mathematics

MDPI

Article

MRA-VSS: A Matrix-Based Reversible and Authenticable Visual Secret-Sharing Scheme Using Dual Meaningful Images

Chia-Chen Lin [1], En-Ting Chu [1], Ya-Fen Chang [2,*] and Ersin Elbasi [3,*]

[1] Department of Computer Science and Information Engineering, National of Chin-Yi University of Technology, Taichung 411030, Taiwan; ally.cclin@ncut.edu.tw (C.-C.L.); lb2t2002@gm.student.ncut.edu.tw (E.-T.C.)
[2] Department of Computer Science and Information Engineering, National Taichung University of Science and Technology, Taichung 411030, Taiwan
[3] College of Engineering and Technology, American University of the Middle East, Egaila 54200, Kuwait
[*] Correspondence: cyf@nutc.edu.tw (Y.-F.C.); ersin.elbasi@aum.edu.kw (E.E.);
Tel.: +886-422196320 (Y.-F.C.); +965-2225-1400 (ext. 2172) (E.E.)

Abstract: Reversible data hiding (RDH) is an approach that emphasizes the imperceptibility of hidden confidential data and the restoration of the original cover image. To achieve these objectives at the same time, in this paper, we design a matrix-based crossover data hiding strategy and then propose a novel matrix-based RDH scheme with dual meaningful image shadows, called MRA-VSS (matrix-based reversible and authenticable visual secret-sharing). Each pixel in a secret image is divided into two parts, and each part is embedded into a cover pixel pair by referring to the intersection point of four overlapping frames. During the share construction phase, not only partial information of the pixel in a secret image but also authentication codes are embedded into the corresponding cover pixel pair. Finally, two meaningful image shadows are derived. The experimental results confirm that our designed MRA-VSS successfully embeds pixels' partial information and authentication code into cover pixel pairs at the cost of slight distortion during data hiding. Nevertheless, the robustness of our scheme under the steganalysis attack and the authentication capability of our scheme are also proven.

Keywords: reversible data hiding; reference matrix; dual images; crossover data hiding; rule singular (RS); authenticable; visual secret-sharing

MSC: 68U10

check for updates

Citation: Lin, C.-C.; Chu, E.-T.; Chang, Y.-F.; Elbasi, E. MRA-VSS: A Matrix-Based Reversible and Authenticable Visual Secret-Sharing Scheme Using Dual Meaningful Images. *Mathematics* **2024**, *12*, 3532. https://doi.org/10.3390/math12223532

Academic Editors: Jonathan Blackledge and Antanas Cenys

Received: 9 October 2024
Revised: 31 October 2024
Accepted: 11 November 2024
Published: 12 November 2024

1. Introduction

Due to the rapid progress of digital processing technology and the booming of social media platforms, the amount of multimedia information transmitted over the Internet in our daily life is exponentially increasing. However, the public property of the Internet makes it a challenge for intellectual property rights because both authorized and unauthorized users can access the transmitted message. Moreover, unauthorized users may not only eavesdrop but also tamper and duplicate the transmitted data. To protect the confidentiality of the transmitted data, conventional cryptographic techniques [1], such as RSA, DES, AES, and so on, are mainly used. In general, cryptographic algorithms consist of two parts: encryption and decryption. Encryption is a procedure of converting plaintext into incomprehensible machine code known as ciphertext. In contrast, decryption is the procedure of restoring meaningless data into meaningful data. Once the sensitive data has been encrypted in advance, the confidentiality of the transmitted data is guaranteed. Unfortunately, the meaningless format becomes another clue to attract the malicious attackers. Data hiding is another approach to imperceptibly conceal secret data in cover media, such as audio, video, image, and text, etc., without drawing malicious users' attention. After the hiding procedure, the cover media are transformed into stego media, and they can be transmitted through the Internet because the difference between the cover media and stego image is slightly tinny and it is hard for attackers to tell the difference. No matter how tinny distortion is caused during the hiding procedure, in conventional data hiding schemes, the original cover media cannot be completely restored and the possible applications are limited.

To support more applications' scenarios, such as applications of satellite images, military, and medical image processing, reversible data hiding (RDH), which is one subcategory of data hiding techniques, becomes an impressive technique because it guarantees an original cover image can be completely restored once the hidden secret data are extracted from the stego image. In 2003, Tian first proposed difference expansion (DE)-based RDH [2] by concealing secrets into the original difference value between the pair of neighboring pixels. Three years later, Ni et al. designed the first histogram shifting (HS)-based RDH scheme [3] by finding the peak points and zero points and adopting pixel shifting operation. Inspired by the research teams of Tian [2] and Ni et al. [3], many DE-based and HS-based RDH schemes have been proposed in the last decade. In general, a single image was adopted as cover media to carry secret data until Chang et al. introduced a dual-image-based RDH approach [4] in 2007.

