted on either the left or right side, and the peak value or its adjacent value is selected for data embedding. Next, the cipher data bits are embedded in each block's peak value or its adjacent value pixels to generate the stego image.

Finally, the peak value or adjacent value and the zero-point value details are communicated. Initially, the stego image is retrieved and divided into blocks on the receiver side. Next, based on the information available for the peak value or adjacent value and the zero-point value, the bits are extracted from the peak value or its adjacent value pixels. Afterward, the bins are readjusted to recover the cover image. After that, the cover image histogram is plotted using Equation (4) to generate a 256-bit random key. Then, the secret key and secret data bits are given as input to the decryption algorithm to generate the original secret message. The proposed technique can be summarized in the following steps:

Step 1: At the beginning, the image is taken, and its histogram is drawn, as shown in Figure 7a,b.

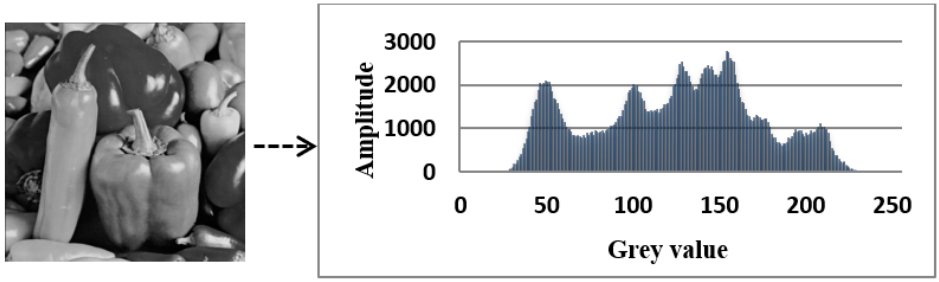


Figure 7. (**a**) cover image, and (**b**) histogram bins of the cover image.

Step 2: The 256-bit key is generated using Equation (4) based on the histogram bin value, and secret data are encrypted using a 256-bit key.

Step 3: The cover image is partitioned into 4 blocks, and a histogram is drawn for each, as shown in Figure 8a,b.

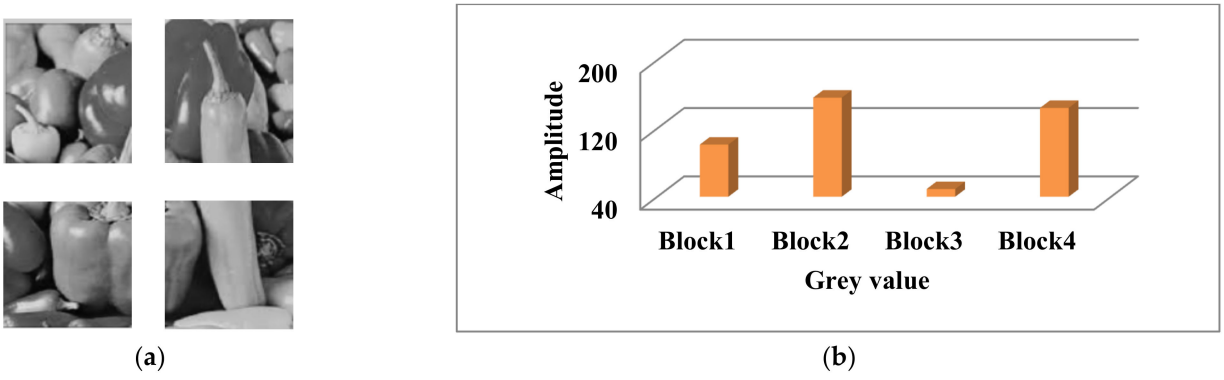


Figure 8. (**a**) Four blocks of the cover image, and (**b**) the histogram of each block.

Step 4: The contrast of each block is determined using Equation (1), and its contrast value is shown in Figure 9.

