mathematics

MDPI

Article

A Matrix Coding-Oriented Reversible Data Hiding Scheme Using Dual Digital Images

Jui-Chuan Liu [1], Ching-Chun Chang [2], Yijie Lin [1,*], Chin-Chen Chang [1,*] and Ji-Hwei Horng [3]

[1] Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan; p1200318@o365.fcu.edu.tw
[2] Information and Communication Security Research Center, Feng Chia University, Taichung 40724, Taiwan; ccc@fcu.edu.tw
[3] Department of Electrical Engineering, National Quemoy University, Kinmen 89250, Taiwan; horng@email.nqu.edu.tw
* Correspondence: p1263670@o365.fcu.edu.tw (Y.L.); ccc@o365.fcu.edu.tw (C.-C.C.)

Abstract: With the development of Internet technology, information security and data protection have become particularly important. Reversible data hiding is an effective technique for data integrity and privacy protection, and secret image sharing is a distinct research field within reversible data hiding. Due to the ability of sharing secret information between two receivers and the larger embedding capacity compared to the traditional reversible data hiding scheme, dual digital images have also attracted extensive research in the past decade. In this paper, we propose a reversible data hiding scheme based on matrix coding using dual digital images. By modifying the bits in the pixels, we can conceal three bits of the secret message in two pixels. In other words, the embedding rate reaches 1.5 bits per pixel (bpp). The experimental results demonstrate that our method has a significantly larger embedding capacity of 786,432 bits compared to previous similar methods while still maintaining acceptable image quality defined by a peak signal-to-noise ratio (PSNR) greater than 30 dB. The proposed scheme is suitable for applications required to pass a large amount of data but with minor security of image quality to be visually acceptable.

Keywords: reversible data hiding; matrix coding; dual digital images; steganography

MSC: 68U10

check for updates

Citation: Liu, J.-C.; Chang, C.-C.; Lin, Y.; Chang, C.-C.; Horng, J.-H. A Matrix Coding-Oriented Reversible Data Hiding Scheme Using Dual Digital Images. *Mathematics* **2024**, *12*, 86. https://doi.org/10.3390/math12010086

Academic Editors: Cheonshik Kim and Ki-Hyun Jung

Received: 11 November 2023
Revised: 5 December 2023
Accepted: 24 December 2023
Published: 26 December 2023

1. Introduction

Since the Internet age started, the Internet has dominated our daily lives, with a tremendous amount of data and information transmitted through the Internet and world wide web every single minute. Some of the data can contain sensitive or secretive information, which requires higher levels of protection to prevent illegal hacking or misusage.

Securing of personal information or industrial knowhow has become essential; hence, scholars are encouraged to find solutions to resolve these serious problems in order to safeguard the communication channels and give users peace of mind. Data hiding (DH) [1,2] is one of the essential research areas, which provides methodologies to protect data effectively. Depending on the applications, content owners and data hiders can choose assorted schemes suitable for their requirements. Some receivers may only need to extract secret messages; yet, others may want to fully recover the original media. Therefore, the data hiding is branched out into irreversible [3,4] and reversible [5,6] depending on whether the original media can be retrieved completely or not after data recovery. Because the full reversibility of the original media offers wider applicability, studies of reversible data hiding (RDH) [7–12] have become more popular in the recent decades.

Digital images are commonly used media for scientists to exercise and verify their concepts and approaches. Secret image sharing (SIS) technology was proved to be a proficient way to protect private images by generating multiple shares called image shadows. The idea of secret image sharing derived from secret sharing was proposed by Shamir back in 1979 [13]. The secret was shared and recovered by employing Lagrange interpolation. Yan et al. realized an SIS scheme based on the Chinese remainder theorem (CRT) [14] later on. With a twist of the SIS technique, a special edition of RDH using dual images was proposed by Chang et al. in 2007 [15]. Dual-image methods generate two stego images, which increase the safety of the secret data, visual image quality, and embedding capacity. Unless both stego images can be obtained simultaneously, the extraction of the secret data cannot be completed. Because dual image schemes can offer stronger safekeeping and recovery abilities, there is higher demand to discover innovative or improved solutions [16–20] to achieve either better visual quality of stego images or higher embedding capacity. Our novel scheme emphasizes enhancing the embedding capacity but with satisfactory image quality. The experimental results assured us that the embedding rates reached 1.5 bits per pixel (bpp). The contributions of this particular study are:

- The embedding capacity is significantly larger, which can be up to 786,432 bits.
- It is a suitable solution for applications requiring high embedding capacity but that can scarify the image quality to be visually acceptable.
- Both the process of embedding and the process of extraction are simple and have a satisfiable execution time. The shadow construction phase took 0.5242 s, while the secret message extraction and the image reconstruction phase took 0.9158 s.

In Section 2, we describe the fundamental concept of a matrix coding method to be utilized in the scheme. The details of data embedding and extraction are explained in Section 3, and the related experiments and analysis are presented in Section 4. At the end of the study, we summarize the findings and the potential future improvement in Section 5.

2. Related Work

In this section, we would like to refresh the principle of a matrix coding method [21], which was initially proposed by Chang et al. in 2008.

The matrix coding method adopts a parity check matrix H as shown in Equation (1). Suppose we have a 7-dimensional cover vector $v = [1010100]$ and a secret message $m = [110]$. According to Equation (2), we can calculate the $Syndrome = [110] \oplus [111] = [001]$. Then, we match the calculated syndrome in Table 1 to obtain the corresponding coset leader [1000000]. Finally, we can calculate the stego vector $v' = v \oplus Coset\ leader = [1010100] \oplus [1000000] = [0010100]$ through Equation (3). To summarize the above process, simply put, the stego vector $v\prime$ changes one bit in v according to the coset leader associated with the syndrome. In this way, the data embedding process is completed. The extraction process is simpler. According to Equation (4), the secret message $m' = Hv' = [110]$ can be easily extracted.

$$H = \begin{bmatrix} 0\,0\,0\,1\,1\,1\,1 \\ 0\,1\,1\,0\,0\,1\,1 \\ 1\,0\,1\,0\,1\,0\,1 \end{bmatrix}. \tag{1}$$

$$Syndrome = m \oplus Hv. \tag{2}$$

$$v' = v \oplus Coset\ leader. \tag{3}$$

$$m' = Hv'. \tag{4}$$

Table 1. The cosets of the matrix coding with the parity check matrix H.