In the dual-image-based RDH approach, two stego images are involved to carry the secret data. The ordinary phases of a data hiding scheme, data hiding and data extraction, are changed to share construction and secret extraction/restoration phases in a dual-image-based RDH scheme. In other words, two stego images may share the same or different source(s) of the cover image(s) to carry the secret data in a dual-image-based RDH scheme. Because the secret data are embedded separately in two stego images, the likelihood of malicious users successfully extracting the hidden information is reduced compared to traditional reversible data hiding methods. However, the requirements for the extraction process in a dual-image-based RDH scheme are quite stringent. The successful extraction of the hidden data depends on having both stego images. Thus, if a secret owner uses this method and distributes the two stego images to different participants, those participants must work together to extract the hidden information.

In Chang et al.'s scheme [4], they first transform binary secret data into quinary digits, and then, a transformed quinary digit is concealed by a pixel pair at a time by distributing them into two corresponding stego images. Next, Zhang and Wang's exploiting modification direction (EMD) matrix [5] was adopted to conceal two quinary digits into a cover pixel pair and derived two stego images finally. During the share construction phase, the main diagonal and the secondary diagonal directions of the EMD matrix were referred to. Eventually, they approximately provided an embedding rate (ER) of 1 bit per pixel (bpp) and acceptable visual quality of stego images. In 2013, Lee and Huang [6] also worked with quinary digits but using combinations of pixel orientations located at two stego images. Their hiding strategy kept the difference between each pixel value of the stego image and the cover image plus or minus one, which also improves their ER as 1.07 bpp and PSNR as 49.6 dB.

Except the EMD matrix [5], various matrices have been designed to either enhance the security of the hidden data or improve the hiding capacity. Two representative matrices are the Sudoku matrix [7] and turtle shell (TS) reference matrix [8]. In 2008, Chang et al. [7] first applied the Sudoku matrix to design a dual-image-based RDH scheme. In their scheme, secret data were first transformed into novenary digits considering a Sudoku matrix can be divided into 3 × 3 non-overlapping blocks. Because each cover pixel pair carried a novenary digit, in average, their ER was about 1.5 bpp, while the PNSR only remained 44 dB. It is noted that, with the structure feature of the Sudoku matrix, the amount of possible solutions of a Sudoku matrix is vast so that the security of the hidden data was achieved. In 2018, Liu and Chang [8] first applied a TS reference matrix to design their dual-image-based RDH. In their scheme, two cover pixels formed a pair and decided on a coordinate in the TS reference matrix. Then, four categories were defined based on which position of TS the coordinate maps to. They also designed a dynamic data hiding based on different categories and made sure the coordinate formed by the stego pixel pair remained at a certain region. Therefore, the main advantage of their scheme is that both the reversibility and authentication capability can be achieved simultaneously, but their ER is only around 1 bpp. Different from previous research teams, Huynh et al. [9] focused on enlarging the payload size. In their scheme, they first converted each pixel of the grayscale secret image into novenary digits. Then, they concealed a novenary digit into a cover pixel pair and derived two stego images. They successfully increased the ER to 2 bpp at a cost of image quality of about 36 dB, which is relatively lower than those of existing schemes.

In 2022, Lin et al. [10] proposed a novel dual-image-based RDH using TS reference matrix. In general, their idea was inspired by Liu and Chang [11], and they sought to make progress on the authentication capability and visual quality of stego images. To achieve the authentication ability, they also defined a predetermined region in advance and made sure the stego pixel pair remained in this region so that, during the extraction and verification phases, the receivers could judge whether the pixel pairs of stego images were tampered with. They reshaped the region to provide the authentication mechanism while reducing the potential distortion during the share construction phase. With the authentication mechanism, the average PSNR was about 48 dB, while the highest ER remained 1 bpp and the average detection ratio (DR) was about 97%. The results showed that 97% of the tampered area can be successfully identified with their scheme. In the same year, Chang et al. [12] proposed a position-aware guided dual-image-based RDH scheme that combines the concepts of TS and sunflower region to enhance the adaptability of data embedding. The average PSNR of this scheme is approximately 46.98 dB, with a maximum embedding rate of 1.25 bpp.

Later, Lin et al. [13] proposed a dual-image-based RDH scheme based on asymmetric orientation combination. They fully utilized the directional differences between different images by adjusting the orientation combinations of pixels within the images to achieve effective data embedding while ensuring a high embedding capacity and visual quality. Their approach significantly enhances the security and stability of data hiding. Under the condition of maximum embedding capacity with a certification mechanism, their scheme maintains an average PSNR of approximately 41.79 dB, a maximum embedding rate of 1.82 bpp, and an average detection rate of about 91%. Solak et al. [14] applied the most significant bit (MSB) and center shifting techniques to design their dual-image-based RDH scheme. Their scheme offered the maximum embedding capacity up to 2.96 bpp at the cost of the average PSNR remaining at about 28.36 dB, although the reversibility of the hidden secret data and the original cover image were guaranteed.