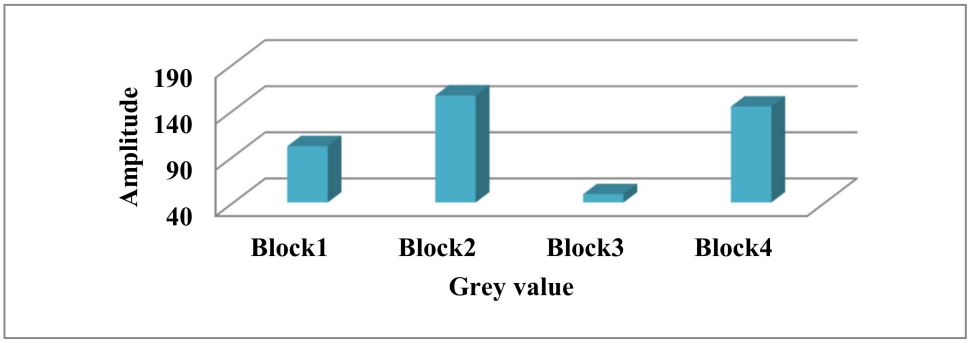


Figure 9. Contrast of respective blocks.

Step 5: Based on the contrast, the direction of histogram shifting is determined using Equation (3) and displayed in Figure 10. Figure 10 shows dynamic data embedding on either side of the peak. The sub-steps are defined below.

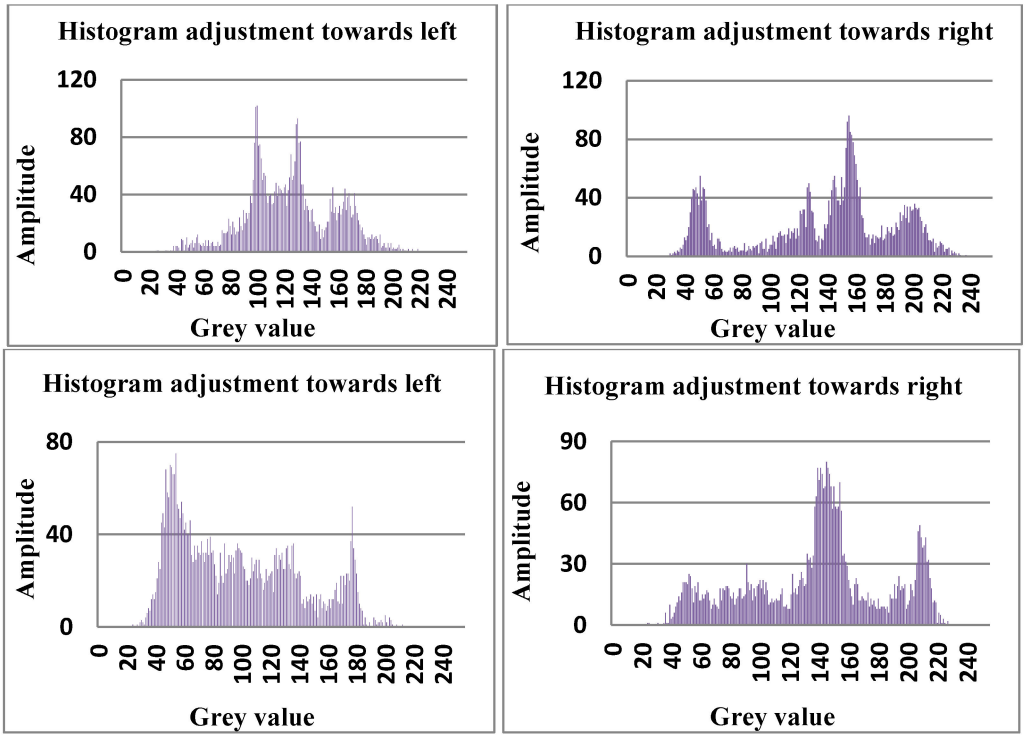


Figure 10. The direction of histogram adjustment in a block.