Syndrome	000	001	010	011	100	101	110	111
Coset leader	0000000	1000000	0100000	0010000	0001000	0000100	0000010	0000001

Through the matrix coding method, we can modify only one bit in the vector to effectively embed three secret bits. This remarkable efficiency not only ensures minimal impact on the original data but also provides a high level of security in concealing sensitive information.

3. Proposed Scheme

The dual image technique is employed for the novel scheme. The shadow construction phase is described in Section 3.1, and the secret message extraction and original image reconstruction phase are detailed in Section 3.2. Two covered images CI_1 and CI_2 are duplicates from the original image OI with size $m \times n$. A secret message S is embedded to covered images CI_1, CI_2 to create shadow images SI_1 and SI_2. The shadow images are sent to designated receivers. When both shadow images appear at the same time, both the recovered secret message RS and the recovered image RI can be extracted. The scheme process is illustrated in Figure 1.

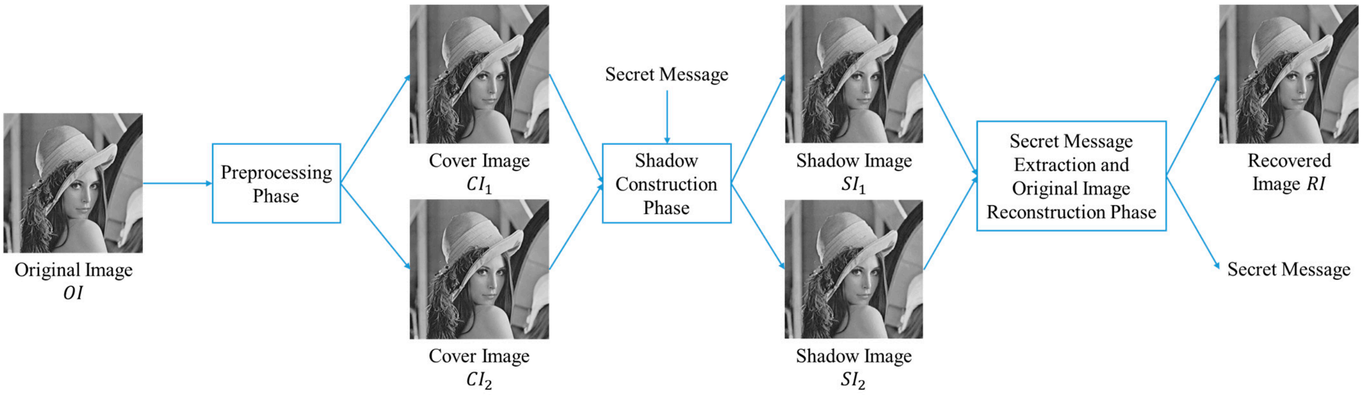


Figure 1. Process of the proposed scheme.

To better understand the process, we show two examples in Figure 2 exercising the whole flow. In Figure 2a, the pixel values of the current pixel pair are converted to their binary format $(10100010)_2$ from 162 first, four LSBs $(0010)_2$ are extracted from the cover pixel of the cover image CI_1 and three LSBs $(010)_2$ are extracted from the cover pixel of the cover image CI_2 to form a 7-dimensional cover vector (0010010). There are three secret bits that can be embedded into the cover vector to create a 7-dimentional shadow vector (0000010) using the matrix coding technique. We split the shadow vector into four bits (0000) and three bits (010) and replace the corresponding pixels: four LSBs in the shadow pixel of the shadow image CI_1 and three LSBs in the shadow pixel of the shadow image CI_2. A recovery bit is the fourth LSB in the shadow pixel of the shadow image CI_2, which records the original bit value of the bit altered during data embedding. By bitwise comparison of two shadow pixels, we can recover the original pixel value with the help of the recovery bit. The pixel value $(10100000)_2$ in the shadow image CI_1 is 160, and the pixel value $(10101010)_2$ in the shadow image CI_2 is 170 after the decimal format conversion.

Figure 2b shows an example similar to Figure 2a, except it is a case when the current pixel count is even. The 7-dimensional cover vertex is composed of three LSBs from the cover pixel of the cover image CI_1 and four LSBs from the cover pixel of the cover image CI_2. After the shadow vertex is generated, the split is three bits for the shadow pixel of the shadow image CI_1 and four bits for the shadow pixel of the image CI_2. The recovery bit becomes the fourth LSB in the shadow pixel of the shadow image CI_1. The exchanging of the bit-split patterns based on odd or even pixel count is to minimize the visual distortion of the shadow images and to keep a balanced visual quality of the two shadows.