In 2024, Kim et al. [15] introduced an improved dual-image-based RDH scheme that integrates embedding direction adjustment (EMD) technology with an optimized least significant bit (LSB) replacement strategy. This approach achieved an average PSNR of 50.74 dB and a maximum embedding rate of about 1.1 bpp. Lee et al. [16] developed a dual-image RDH approach based on vector coordinates and triangle order coding (TOC). Their scheme achieved an average PSNR of 34.78 dB at high embedding rates, with a maximum embedding capacity of up to 2.5 bpp. Subsequently, Liu et al. [17] designed a novel dual-image RDH method using matrix coding with an average PSNR of 36.36 dB and a maximum embedding rate of 1.5 bpp.

Although dual-image-based RDH schemes have achieved notable improvements in either hiding capacity or image quality, the openness of the Internet makes the transmitted stego images vulnerable to tampering by malicious attackers. In these schemes, if one of the stego images is altered, it must be resent to retrieve the hidden secret data, which is particularly critical in application fields like healthcare or the military, where data integrity and usability are essential requirements. To improve the usability of received stego images and facilitate smooth data extraction, it is essential to detect any malicious modifications that may have occurred.

However, despite the significance of authenticable capability, this requirement has not been thoroughly examined, as evidenced by the summary of characteristics for seven representative dual-image-based RDH schemes [6,8–11,13,15] presented in Table 1. Moreover, the data in Table 1 indicate that improving the authenticable capability often affects either the image quality of the stego images or the hiding capacity. To address this challenge, this study incorporates verification codes during the data embedding process and introduces an additional verification algorithm to help the receiver detect any tampering of stego images during transmission. This approach enhances both the security of network transmission and the usability of the received stego images. The proposed verification mechanism allows the receiver to confirm the accuracy and integrity of the data without significantly compromising the image quality, which is a key innovation of our proposed MRA-VSS scheme.

Table 1. Characteristics of seven representative schemes [6,8–11,13,15].

Schemes	bpp	PSNR for *SI1*	PSNR for *SI2*	Reversibility	Authenticable
[6]	1.07	49.62	49.63	Yes	No
[8]	1.00	51.76	45.71	Yes	Yes
[9]	1.99	39.32	39.16	Yes	No
[10]	1.00	50.17	47.15	Yes	Yes
[11]	1.25	49.38	49.55	Yes	No
[13] [1]	1.48	45.54	45.88	Yes	Yes
[15]	1.10	50.35	51.03	Yes	No

[1] The threshold r was set to 3 and 7 in [13], and the PSNR values presented for *SI1* and *SI2* were average PSNRs.

In order to detect tampered pixels of stego images more effectively, and improve the payload size and PSNRs of stego images at the same time, in this paper, we designed a novel authenticable dual-image-based RDH based on the combination of diagonal pairing and intersection point, called MRA-VSS, a matrix-based reversible and authenticable visual secret-sharing scheme. In our scheme, a reference matrix was first established. Then, four frames that share a common intersection and overlapping boundaries were created. Each pixel pair from the grayscale secret image was divided into two parts, which were hidden using a cover pixel pair along with an authentication code. The diagonal pairing policy of two stego images was derived. In other words, our MRA-VSS scheme not only enhances the authenticity of stego images but also aligns with current trends in RDH technology. It enables the complete recovery of the original cover image after extracting the hidden data while preserving image quality, thereby underscoring the significant role of RDH in the field of data hiding technology.

The main contributions of the proposed MRA-VSS scheme are listed as follows:

(1) Two stego images maintain a good visual quality;
(2) Effectively authenticates the tampered pixels of stego images;
(3) Achieves robustness under RS analysis and the pixel value difference histogram (PDH) analysis.

The rest of this paper is organized as follows. Section 2 briefly reviews Chang et al.'s scheme [4] because their scheme is a pioneer in the field of dual-image-based RDH approach. The proposed authenticable dual-image-based RDH scheme MRA-VSS is described in Section 3. The experimental results are presented in Section 4. The conclusions are drawn in Section 5.

2. Review of Authenticable Dual-Image-Based Schemes Using a Reference Matrix

Inspired by Zhang and Wang's EMD data hiding scheme [5], Chang et al. [4] proposed the first dual-image-based RDH scheme using EMD reference matrix. In Chang et al.'s scheme, the secret data are transformed into a sequence of quinary digits, and a 256 × 256 EMD matrix M_{ref} indicates how to modify each cover pixel pair to conceal a quinary digit according to Equation (1):

$$M_{ref}(P_i, P_j) = (P_i + 2 \times P_j) \bmod 5 \quad (1)$$

where P_i and P_j are two neighboring pixels in a cover image and form a pixel pair. Using the mapping function defined in Equation (1), each pixel pair in a cover image can map one and only one element in the EMD matrix M_{ref}.