Step 5.1: The peak is determined from the histogram using Equation (5):

$$P = \max(h_i) \;\; 0 \le i \le 255 \tag{5}$$

Step 5.2: Histogram shifting is required on the left or right side of the peak value based on the exposure value using Equation (2).

Step 5.3: The peak or its adjacent pixel is selected using Equation (6):

$$\mathrm{P_{Peak}} = \begin{cases} \mathrm{P_{Peak}} \quad \mathrm{HRS} & \text{If } \mathrm{P_{Peak}}\%2 = 0 \\ \mathrm{P_{Peak}} + 1 \quad \mathrm{HRS} & \text{If } \mathrm{P_{Peak}}\%2 = 1 \\ \mathrm{P_{Peak}} - 1 \quad \mathrm{HLS} & \text{If } \mathrm{P_{Peak}}\%2 = 0 \\ \mathrm{P_{Peak}} \quad \mathrm{HLS} & \text{If } \mathrm{P_{Peak}}\%2 = 1 \end{cases} \tag{6}$$

Step 5.4: The adjacent pixels are adjusted by 1. Equation (7) is used for a right shift, and Equation (8) is used for a left shift:

$$Adjacent\ pixels(i+1) = Adjacent\ pixels(i) \quad Adjacent\ pixels \le i < zerovalue \tag{7}$$

$$Adjacent\ pixels(i-1) = Adjacent\ pixels(i) \quad Adjacent\ pixels \le i < zerovalue \tag{8}$$

Step 5.5: The data bits are embedded in the LSB of the peak using Equation (9):

$$P_{Peak} = P_{Peak} - h \qquad (h = 254)$$

$$P_{Peak} = P_{Peak} + DH \tag{9}$$

Step 6: The peak value or its adjacent value is selected based on the information on whether the peak value is even or odd, as shown in Table 1. Thus, its adjustment pixel 49 is selected for data embedding.

Table 1. Gray level and its maximum peak value.

Block	Gray Level	Maximum Peak Value
1	121	1278
2	134	1398
3	53	1003
4	149	1234

Step 7: The histogram shifting is completed.

Step 8: Afterward, the secret bit is embedded in the peak or its adjacent value, generating stego image blocks. Finally, the blocks are concatenated to produce a stego image, as shown in Figure 11a,b.

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

Figure 11. (**a**) Four blocks of the stego image, and (**b**) the stego image.

4. Experimental Results and Discussion

This work considers standard grayscale images, as shown in Table 2. The secret data are randomly generated. This work is executed using MATLAB 2017a. The system configuration for carrying out these operations is an Intel core-i5 with 8 GB of RAM. The cover image and the respective stego images that are produced are shown in Table 2. The performance matrices with respect to the quantitative analysis are discussed in subsequent sections.

Table 2. The cover image and the respective stego images.

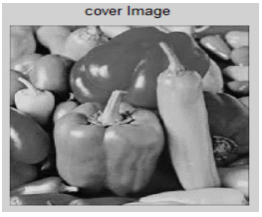
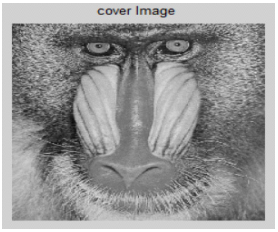
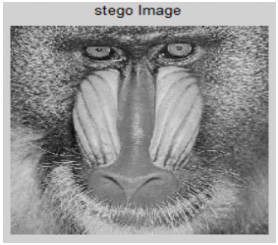
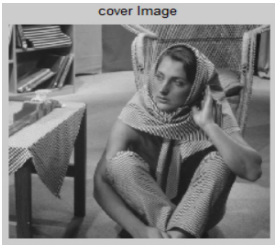
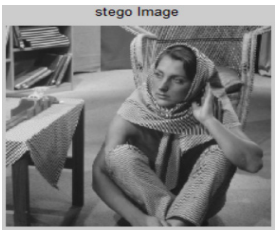
Images	Cover Image	Stego Image
Pepper		
Baboon		