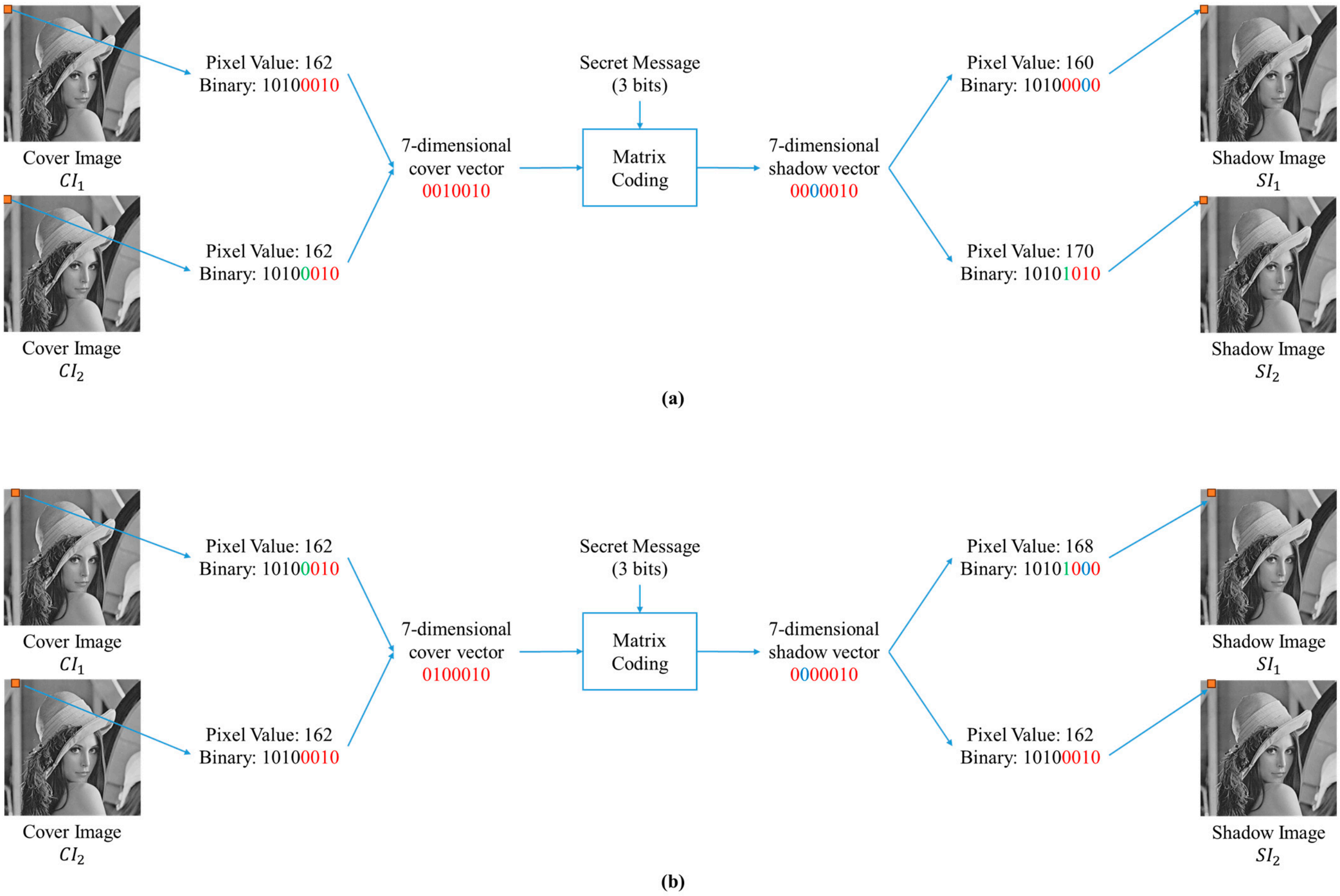


Figure 2. Examples of the proposed flow: (**a**) the odd pixel count, (**b**) the even pixel count.

3.1. Shadow Construction Phase

To embed a secret message, we move through a shadow construction phase to generate two shadow images using the matrix code method described in Section 2.

In order to meet the requirement of being reversible, we use a pixel pair, one from cover image $CI_1 = \left\{p_{1,0},\ p_{1,1},\ \cdots,\ p_{1,(n\times m)-1}\right\}$ and the corresponding pixel from $CI_2 = \left\{p_{2,0},\ p_{2,1},\ \cdots,\ p_{2,(n\times m)-1}\right\}$, where n is the total number of pixels in images. $S = \{s_0,\ s_1,\ \cdots,\ s_{k,} \cdots,\ s_{r-1}\}$, where $s_k \in \{0, 1\}$, and r is the length of secret bits. When a cover pixel pair $pp_i = (p_{1i},\ p_{2i})$, the two pixel values for the pair are converted into binary format and represented as $p_{1,i} = \left(b_{1,7}, b_{1,6},\ b_{1,5},\ \cdots,\ b_{1,0}\right)_2$ and $p_{2,i} = \left(b_{2,7}, b_{2,6},\ b_{2,5},\ \cdots,\ b_{2,0}\right)_2$. A 7-dimensional cover vector v_i is then constructed by using the least significant bits (LSBs) in these two cover pixels according to Equation (5).

$$v_i = \begin{cases} \left(b_{1,3},\ b_{1,2}, b_{1,1},\ b_{1,0},\ b_{2,2},\ b_{2,1}, b_{2,0}\right),\ if\ i\ is\ odd \\ \left(b_{1,2},\ b_{1,1}, b_{1,0},\ b_{2,3},\ b_{2,2},\ b_{2,1}, b_{2,0}\right),\ if\ i\ is\ even \end{cases}, \tag{5}$$

where i is the index of the current pixel, and $0 \le i \le (n \times m) - 1$. The i can also be treated as the current pixel count pc. Therefore, pc is the same as i. Algorithm 1 describes the construction of shadow images SI_1 and SI_2 step by step.