During the share construction phase, for a given cover pixel pair (P_i, P_j), it is mapped to an element denoted as $M_{ref}(P_i, P_j)$ of matrix M_{ref} at the intersection of column P_i and row P_j. Later, a 5 × 5 block B in matrix M_{ref} is formed using the mapped intersection as the central point and eight elements located at two diagonal lines are selected as the reference points, as shown in Figure 1. It is noted that two diagonal lines of block B include five different values ranging from 0 to 4.

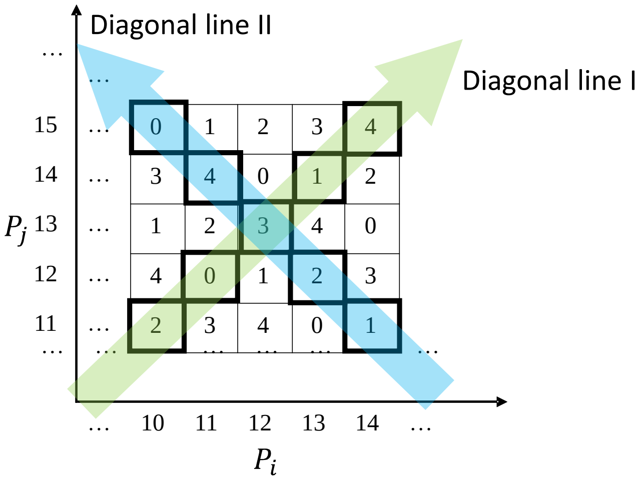


Figure 1. Diagram for Chang et al.'s candidate elements' selection.

The five elements situated at a diagonal line indicate a set of candidates for a pixel pair located at the same coordinate as $M_{ref}(P_i, P_j)$ of a share. By modifying the cover pixel pair $M_{ref}(P_i, P_j)$ to any element located at two diagonal lines, a quinary secret digit is concealed. Assume there are two quinary digits denoted as d_1 and d_2, $M_{ref}(P'_i, P'_j) = d_1$ and $M_{ref}(P''i, P''j) = d_2$. For share 1, the cover pixel pair $M_{ref}(P_i, P_j)$ is changed to $M_{ref}(P'_i, P'_j)$. For share 2, the cover pixel pair $M_{ref}(P_i, P_j)$ is changed to $M_{ref}(P''i, P''j)$. During extraction and restoration, the hidden secret quinary digits can be easily extracted by mapping the pixel pairs of shares to the EMD matrix M_{ref}. Finally, the corresponding central points can be derived and pixel pairs of the cover image can be restored.

Although Chang et al.'s scheme [4] does not provide an authentication mechanism, their share construction operation is simple and efficient. Inspired by their scheme, many scholars have subsequently proposed various schemes, trying to pursue breakthroughs in storage, security, and verifiability.

3. Proposed MRA-VSS Scheme

To increase the hiding capacity, and improve the verifiability while maintaining a competitive visual quality of shares, in this paper, a novel dual-image-based RDH scheme called MRA-VSS using a reference matrix and the combination of diagonal pairing and intersection point is proposed. The flowchart of the proposed dual-image-based RDH scheme is demonstrated in Figure 2.

With our proposed MRA-VSS, a secret grayscale image that is half the size of the cover image can be concealed via two meaningful shares. In this section, the definitions of the proposed MRA-VSS scheme are presented first in Section 3.1. Then, the details of the share construction, and secret extraction and verification phases are described in the following two subsections. The verification of integrity is presented in Section 3.4. Finally, an example is demonstrated in Section 3.5 to provide a better explanation for our proposed MRA-VSS scheme.