Table 2. *Cont.*

Images	Cover Image	Stego Image
Barbara		
Boat		
Female		
Couple		
House		

4.1. Embedding Capacity

This measure estimates the total number of bits inserted in the cover image. It is based on Equation (10). Here, bpp refers to the bits per pixel.

$$bpp = \frac{Number\ of\ Bits\ Embedded}{Number\ of\ Pixels\ in\ the\ Cover\ Image} \tag{10}$$

In this work, the image is divided into four blocks, and each block's peak value is used for the data hiding. Thus, the total capacity in terms of BPP is presented in Table 3. The experimental results show that different images achieve different capacities due to different peak values. The outcome signals that House achieves the highest embedding capacity compared to the other images.

Table 3. Capacity for the standard dataset images.

Images	BPP
Pepper	0.9
Baboon	0.9
Barbara	0.9
Boat	0.9
Female	0.9
Couple	0.9
House	0.9
Tree	0.9
Airplane	0.9
Jellybeans	0.9
Splash	0.9
Oakland	0.9
Earth	0.9

4.2. Peak Signal-to-Noise Ratio (PSNR)

The PSNR computes the uniqueness between two images in decibels (dB). The PSNR is computed using Equation (11):

$$PSNR = 10\log_{10}\frac{Max^2}{MSE} \tag{11}$$

$$MSE(C_I, S_I) = \frac{1}{AB}\sum_{i=1}^{A}\sum_{j=1}^{B}(C(i,j) - S(i,j))^2 \tag{12}$$

Here, MSE is the mean square error. C_I and S_I denote the cover and stego images, respectively. In Table 4, for the different cover images, the PSNR value is presented. It is found that the Female image has achieved the highest PSNR compared to the other images due to less distance in the peak signal value and zero value available in the histogram for the image.

Table 4. PSNR for the standard dataset images.

Images	PSNR
Pepper	54.21
Baboon	54.19
Barbara	57.58
Boat	65.47
Female	66.42
Couple	64.70
House	56.33
Tree	59.92
Airplane	65.00
Jellybeans	64.79
Splash	58.50
Oakland	59.71
Earth	55.45

4.3. Structural Similarity Index Measure (SSIM) and Quality Index (Q)

The SSIM finds the measure of similarity between images [32]. Its value varies between −1 and 1. Table 5 shows the SSIM between the cover and stego images. It is estimated based on Equation (13). Here, A_{mn}, A_{mean}, B_{mn}, and B_{mean} are the means and variances for the images.

$$SSIM = \frac{\sum_{m=1}^{J}\sum_{n=1}^{K}(A_{mn} - A_{mean})(B_{mn} - B_{mean})}{\sqrt{\sum_{m=1}^{J}\sum_{n=1}^{K}((A_{mn} - A_{mean})^2)\sum_{n=1}^{k}\sum_{n=1}^{k}(B_{mn} - B_{mean})^2}} \tag{13}$$

Table 5. SSIM for the standard dataset images.

Images	SSIM
Pepper	1
Baboon	0.99
Barbara	1
Boat	1
Female	1
Couple	0.99
House	0.99
Tree	1
Airplane	1
Jellybeans	1
Splash	1
Oakland	0.99
Earth	0.99

The quality index (Q) is one of the metrics that finds the similarity between the cover and stego images. The highest value for Q is one. This can be achieved when two images are entirely equal. Q can be obtained using Equation (14):

$$Q = \frac{4\,\sigma_{xy}\,\bar{a}\,\bar{b}}{\left(\sigma_x^2 + \sigma_y^2\right)\left[(\bar{a})^2 + (\bar{b})^2\right]} \tag{14}$$

Here, σ_x and σ_y are the standard deviations, and $\bar{a}$ and $\bar{b}$ denote the means for the individual images.