Algorithm 1. Shadow Construction

```
Input      An original image $OI$ and a secret message $S$.
Output     Shadow images $SI_1$, $SI_2$.
Step 1     Duplicate the original image and create two cover images $CI_1$, $CI_{2.}$
Step 2     Set the initial secret bit count $bc = 0$
Step 3     FOR each $pc$, $0 \leq pc \ \leq (n \times m) - 1$
Step 3a        Obtain three secret bits $s_{bc} + s_{bc+1} + s_{bc+2}$
Step 3b        Select current cover pixel pair $pp_i = \left(p_{1,i}, \ \ p_{2,i}\right)$, where $i = pc$, pixel $p_{1,i}$
           from the cover image $CI_1$ and pixel $p_{2,i}$ from the cover image $CI_2$.
Step 3c        Convert pixel values $p_{1,i}$ and $p_{2,i}$ to binary.
Step 3d        Construct the 7-dimensional cover vector $v_i$ using Equation (5).
Step 3e        Calculate the *Syndrome* and obtain the shadow vector $sv_i$ using
           Equations (2) and (3).
Step 3f        Let $v_i = \left(vb_{i,6}, \ vb_{i,5} \ , \ vb_{i,4} \ , \ vb_{i,3} \ , \ vb_{i,2} \ , \ vb_{i,1} \ , \ vb_{i,0}\right)$ and
                   $sv_i = \left(sb_{i,6} \ , \ sb_{i,5} \ , \ sb_{i,4} \ , \ sb_{i,3} \ , \ sb_{i,2} \ , \ sb_{i,1} \ , \ sb_{i,0}\right)$
Step 3g        Set the recovery bit $b_0$ to store the original bit value for recovery as
           below,
                 $is\ Same = \left(\left(sb\ _{i,5} \ , \ sb_{i,4} \ , \ sb_{i,3}\right) == \left(sb\ _{i,2} \ , \ sb_{i,1} \ , \ sb_{i,0}\right)\right)$
           IF *is Same*
                               $b_0 = vb_{i,6}$
           ELSE
                               $j = 0$
           WHILE $j < 3$
           IF $sb_{i,j+3} \neq \ sb_{i,j}$
                               $b_0 = vb_{i,j}$
           BREAK
           END
                               $j = j + 1$
           END
           END
Step 3h        Set shadow pixel pair $spp_i = \left(sp_{1,i} \ , sp_{2,i}\right)$, where $sp_{1,i,}$ is the current
           pixel in shadow images $SI_1$ and $sp_{2,i,}$ is the current pixel in shadow images
           $SI_2$ according to
           IF $pc$ is odd
           $sp_{1,i} \ = (b_{1,7}, \ b_{1,6}, \ b_{1,5}, b_{1,4}, \ sb_{i,6}, \ sb_{i,5}, \ sb_{i,4}, \ sb_{i,3})$
           $sp_{2,i} \ = (b_{2,7}, b_{2,6}, \ b_{2,5}, b_{2,4}, b_0, \ sb_{i,2}, \ sb_{i,1}, \ sb_{i,0}\Big)$
           ELSE
           $sp_{1,i} = (b_{1,7}, \ b_{1,6}, \ b_{1,5}, b_{1,4}, \ b_0, \ sb_{i,6}, \ sb_{i,5} \ , \ sb_{i,4})$
           $sp_{2,i} = (b_{2,7}, b_{2,6}, b_{2,5}, b_{2,4}, \ sb_{i,3}, \ sb_{i,2}, \ sb_{i,1}, sb_{i,0})$
           END
           END
Step 4     Export shadow images $SI_1$, $SI_2$.
```

3.2. Secret Message Extraction and Original Image Reconstruction Phase

The secret extraction and recovery of the original image is simple and straight forward, which can save computation time. After having both of the shadow images, a shadow vector can be constructed using Equation (5). Secret bits can be extracted from the shadow vector by looking up Table 1 directly. The shadow vector is the coset value in the matrix coding table to obtain the corresponding syndrome, which is the desired three secret bits to be extracted. By using the value of the recovery bit, the shadow vector is converted back to the original vector (or it can be called a recovered vector). The original vector (or recovered vector) is split into two sets of bits and restores the LSBs of the pixel back to the original image (or the recovered image). To clarify the process of extraction and recovery, Algorithm 2 explains the steps in detail.

Algorithm 2. Secret Message Extraction and Original Image Reconstruction

```
Input     Dual shadow images $SI_1$, $SI_2$.
Output    Recovered image $RI$, and recovered secret message $RS$.
Step 1    Duplicate $SI_1$ to $RI$.
Step 2    Set the initial secret bit count $bc = 0$.
Step 3    FOR each $pc$, $0 \leq pc \leq (n \times m) - 1$
              Set $i = pc$
Step 3a       Set the current shadow pixel pair $spp_i = \left(sp_{1,i}\ ,\ sp_{2,i}\right)$, where $sp_{1,i,}$ is
          the current pixel in the shadow image $SI_1$ and $sp_{2,i,}$ is the current pixel in
          the shadow images $SI_2$.
Step 3b       Convert pixel values $sp_{1,i}$ and $sp_{2,i}$ to binary and let
          $sp_{1,\ i} = \left(sb_{1,7},\ sb_{1,6},\ sb_{1,5}, sb_{1,4},\ sb_{1,3}, sb_{1,2}, sb_{1,1}, sb_{1,0}\right)$ and
          $sp_{2,\ i} = \left(sb_{2,7},\ sb_{2,6},\ sb_{2,5}, sb_{2,4},\ sb_{2,3}, sb_{2,2}, sb_{2,1}, sb_{2,0}\right)$.
Step 3c       Construct the shadow vector $sv_i$ =
          $\left(sb_{i,6}\ ,\ sb_{i,5}\ ,\ sb_{i,4}\ ,\ sb_{i,3}\ ,\ sb_{i,2}\ ,\ sb_{i,1}\ ,\ sb_{i,0}\right)$ using Equation (5) and use it as
          the coset leader.
Step 3d       Extract three secret bits $s_{bc} + s_{bc+1} + s_{bc+2}$ based on the coset leader in
          Table 1 and append them to recovered secret message $RS$.
Step 3e       $bc = bc + 3$
Step 3f       Obtain the original bit value $b_0$,
          IF $pc$ is odd
                  $b_0 = sb_{2,3}$
          ELSE
          $b_0 = sb_{1,3}$
          END
Step 3g       Let $rp_i = (rb_{i,7},\ rb_{i,6},\ rb_{i,5},\ rb_{i,4},\ rb_{i,3},\ rb_{i,2},\ rb_{i,1},\ rb_{i,0})$
Step 3h       Set the altered bit value back to its original value by the following:
                  $is\ Same = true$
                  $j = 0$
          WHILE $j < 3$
          IF $sb_{i,j+3} \neq\ sb_{i,j}$
                  $rb_{i,j} = b_0$
                  $is\ Same = false$
          BREAK
          END
                  $j = j + 1$
          END
          IF $is\ Same = true$
                  $rb_{i,3} = b_0$
          END
          END
Step 4    Export recovered images $RI$ and recovered secret message $RS$.
```

3.3. Processing Flow Examples

Figure 3 shows the embedding, extraction, and recovery procedures using two examples. The flow examples (a) and (b) first illustrate how bits are extracted from two cover images, how an original vector is formed, and how shadow images are set based on intermediate-created shadow vector after secret embedding using matrix coding. Then, they show how a shadow vector is formed from shadow images to recover hidden secrets and show the recovered vector and the recovered image by replacing the altered bit value with the recovery bit value as well.