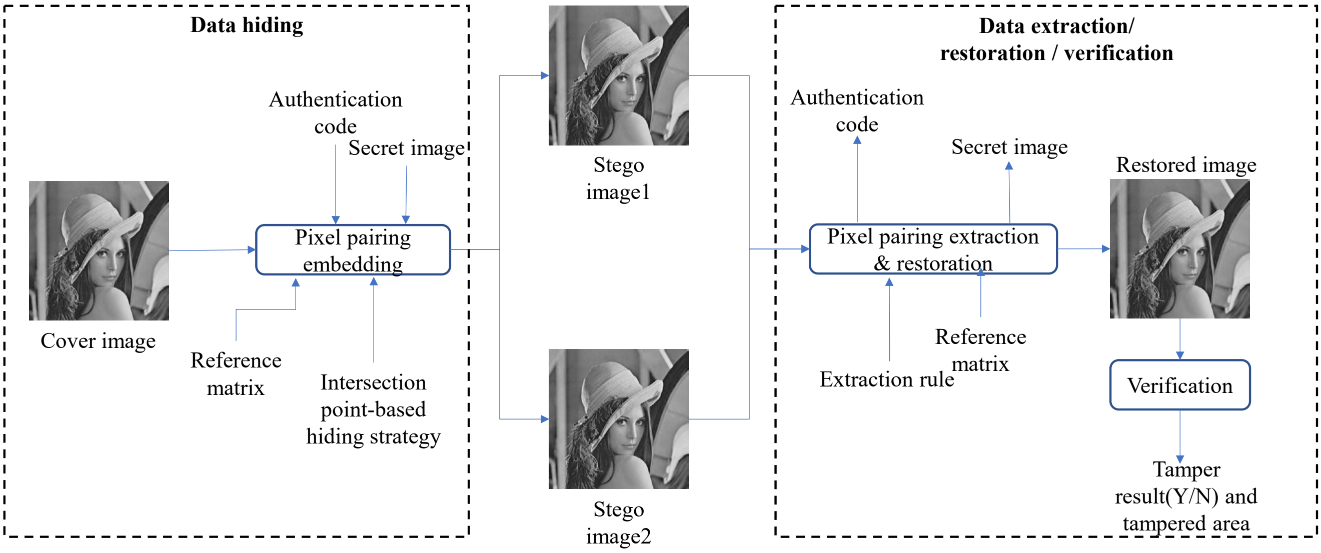


Figure 2. Flowchart of our proposed dual-image-based RDH called MRA-VSS.

3.1. *Definitions*

In our proposed MRA-VSS scheme, there are two important structures: one is the reference matrix M_{ref} and the other is the four frames within the matrix. In this section, the related definitions of these two structures are provided.

3.1.1. Reference Matrix $\mathrm{M_{ref}}$

Following the pixels' values of a grayscale image, ranging from 0 to 255, for the reference matrix M_{ref}, the value of X-axis ranges from 0 to 255, and the value of Y-axis also ranges from 0 to 255. The cellular values of reference matrix M_{ref} are defined according to the following rules:

Rule 1: The values in each row increase sequentially from 0 to 8 from left to right.

Rule 2: The values of each row are repeated in the numerical order of (0, 1, 2, 3, 4, 5, 6, 7, 8).

Rule 3: From the bottom row to the top, the starting value of each row repeats the numerical order of 0, 3, and 6 in sequence.

Finally, a matrix M_{ref} served as a reference matrix is constructed for data embedding, as shown in Figure 3.

3.1.2. Four Overlapping Frames

For a given cover pixel pair (P_i, P_j), such as (4,5), pixel P_i maps to the X-axis of matrix M_{ref} and pixel P_j maps to the Y-axis of matrix M_{ref}. $M_{ref}(P_i, P_j)$ serves as the intersection point and four overlapping frames are then constructed, as shown in Figure 3. Each frame overlaps with its neighboring frames with three neighboring pixels, and the intersection point pixel is the one that is covered with four frames. Four frames are denoted as Red, Green, Yellow, and Blue. The Red frame is located on the upper right up, and the rest three frames are Green, Yellow, and Blue in a counterclockwise direction order.

3.2. *Construction of Dual Stego Images with Our Proposed Matrix-Based Crossover Data Hiding Strategy*

To increase the hiding capacity while maintaining the reversibility of the cover image and competitive visual quality of two shares, a matrix-based crossover data hiding method is proposed in this subsection. Our proposed matrix-based crossover data hiding strategy comprises nine steps, as follows:

Step 1: Read two consecutive adjacent pixels (P_i, P_j) from the cover image *CI* as the cover pixel-pair and read four secret bits s_1, s_2, s_3, and s_4 from the secret bit stream *S*, where $I = 1$ to W, $j = 1$ to H, W is the width of the cover image, and H is the height of the cover image.

Step 2: Find the MSBs of P_i and P_j, and perform XOR operator to obtain one-bit *ac* serving as the authentication code.

Step 3: Construct the reference matrix M based on the construction rules described in Section 3.1.

Step 4: Duplicate the cover pixel pair (P_i, P_j) to two copies (P_{1i}, P_{1j}) and (P_{2i}, P_{2j}), where (P_{1i}, P_{1j}) belongs to stego image *SI1* and (P_{2i}, P_{2j}) belongs to stego image *SI2*.