4.4. Statistical Tests

In this section, statistical tests are applied to the cover and stego histograms to check the normal distribution using various tests, including (1) the two-sample *t*-test and (2) the Kolmogorov–Smirnov test. The two-sample *t*-test is applied to check whether the average difference between the two groups is significant or not. In steganography, the cover and stego image histograms are two groups in which the average difference is determined. There are two types of hypotheses: null and alternative. The null hypothesis suggests that the data in the vectors x and y come from an independent random sample from a normal distribution with equal mean and unknown variance.

Conversely, in the alternative hypothesis, x and y come from a sample with unequal mean. Similarly, the two-sample Kolmogorov–Smirnov test is applied to check whether the data in the cover and stego histograms in the vectors x and y come from the same continuous distribution. Based on the distribution, it is defined as the null hypothesis or the alternative hypothesis. Table 6 calculates the two-sample *t*-test and the Kolmogorov–Smirnov test for the different images. The results show that our proposed technique passes the statistical tests.

4.5. Analysis of PSNR, BPP, and Q

In this section, the outcomes of our work and the already-present histogram-shifting algorithms with respect to the PSNR, embedding capacity, and Q are computed. The experimental results show that the improved histogram-shifting reversible data embedding algorithm achieves better PSNR, acceptable embedding capacity, and superior Q value compared to existing techniques. Table 7 presents the results for PSNR, BPP, SSIM, and Q for the proposed technique and the techniques proposed by Zong [17] and Rajkumar and Vasuki [16]. The average PSNR is 58.70 dB with a 0.932-bit rate, which is much better than the existing techniques. Furthermore, the obtained SSIM and Q values are also encouraging as the average of the respective values lies between the range of 0.99 and 1.

Table 6. Two-sample *t*-test and Kolmogorov–Smirnov test.

Images	Two-Sample *t*-Test			Two-Sample Kolmogorov–Smirnov Test		
	H	P	CI	h	p	KS Statistic Test
Pepper	0	1	−125.77:125.77	0	1	0.0234
Baboon	0	1	−153.71:153.71	0	1	0.0313
Barbara	0	1	−139.99:139.99	0	1	0.0273
Boat	0	1	−222.31:222.32	0	1	0.0195
Female	0	1	−216.92:216.92	0	1	0.0195
Couple	0	1	−316.42:316.42	0	1	0.0156
House	0	1	−407.46:407.46	0	1	0.0234
Tree	0	1	−179.92:179.92	0	1	0.0195
Airplane	0	1	−294.76:294.76	0	1	0.0156
Jellybeans	0	1	−492.98:492.98	0	1	0.0078
Splash	0	1	−202.64:202.64	0	1	0.0273
Oakland	0	1	−231.67:231.67	0	1	0.0195
Earth	0	1	−179.38:179.38	0	1	0.0195

Table 7. Results for PSNR, bpp, and Q.

Images	Zong [17]			Rajkumar and Vasuki [16]			Proposed Technique		
	PSNR (dB)	Bit Rate	Q	PSNR (dB)	Bit Rate	Q	PSNR (dB)	Bit Rate	Q
Rice	49.07	0.0035	0.99	53.34	0.028	0.99	55.07	0.906	0.99
Barbara	47.87	0.0013	0.99	52.03	0.010	0.99	57.58	0.976	1
Boat	52.34	0.0014	0.99	56.90	0.011	0.99	65.47	0.987	0.99
House	37.17	0.0124	0.99	40.40	0.099	0.99	56.33	0.876	0.99
Mandrill	43.67	0.0017	0.99	47.47	0.014	0.99	54.19	0.854	0.99
Pepper	45.56	0.0018	0.99	55.44	0.015	0.99	54.21	0.932	0.99
Earth	47.45	0.0016	0.99	53.67	0.013	0.99	55.45	0.939	1
Jellybeans	48.98	0.0015	0.99	54.64	0.013	0.99	64.79	0.991	0.99
Airplane	49.34	0.0014	0.99	52.78	0.016	0.99	65.00	0.866	0.99
Tree	49.54	0.0016	0.99	55.45	0.019	0.99	59.92	0.963	0.99
Average	**47.04**	**0.00267**	**0.99**	**52.08**	**0.0225**	**0.99**	**58.70**	**0.932**	**0.99**