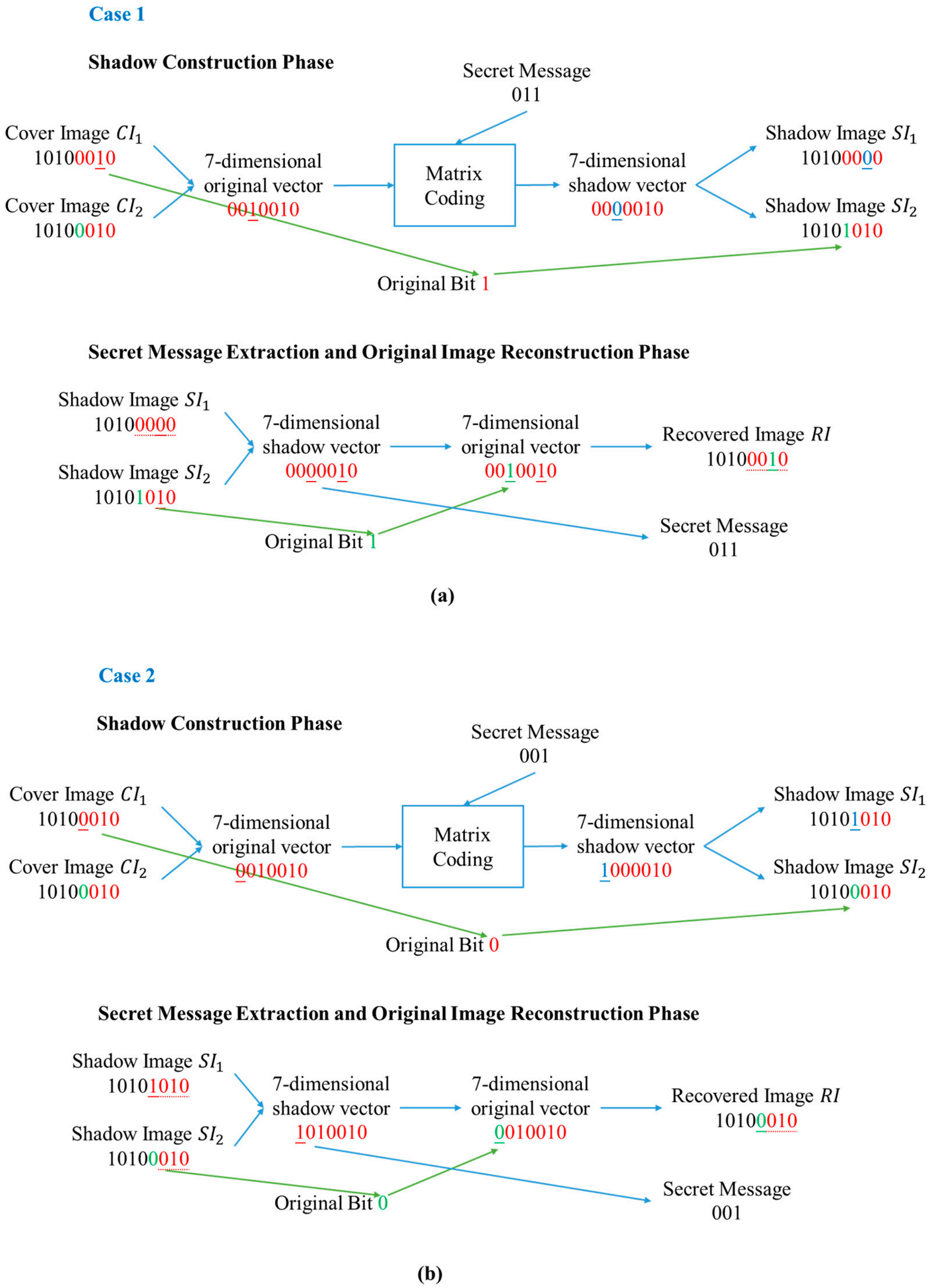


Figure 3. Examples for embedding, extraction, and recovery: (**a**) the odd pixel count, (**b**) the even pixel count.

Let us take the example (a), which is the case of dealing with an odd number of pixels. During the shadow construction phase, the two cover pixels are $(10100010)_2$. A 7-dimensional cover vector $(0010010)_2$ is formed by four LSBs of a pixel from the cover image 1 and three LSBs of a pixel from the cover image 2. Assume the secret bits are $(011)_2$, and through lookup Table 1, the syndrome $(0010000)_2$ is the coset leader corresponding to the secret bits $(011)_2$ according to Equation (2). Perform XOR calculation with the original vector, and a 7-dimensional shadow vector $(0000010)_2$ is generated and split to update the four LSBs in the shadow pixel 1 and the three LSBs in the shadow pixel 2. The fourth bit from the left of the shadow pixel 2 is the recovery bit, which records the original bit value (1) for the second bit from the left of the cover pixel 1. In the secret message extraction and the image reconstruction phase, a shadow vector is formed by the two pixels of two shadow images the same way we formed the cover vector from two pixels of two cover images. We can then extract the secret bits $(011)_2$ by using Table 1 directly. As for recovery of the original image, we can convert the shadow vector back to the original vector using the saved recovery bit value and update the four LSBs with any one of the shadow pixels to recover the original pixel, which can also be called a recovered pixel. Figure 3b moves through the same process with an example dealing with an even number of pixels.

4. Experimental Results

In this section, we evaluate the performance of our proposed matrix coding using a dual digital images scheme. As depicted in Figure 4, we selected eight standard gray images for our experiments. Our experiments were conducted on a laptop running the Windows 10 operating system with MATLAB R2023b. The laptop is equipped with a 3.20 GHz AMD Ryzen 7 CPU and 16 GB of RAM. We also compared the experimental results with other advanced reversible data hiding schemes based on dual images and our scheme demonstrated a significant advantage in embedding capacity (EC).