Step 5: Segment the four secret bits (s_1, s_2, s_3, and s_4) and one-bit *ac* into two units $U1 = (s_1, s_2)$ and $U2 = (s_3, s_4, ac)$ and transform each unit into the decimal value $D_{U1} = decimal(s_1, s_2)$ and $D_{U2} = decimal(s_3, s_4, ac)$, respectively:

$$D_{U1} = decimal(U1), \tag{2}$$

$$D_{U2} = decimal(U2), \tag{3}$$

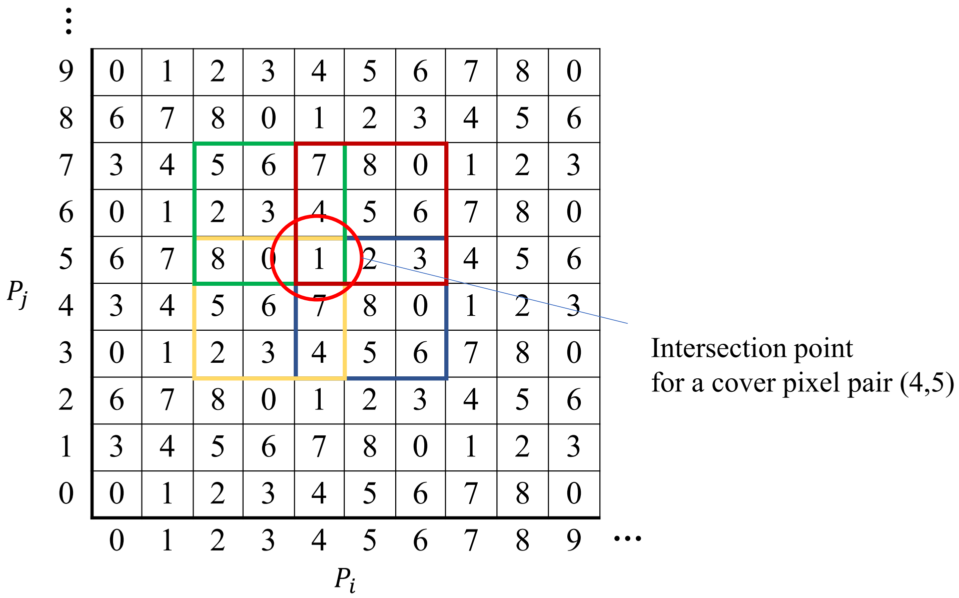
where *decimal* () is the decimal conversion function.

Step 6: Map the pixel pair (P_{1i}, P_{1j}) to matrix M_{ref}, set M_{ref} (P_{1i}, P_{1j}) as the intersection point, and then construct four frames according to the definitions provided in Section 3.1.

Step 7: Select a frame for the pixel pair (P_{1i}, P_{1j}) according to the following rules:

$$\text{frame} = \begin{cases} \text{Red frame}, & \text{if } D_{U1} = 0 \\ \text{Blue frame}, & \text{if } D_{U1} = 1 \\ \text{Green frame}, & \text{if } D_{U1} = 2 \\ \text{Yellow frame}, & \text{otherwise} \end{cases} \tag{4}$$

where D_{U1} is the decimal representation of unit $U1$, and $U1$ contains the first two secret bits s_1 and s_2 of the selected four successive secret bits.



P_j										
9	0	1	2	3	4	5	6	7	8	0
8	6	7	8	0	1	2	3	4	5	6
7	3	4	5	6	7	8	0	1	2	3
6	0	1	2	3	4	5	6	7	8	0
5	6	7	8	0	1	2	3	4	5	6
4	3	4	5	6	7	8	0	1	2	3
3	0	1	2	3	4	5	6	7	8	0
2	6	7	8	0	1	2	3	4	5	6
1	3	4	5	6	7	8	0	1	2	3
0	0	1	2	3	4	5	6	7	8	0
	0	1	2	3	4	5	6	7	8	9

Figure 3. Example of an intersection point for a cover pixel pair (4, 5) and four corresponding embedding frames. The red frame is the top-right frame, the green frame is the top-left frame, the yellow frame is the bottom-left frame, and the blue frame is the bottom-right frame.

Step 8: Find a pixel pair (P'_{1i}, P'_{1j}) of stego image *SI1* from the frame determined in Step 7, and make sure $M_{ref}(P'_{1i}, P'_{1j}) = D_{U2}$, where D_{U2} is the decimal representation of unit $U2$, and $U2$ contains the last two secret bits, s_3 and s_3, of the selected four successive secret bits that are read in Step 1 and one-bit authentication code *ac* of the cover pixel pair (P_i, P_j).

Step 9: Modify (P_{2i}, P_{2j}) of stego image *SI2* to (P'_{2i}, P'_{2j}) so that the frame where (P'_{2i}, P'_{2j}) located at is at the opposite direction of the frame to which (P'_{1i}, P'_{1j}) of stego image *SI1* belongs. Also, (P'_{2i}, P'_{2j}) is located at the center position of its frame.

Step 10: Output (P'_{1i}, P'_{1j}) and (P'_{2i}, P'_{2j}) as the pixel pair of stego images *SI1* and *SI2*, respectively.

Step 11: Judge whether the process of the cover pixel pairs and the secret data stream is completed; if it is not, return to Step 1. Otherwise, collect all outputted stego pixel pairs of stego images *SI1* and *SI2*, and then, form stego images *SI1* and *SI2*, respectively. Finally, two stego images are sent to two different participants separately.