5. Conclusions and Future Research Direction

In this paper, a dynamic block-based, histogram shifting-based RDH technique is suggested to raise the embedding capacity and quality of stego images. Furthermore, embedding is performed based on a contrast strategy. To strengthen robustness, the secret data are scrambled using randomly generated keys, and a 256-bit key is generated based on the cover image's histogram. In addition, error correction codes are added to the encrypted data before embedding. The experimental results show that the proposed approach achieves better PSNR and embedding capacity than existing histogram-shifting algorithms. The devised work could be applicable in various real-life cases, mainly in medical applications, telemedicine, and secure and confidential communication systems. In the future, the primary focus will be to identify the optimal changes to achieve minimum stego quality reduction. Additionally, using neural network-based pixel selection approaches can be beneficial in selecting the optimal pixels for embedding the secret information.

Author Contributions: Conceptualization, S.K. and A.K.S.; Data curation, R.K.R.; Investigation, M.S. and A.K.S.; Methodology, S.K. and A.K.S.; Writing—review and editing, M.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work did not receive any funding directly or indirectly from any source or agency.

Data Availability Statement: Not applicable.

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

References

1. Megías, D.; Mazurczyk, W.; Kuribayashi, M. Data hiding and its applications: Digital watermarking and steganography. *Appl. Sci.* **2021**, *11*, 10928. [CrossRef]
2. Takaoğlu, M.; Özyavaş, A.; Ajlouni, N.; Alshahrani, A.; Alkasasbeh, B. A novel and robust hybrid blockchain and steganography Scheme. *Appl. Sci.* **2021**, *11*, 10698. [CrossRef]
3. Zakaria, A.A.; Hussain, M.; Wahab, A.W.A.; Idris, M.Y.I.; Abdullah, N.A.; Jung, K.-H. High-capacity image steganography with minimum modified bits based on data mapping and LSB substitution. *Appl. Sci.* **2018**, *8*, 2199. [CrossRef]
4. Darwis, D.; Junaidi, A.; Shofiana, D.A. A new digital image steganography based on center embedded pixel positioning. *Cybern. Inf. Technol.* **2021**, *21*, 89–104. [CrossRef]
5. Navadiya, C.; Sanghani, N. Comparative survey of digital image steganography spatial domain techniques. In *Data Science and Intelligent Applications: Proceedings of ICDSIA 2020*; Springer: Singapore, 2021; pp. 491–497.
6. Hussain, M.; Wahab, A.W.A.; Bin Idris, Y.I.; Ho, A.T.; Jung, K.-H. Image steganography in spatial domain: A survey. *Signal Process. Image Commun.* **2018**, *65*, 46–66. [CrossRef]
7. Puteaux, P.; Puech, W. A recursive reversible data hiding in encrypted images technique with a very high payload. *IEEE Trans. Multimed.* **2020**, *23*, 636–650. [CrossRef]
8. 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]
9. Kulkarni, R.; Dinesh, V.S.; Bhagya, R.; Bharathi, R. Difference expansion based reversible data hiding scheme for watermarking. *Int. J. Res. Eng. Sci. Manag.* **2021**, *4*, 193–195.
10. Chen, H.; Wang, J.; Zhou, Y.; Chang, T.; Shi, K.; Yuan, J. Improving the security of reversible data hiding using multiple histogram modification. *Math. Probl. Eng.* **2022**, *2022*, 7192697. [CrossRef]
11. Puteaux, P.; Puech, W. An efficient MSB prediction-based technique for high-capacity reversible data hiding in encrypted images. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 1670–1681. [CrossRef]