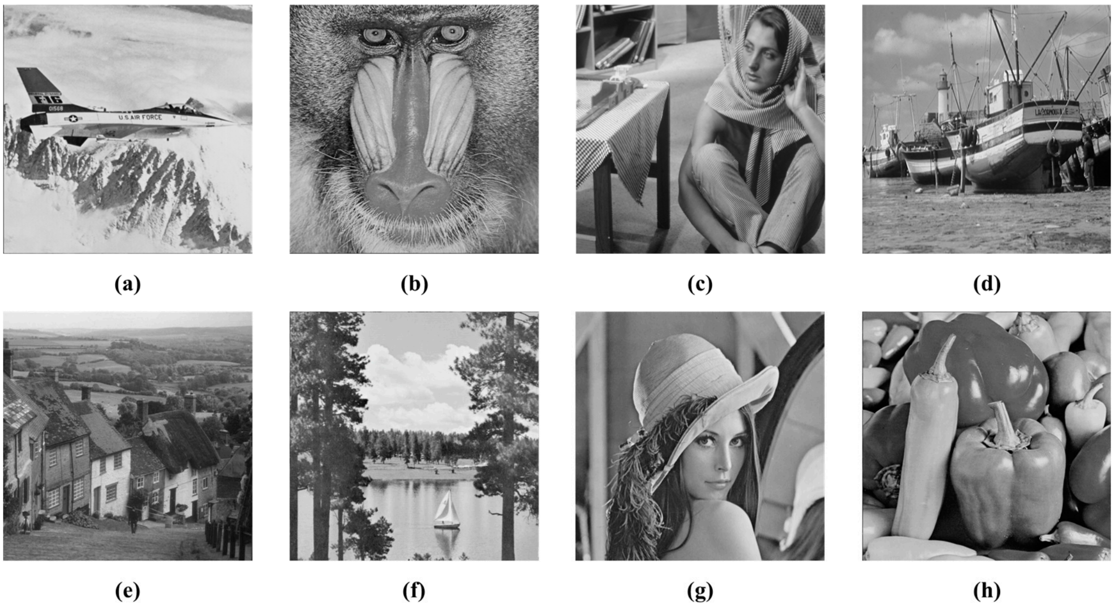


Figure 4. Eight 512 × 512 test images: (**a**) airplane, (**b**) baboon, (**c**) Barbara, (**d**) boat, (**e**) Goldhill, (**f**) lake, (**g**) Lena, (**h**) peppers.

The Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity Index (SSIM) are widely used as visual quality indicators for evaluating the performance of data hiding. The PSNR is employed to assess the difference in visual quality between two images and is calculated using Equations (6) and (7). In Equation (7), m and n represent the size of the image, while i and j represent individual pixels. In this context, I represents the original image, and K represents the shadow image. A smaller Mean Square Error (MSE) corresponds to less distortion in the image, indicating higher quality in the constructed image. Conversely, because the PSNR and MSE are inversely proportional, a higher PSNR value reflects the same conclusion.

$$PSNR = 10 \times log_{10} \frac{255^2}{MSE} \tag{6}$$

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} [I(i,j) - K(i,j)]^2 \tag{7}$$

The SSIM is an indicator that quantifies the similarity between two images. It is primarily used to assess the similarity and dissimilarity between two images, denoted as x and y. As shown in Equation (8), the SSIM algorithm separately compares the luminance, contrast, and structure of two images and then combines them using weighted products. In this equation, μ_x and μ_y represent the mean luminance, σ_x and σ_y denote the standard deviation of the luminance, σ_{xy} represents the covariance of x and y, and C is a constant used to maintain stability. The closer the SSIM is to 1, the higher the similarity between the two images.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)}. \tag{8}$$

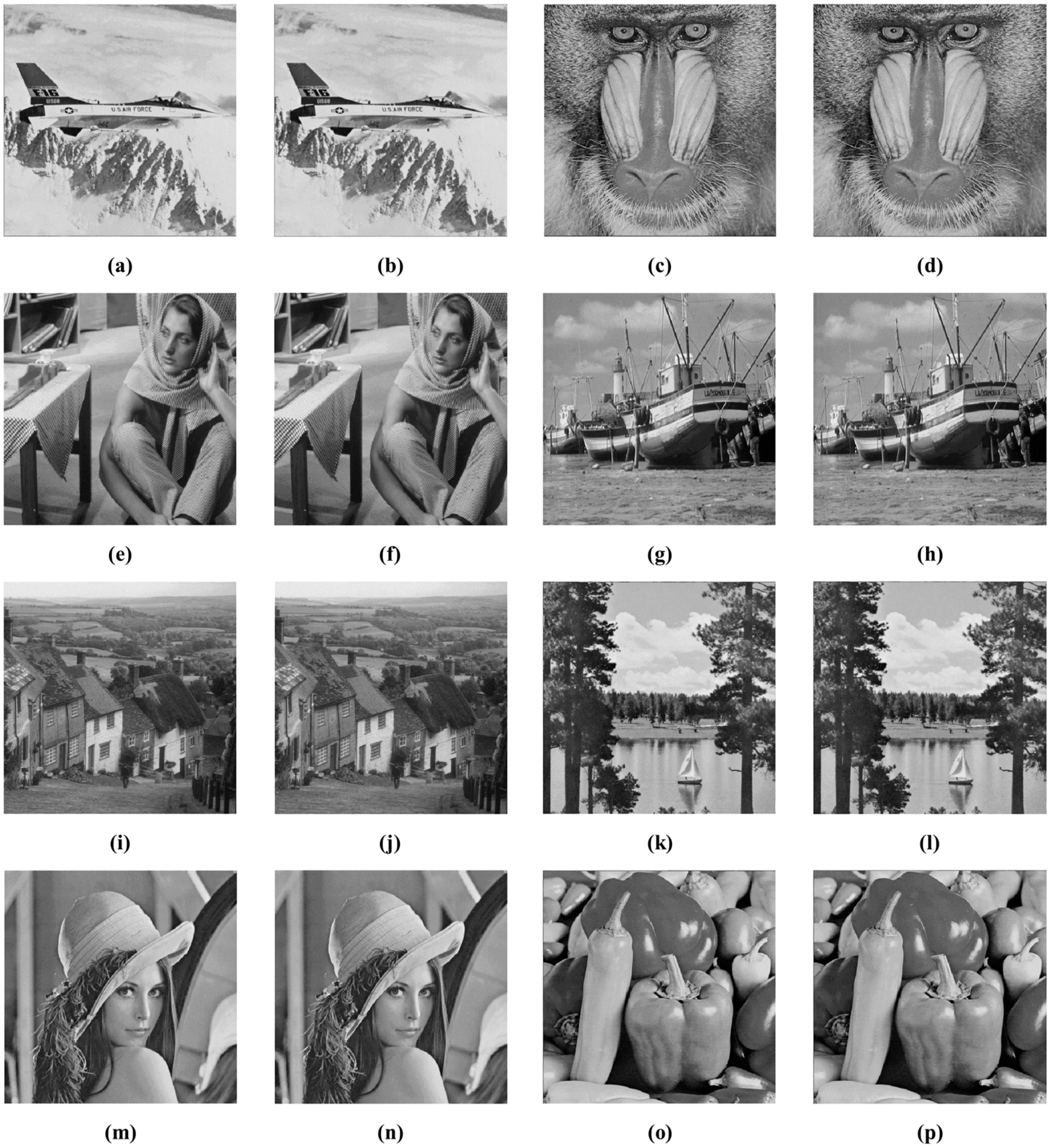
Figure 5 illustrates the shadow image constructed by our innovative matrix coding scheme. Clearly, the disparity between the constructed shadow image and the original image is minimal. It is challenging for us to discern any perceptible distortion with the naked eye, underscoring the superior visual quality achieved by our scheme. Table 2 illustrates the results obtained using our proposed matrix coding scheme to construct shadow 1 and shadow 2 from test images. It calculates the PSNR and SSIM values between these shadow images and the original image, as well as their average values. The average PSNR is approximately 36.34 dB, which is generally considered challenging to distinguish with the naked eye when it exceeds 30; these data support our conclusion. Furthermore, the average SSIM value is remarkably high at 0.9227, approaching 1. This indicates that the shadows constructed by our proposed scheme closely resemble the original images, confirming their excellent visual quality. These outstanding results substantiate the effectiveness of our solution and demonstrate its superiority in preserving image fidelity.