Note that the matrix M_{ref} does not need to be sent along with the stego image because the recipients can reconstruct the matrix M_{ref} based on the pre-shared construction knowledge regarding matrix M_{ref}. However, there is one assumption that must be held in advance to extract the hidden confidential data and restore the original cover image, which is that two participants must co-work and share his/her received stego image.

3.3. Recovery of Secret Data and Cover Image

When the dual stego images *SI1* and *SI2* are obtained, one recipient shares his/her received stego image with the other recipient and the extraction of hidden secret data and restoration of the cover image begins. The steps of the recovery of secret data and cover image are listed below:

Step 1: Read two consecutive adjacent pixels (P'_{1i}, P'_{1j}) of stego image *SI1* and (P'_{2i}, P'_{2j}) of stego image *SI2*.

Step 2: Map (P'_{1i}, P'_{1j}) and (P'_{2i}, P'_{2j}) of stego images *SI1* and *SI2* to matrix M_{ref}.

Step 3: Find the intersection point (P'_i, P'_j) based on the pixel pair (P'_{2i}, P'_{2j}) according to the following rules:

$$\left(P'_i, P'_j\right) = \begin{cases} \left(P'_{1i}+1, P'_{1j}+1\right), \text{ if frame of } \left(P'_{2i}, P'_{2j}\right) \text{ is Red} \\ \left(P'_{1i}-1, P'_{1j}-1\right), \text{ if frame of } \left(P'_{2i}, P'_{2j}\right) \text{ is Blue} \\ \left(P'_{1i}-1, P'_{1j}+1\right), \text{ if frame of } \left(P'_{2i}, P'_{2j}\right) \text{ is Green} \\ \left(P'_{1i}+1, P'_{1j}-1\right), \text{ otherwise} \end{cases} \tag{5}$$

Step 4: Find D'_{U1} according to the following rules:

$$D'_{U1} = \begin{cases} 0, \text{ if frame of } \left(P'_{1i}, P'_{1j}\right) \text{ is Red} \\ 1, \text{ if frame of } \left(P'_{1i}, P'_{1j}\right) \text{ is Blue} \\ 2, \text{ if frame of } \left(P'_{1i}, P'_{1j}\right) \text{ is Green} \\ 3, \text{ otherwise} \end{cases} \tag{6}$$

Transform D'_{U1} into a binary representation so that the first two hidden secret bits s'_1 and s'_2 are obtained.

Step 5: Find $D'_{U2} = M_{ref}(P'_{2i}, P'_{2j})$ and transform D'_{U2} into a binary representation. Finally, the last two hidden secret bits s'_3 and s'_4 and one-bit ac′ are obtained.

Step 6: Output the intersection point (P'_i, P'_j) as the restored cover pixel pair and output the extracted four secret bits s'_1, s'_2, s'_3, and s'_4 and one-bit ac′.

Step 7: Judge whether the process of the pixel pairs of stego images *SI1* and *SI2* is completed; if it is not, return to Step 1. Otherwise, collect all restored pixel pairs and then form a restored cover image, collect all extracted secret bits, and form an extracted secret bit stream. Finally, collect all extracted authentication code *ac*′s and form an extracted authentication map for later integrity verification.

3.4. Verification of the Integrity of Stego Images

The matrix-based data hiding strategy demonstrated in Section 3.2 always guarantees there are two relations of the relative position of two stego pixel pairs that are satisfied when they map to matrix M_{ref}: (1) both overlap with each other, or (2) there is a diagonal relationship between the stego pixel pairs (P'_{1i}, P'_{1j}) and (P'_{2i}, P'_{2j}) of stego images *SI1* and *SI2*. These two relations will be used to check whether two stego images have been tampered with during the data transmission. Besides this diagonal relationship principle, two extra verification rules were designed in our proposed scheme. In general, our four integrity verification rules are listed below:

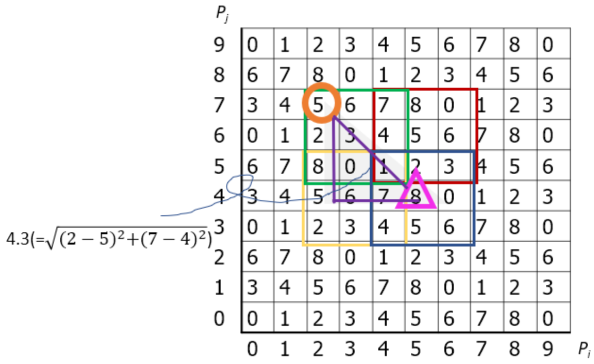
Rule 1: There is a diagonal relationship between the stego pixel pairs (P'_{1i}, P'_{1j}) and (P'_{2i}, P'_{2j}) of stego images *SI1* and *SI2* when these two stego pixel pairs map to matrix M and they are not mapped to the same coordinate.