12. Kumar, S.; Gupta, A.; Walia, G.S. Reversible data hiding: A contemporary survey of state-of-the-art, opportunities and challenges. *Appl. Intell.* **2021**, *52*, 7373–7406. [CrossRef]
13. Faragallah, O.S.; Elaskily, M.A.; Alenezi, A.F.; El-Sayed, H.S.; Kelash, H.M. Quadruple histogram shifting-based reversible information hiding approach for digital images. *Multimed. Tools Appl.* **2021**, *80*, 26297–26317. [CrossRef]
14. Sahu, A.K.; Swain, G. A novel n-rightmost bit replacement image steganography technique. *3D Res.* **2019**, *10*, 2. [CrossRef]
15. He, W.; Xiong, G.; Wang, Y. Reversible Data hiding based on adaptive multiple histograms modification. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 3000–3012. [CrossRef]
16. Rajkumar, R.; Vasuki, A. Reversible and robust image watermarking based on histogram shifting. *Clust. Comput.* **2018**, *22*, 12313–12323. [CrossRef]
17. Zong, T.; Xiang, Y.; Natgunanathan, I.; Guo, S.; Zhou, W.; Beliakov, G. Robust histogram shape-based technique for image watermarking. *IEEE Trans. Circuits Syst. Video Technol.* **2014**, *25*, 717–729. [CrossRef]
18. Chang, I.-C.; Hu, Y.-C.; Chen, W.-L.; Lo, C.-C. High capacity reversible data hiding scheme based on residual histogram shifting for block truncation coding. *Signal Process.* **2015**, *108*, 376–388. [CrossRef]
19. Lin, J.; Chang, C.-C.; Horng, J.-H. Asymmetric data hiding for compressed images with high payload and reversibility. *Symmetry* **2021**, *13*, 2355. [CrossRef]
20. Yadav, P.; Mishra, N.; Sharma, S. A secure video steganography with encryption based on LSB technique. In Proceedings of the 2013 IEEE International Conference on Computational Intelligence and Computing Research, Enathi, India, 26–28 December 2013.
21. Saini, J.K.; Verma, H.K. A hybrid approach for image security by combining encryption and steganography. In Proceedings of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013), Shimla, India, 9–11 December 2013.
22. Singh, S.K.; Gopi, V.P.; Palanisamy, P. Image security using DES and RNS with reversible watermarking. In Proceedings of the 2014 International Conference on Electronics and Communication Systems (ICECS), Coimbatore, India, 13–14 February 2014.
23. Patel, K.; Utareja, S.; Gupta, H. Information hiding using least significant bit steganography and blowfish algorithm. *Int. J. Comput. Appl.* **2013**, *63*, 24–28. [CrossRef]
24. Jain, M.; Lenka, S.K.; Vasistha, S.K. Adaptive circular queue image steganography with RSA cryptosystem. *Perspect. Sci.* **2016**, *8*, 417–420. [CrossRef]
25. Rai, A.K.; Kumar, N.; Kumar, R.; Om, H.; Chand, S.; Jung, K.H. Intra-Block Correlation Based Reversible Data Hiding in Encrypted Images Using Parametric Binary Tree Labeling. *Symmetry* **2021**, *13*, 1072. [CrossRef]
26. Xu, S.; Horng, J.-H.; Chang, C.-C. Reversible data hiding scheme based on VQ prediction and adaptive parametric binary tree labeling for encrypted images. *IEEE Access* **2021**, *9*, 55191–55204. [CrossRef]
27. Aziz, F.; Ahmad, T.; Malik, A.H.; Uddin, M.I.; Ahmad, S.; Sharaf, M. Reversible data hiding techniques with high message embedding capacity in images. *PLoS ONE* **2020**, *15*, e0231602. [CrossRef] [PubMed]
28. Sahu, A.K. A logistic map based blind and fragile watermarking for tamper detection and localization in images. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *13*, 3869–3881. [CrossRef]
29. Volume 2: Aerials. Available online: http://sipi.usc.edu/database/database.php?volume=aerials&image=5#top (accessed on 19 August 2022).
30. Ayyappan, S.; Lakshmi, C. A review on reversible data hiding techniques. *Int. J. Appl. Eng. Res.* **2018**, *13*, 2857–2864.