Table 2. Proposed scheme for PSNR and SSIM on different images.

Images	**PSNR (dB)**			**SSIM**		
	Shadow 1	**Shadow 2**	**Average**	**Shadow 1**	**Shadow 2**	**Average**
Airplane	36.36	36.35	36.35	0.8990	0.8984	0.8987
Baboon	36.33	36.34	36.33	0.9645	0.9644	0.9645
Barbara	36.36	36.36	36.36	0.9313	0.9313	0.9313
Boat	36.30	36.27	36.28	0.9259	0.9255	0.9257
Goldhill	36.32	36.33	36.32	0.9274	0.9279	0.9277
Lena	36.41	36.37	36.39	0.9030	0.9026	0.9028
Lake	36.34	36.36	36.35	0.9253	0.9256	0.9255
Peppers	36.36	36.36	36.36	0.9053	0.9053	0.9053
Average	36.35	36.34	36.34	0.9227	0.9226	0.9227

Table 3 presents a comparison of the performance indicators between our scheme and other schemes based on reversible data hiding using dual images. Our primary focus is on the EC and PSNR. The embedding rate is expressed in bits per pixel (bpp), calculated as shown in Equation (9), where M and N represent the image dimensions. The embedding capacity is divided by all pixels to signify how many bits can be embedded in each pixel. The experimental results demonstrate that the embedding capacity of our proposed scheme reaches 786,432 bits, which is equivalent to 1.5 bpp calculated as $\frac{786{,}432}{512\times512}$ using Equation (9). The EC of the novel scheme significantly exceeds that of other schemes. When compared to a scheme with the largest embedding capacity, ours is nearly 50% higher than the one with 557,339 bits. Even with our PSNR above 36 dB, it can be still lower than that of other solutions. However, this is consistent with the laws of nature. A larger embedding capacity inherently entails more modifications, resulting in greater distortion. However, our PSNR remains above 30, meeting the criteria for high visual quality. It is challenging for the naked eye to discern any distortion, making this trade-off acceptable in light of the significantly increased embedding capacity.

$$bpp = \frac{EC}{M \times N} \tag{9}$$



(a) (b) (c) (d) (e) (f) (g) (h) (i) (j) (k) (l) (m) (n) (o) (p)

Figure 5. Shadow images of eight test images, with shadow 1 on the left and shadow 2 on the right: (**a**,**b**) airplane, (**c**,**d**) baboon, (**e**,**f**) Barbara, (**g**,**h**) boat, (**i**,**j**) Goldhill, (**k**,**l**) lake, (**m**,**n**) Lena, (**o**,**p**) peppers.

Table 3. Comparison of the maximum EC, bpp, and PSNR values with other reversible data hiding scheme based on dual images.

Scheme	Indicator	Barbara	Goldhill	Lena	Peppers
proposed scheme	EC	786,432	786,432	786,432	786,432
	bpp	1.50	1.50	1.50	1.50
	$PSNR_1$	36.36	36.32	36.41	36.36
	$PSNR_2$	36.36	36.33	36.37	36.36
	$PSNR_{AVG}$	36.36	36.32	36.39	36.36
Qin et al. [16]	EC	557,339	557,194	557,052	557,245
	bpp	1.06	1.06	1.06	1.06
	$PSNR_1$	52.12	52.12	52.11	51.25
	$PSNR_2$	41.58	41.58	41.58	41.52
	$PSNR_{AVG}$	46.85	46.85	46.85	46.39
Lu et al. [17]	EC	524,288	524,288	524,288	524,192
	bpp	1.00	1.00	1.00	1.00
	$PSNR_1$	49.14	49.17	49.13	49.11
	$PSNR_2$	49.11	49.09	49.12	49.08
	$PSNR_{AVG}$	49.13	49.13	49.13	49.10
Jana et al. [19]	EC	74,752	74,752	75,752	73,728
	bpp	0.14	0.14	0.14	0.14
	$PSNR_1$	51.86	51.86	51.85	51.84
	$PSNR_2$	51.96	51.97	51.56	51.94
	$PSNR_{AVG}$	51.91	51.92	51.71	51.89
Kim et al. [20]	EC	524,288	524,288	524,288	524,288
	bpp	1.00	1.00	1.00	1.00
	$PSNR_1$	54.12	54.16	54.14	54.15
	$PSNR_2$	48.14	48.11	48.13	48.12
	$PSNR_{AVG}$	51.13	51.14	51.14	51.14

Table 4 shows the execution time of our proposed scheme in the secret message extraction and original image reconstruction phase. It is evident that the execution time is consistently within 1 s at every stage demonstrating the great performance of our scheme.