31. Sahu, A.K.; Hassaballah, M.; Rao, R.S.; Suresh, G. Logistic-map based fragile image watermarking scheme for tamper detection and localization. *Multimed. Tools Appl.* **2022**, 1–32. [CrossRef]
32. Wang, J.; Mao, N.; Chen, X.; Ni, J.; Wang, C.; Shi, Y. Multiple histograms based reversible data hiding by using FCM clustering. *Signal Process.* **2019**, *159*, 193–203. [CrossRef]
33. Sahu, A.K.; Sahu, M.; Patro, P.; Sahu, G.; Nayak, S.R. Dual image-based reversible fragile watermarking scheme for tamper detection and localization. *Pattern Anal. Appl.* **2022**, 1–20. [CrossRef]
34. Zhou, K.; Ding, Y.; Bi, W. High-capacity PVO-based reversible data hiding scheme using changeable step size. *Multimed. Tools Appl.* **2020**, *80*, 1123–1141. [CrossRef]
35. Pan, Z.; Gao, E. Reversible data hiding based on novel embedding structure PVO and adaptive block-merging strategy. *Multimed. Tools Appl.* **2019**, *78*, 26047–26071. [CrossRef]
36. Cox, I.J.; Miller, M.L.; Bloom, J.A.; Fridrich, J.; Kalker, T. *Digital Watermarking and Steganography*; Morgan Kaufmann: Burlington, MA, USA, 2007.
37. Fallahpour, M.; Megias, D.; Ghanbari, M. Reversible and high-capacity data hiding in medical images. *IET Image Process.* **2011**, *5*, 190–197. [CrossRef]
38. Wang, X.; Li, L.; Chang, C.-C.; Huang, Y. Multi-level reversible data hiding for crypto-imagery via a block-wise substitution-transposition cipher. *J. Inf. Secur. Appl.* **2021**, *64*, 103067. [CrossRef]
39. Manikandan, V.; Masilamani, V. Histogram shifting-based blind watermarking scheme for copyright protection in 5G. *Comput. Electr. Eng.* **2018**, *72*, 614–630. [CrossRef]
40. Sahu, A.K.; Swain, G.; Sahu, M.; Hemalatha, J. Multi-directional block based PVD and modulus function image steganography to avoid FOBP and IEP. *J. Inf. Secur. Appl.* **2021**, *58*, 102808. [CrossRef]
41. Kumar, R.; Jung, K.-H. Enhanced pairwise IPVO-based reversible data hiding scheme using rhombus context. *Inf. Sci.* **2020**, *536*, 101–119. [CrossRef]
42. He, W.; Xiong, G.; Weng, S.; Cai, Z.; Wang, Y. Reversible data hiding using multi-pass pixel-value-ordering and pairwise prediction-error expansion. *Inf. Sci.* **2018**, *467*, 784–799. [CrossRef]
43. Sahu, A.K.; Gutub, A. Improving grayscale steganography to protect personal information disclosure within hotel services. *Multimedia Tools Appl.* **2022**, *81*, 30663–30683. [CrossRef]
44. Chang, J.; Ding, F.; Li, X.; Zhu, G. Hybrid prediction-based pixel-value-ordering technique for reversible data hiding. *J. Vis. Commun. Image Represent.* **2021**, *77*, 103097. [CrossRef]
45. Sahu, A.K.; Umachandran, K.; Biradar, V.D.; Comfort, O.; Hema, V.S.V.; Odimegwu, F.; Saifullah, M.A. A Study on Content Tampering in Multimedia Watermarking. *SN Comput. Sci.* **2023**, *4*, 222. [CrossRef]
46. Darehnaei, Z.G.; Shokouhifar, M.; Yazdanjouei, H.; Fatemi, S.M.J.R. SI-EDTL: Swarm intelligence ensemble deep transfer learning for multiple vehicle detection in UAV images. *Concurr. Comput. Pract. Exp.* **2021**, *34*, e6726.