Table 4. The execution time of our proposed scheme.

Phase	Execution Time (s)
Shadow Construction Phase	0.5242
Secret Message Extraction and Original Image Reconstruction Phase	0.9158

5. Conclusions

In this paper, we propose a reversible data hiding scheme with a high embedding capacity using matrix coding based on dual images. Our solution only requires modifying or not modifying one bit, enabling us to conceal three bits of a secret message in two pixels. The experimental results demonstrate that this solution significantly increases the embedding capacity when compared to other similar methods, allowing for up to

786,432 bits, which is equivalent to 1.5 bpp, all while maintaining a high level of visual quality. This illustrates the superiority and applicability of our scheme.

Applications that require dual sharing of information between two and only two receivers, such as a couple who share secret arrangements, to recover the original media can consider utilizing our scheme. In the future, we will investigate different types of matrix coding to improve the embedding capacity or to improve the visual quality.

Author Contributions: Conceptualization, J.-C.L., Y.L. and C.-C.C. (Chin-Chen Chang); methodology, J.-C.L., Y.L. and C.-C.C. (Chin-Chen Chang); software, Y.L.; validation, Y.L.; writing—original draft preparation, J.-C.L. and Y.L.; writing—review and editing, J.-C.L., Y.L., C.-C.C. (Chin-Chen Chang), J.-H.H. and C.-C.C. (Ching-Chun Chang). All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

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

References

1. Kumar, R.; Chand, S. A new image steganography technique based on similarity in secret message. In Proceedings of the Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), Noida, India, 26–27 September 2013; IET: Stevenage, Hertfordshire, UK, 2013; pp. 376–379. [CrossRef]
2. Sahu, A.K.; Swain, G. An optimal information hiding approach based on pixel value differencing and modulus function. *Wirel. Pers. Commun.* **2019**, *108*, 159–174. [CrossRef]
3. Bender, W.; Gruhl, D.; Morimoto, N.; Lu, A. Techniques for data hiding. *IBM Syst. J.* **1996**, *35*, 313–336. [CrossRef]
4. Moulin, P.; O'Sullivan, J.A. Information-theoretic analysis of information hiding. *IEEE Trans. Inf. Theory* **2003**, *49*, 563–593. [CrossRef]
5. Celik, M.U.; Sharma, G.; Tekalp, A.M.; Saber, E. Lossless generalized-LSB data embedding. *IEEE Trans. Image Process.* **2005**, *14*, 253–266. [CrossRef] [PubMed]
6. Zhang, W.; Hu, X.; Li, X.; Yu, N. Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression. *IEEE Trans. Image Process.* **2013**, *22*, 2775–2785. [CrossRef]
7. Lin, C.C.; Liu, X.L.; Tai, W.L.; Yuan, S.M. A novel reversible data hiding scheme based on AMBTC compression technique. *Multimed. Tools Appl.* **2015**, *74*, 3823–3842. [CrossRef]
8. Sun, W.; Lu, Z.M.; Wen, Y.C.; Yu, F.X.; Shen, R.J. High performance reversible data hiding for block truncation coding compressed images. *Signal Image Video Process.* **2013**, *7*, 297–306. [CrossRef]
9. Chen, K.M. High capacity reversible data hiding based on the compression of pixel differences. *Mathematics* **2020**, *8*, 1435. [CrossRef]
10. 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]
11. Mittal, S.; Goyal, S.; Aggarwal, S.; Kumar, R. Interpolative AMBTC based reversible data hiding in encrypted images using rhombus mean. In Proceedings of the 2023 International Conference on Device Intelligence, Computing and Communication Technologies (DICCT), Dehradun, India, 17–18 March 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 451–456. [CrossRef]
12. Kumar, R.; Sharma, D.; Dua, A.; Jung, K.H. A review of different prediction methods for reversible data hiding. *J. Inf. Secur. Appl.* **2023**, *78*, 103572. [CrossRef]
13. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
14. Yan, W.; Ding, W.; Dongxu, Q. Image sharing based on Chinese remainder theorem. *J. North China Univ. Technol.* **2000**, *12*, 6–9.
15. Chang, C.C.; Kieu, T.D.; Chou, Y.C. Reversible data hiding scheme using two steganographic images. In Proceedings of the TENCON 2007—2007 IEEE Region 10 Conference, Taipei, Taiwan, 30 October–2 November 2007; IEEE: Piscataway, NJ, USA, 2007; pp. 1–4. [CrossRef]
16. Qin, C.; Chang, C.C.; Hsu, T.J. Reversible data hiding scheme based on exploiting modification direction with two steganographic images. *Multimed. Tools Appl.* **2015**, *74*, 5861–5872. [CrossRef]
17. Lu, T.C.; Tseng, C.Y.; Wu, J.H. Dual imaging-based reversible hiding technique using LSB matching. *Signal Process.* **2015**, *108*, 77–89. [CrossRef]
18. Huang, C.T.; Weng, C.Y.; Shongwe, N.S. Capacity-Raising Reversible Data Hiding Using Empirical Plus–Minus One in Dual Images. *Mathematics* **2023**, *11*, 1764. [CrossRef]
19. Jana, B.; Giri, D.; Kumar Mondal, S. Dual image based reversible data hiding scheme using (7, 4) hamming code. *Multimed. Tools Appl.* **2018**, *77*, 763–785. [CrossRef]

20. Kim, C.; Yang, C.N.; Zhou, Z.; Jung, K.H. Dual efficient reversible data hiding using Hamming code and OPAP. *J. Inf. Secur. Appl.* **2023**, *76*, 103544. [CrossRef]
21. Chang, C.C.; Kieu, T.D.; Chou, Y.C. A high payload steganographic scheme based on (7, 4) hamming code for digital images. In Proceedings of the 2008 International Symposium on Electronic Commerce and Security, Guangzhou, China, 3–5 August 2008; IEEE: Piscataway, NJ, USA, 2008; pp. 16–21. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.