Rule 2: The extracted one-bit authentication code ac' must be equal to the XOR operation result of the MSBs of P'_{1i} and P'_{1j}, $ac' = MSB\left(P'_{1i}\right)\ \oplus \acute{o}MSB\left(P'_{1i}\right)$, where $MSB()$ is the most significant bit (MSB) function.

Rule 3: The Euclidean distance between the stego pixel pairs (P'_{1i}, P'_{1j}) and (P'_{2i}, P'_{2j}) is always lower than or equal to 4.3.

Rule 4: For a given pixel, when its two neighboring pixels are identified as having been tampered with, the current pixel is determined as having been tampered with.

The reason that the Euclidean distance between the stego pixel pairs (P'_{1i}, P'_{1j}) and (P'_{2i}, P'_{2j}) is always lower than or equal to 4.3 is that the stego pixel pair (P'_{2i}, P'_{2j}) marked in a pink triangle shape is located at the center point of the opposite frame of which frame the stego pixel pair (P'_{1i}, P'_{1j}) marked in an orange circle is located at, as shown in Figure 4. Assume the stego pixel pair (P'_{1i}, P'_{1j}) of stego image *SI1* marked in an orange circle is located at (2, 7) in the Green frame and the stego pixel pair (P'_{2i}, P'_{2j}) marked in a pink tringle shape is located at (5, 4) in the Blue frame. Note that the center point of the Blue frame is fixed and its coordinate is (5, 4), and the coordinate that is located at the Green frame and maintains the farthest Euclidean distance from the center point of Blue frame is (2, 7). In this case, the Euclidean distance between (2, 7) and (5, 4) is $4.3(=\sqrt{(2-5)^2+(7-4)^2})$.



P_j										
9	0	1	2	3	4	5	6	7	8	0
8	6	7	8	0	1	2	3	4	5	6
7	3	4	5	6	7	8	0	1	2	3
6	0	1	2	3	4	5	6	7	8	0
5	6	7	8	0	1	2	3	4	5	6
4	3	4	5	6	7	8	0	1	2	3
3	0	1	2	3	4	5	6	7	8	0
2	6	7	8	0	1	2	3	4	5	6
1	3	4	5	6	7	8	0	1	2	3
0	0	1	2	3	4	5	6	7	8	0
	0	1	2	3	4	5	6	7	8	9 P_i

Figure 4. Example of the Euclidean distance between the stego pixel pairs (P'_{1i}, P'_{1j}) and (P'_{2i}, P'_{2j}). Four corresponding embedding frames are denoted as Red, Green, Yellow, and Blue. The red frame is the top-right frame, the green frame is the top-left frame, the yellow frame is the bottom-left frame, and the blue frame is the bottom-right frame.

When one of the four rules is not satisfied, the corresponding stego pixel pairs will be judged as having been tampered with during transmission, and it is marked in the integrity map. The same verification process is conducted until all stego pixel pairs are checked. Finally, with the marked integrity map, the tampered cover pixel pairs can be identified. To further enhance the verification of our scheme, we implemented a refinement mechanism similar to that proposed in [18], where a pixel is marked as having been tampered with if its two adjacent pixels have already been identified as having been tampered with.

3.5. Example of Our Proposed MRA-VSS Scheme

To provide a clear picture of our proposed construction of stego pixels, extraction, and recovery, an example that covers the above three operations is demonstrated in this subsection. Assume the cover pixel pairs are (4, 5) and the corresponding four secret bits are 0101. The MSBs of pixels 4 and 5 are 0 and 0, respectively; therefore, their authentication code is "0". Segment four secret bits "0101" and one-bit authentication code "0" into two units: $U1 = (01)_2$ and $U2 = (010)_2$. Their decimal values are $D_{U1} = 1$ and $D_{U2} = 2$, respectively. Because $D_{U1} = 1$ and $D_{U2} = 2$, the Green frame is chosen, according to Equation (4), and (P'_{1i}, P'_{1j}) of stego image *SI1* is set as (2, 6) due to $M_{ref}(P'_{1i} = 2, P'_{1j} = 6) = 2$. The opposite frame of the Green frame is the Blue frame and the central point of the Blue frame is (5, 4); therefore, the stego pixel pair (P'_{2i}, P'_{2j}) of stego image *SI2* is set as (5, 4).

Assuming two stego pixel pairs are delivered to two recipients safely, the recipients co-work with each other to extract the hidden secret bits and authentication code as follows: Because the received stego pixel pairs are (2, 6) and (5, 4), using (2, 6) and (5, 4), we can determine that the two pixel pairs are positioned in the Green and Blue frames, respectively. The cover pixel pair (4, 5) is obtained according to Equation (5). $D'_{U2} = 2$ is obtained after mapping (2, 6) to matrix M and its $M_{ref}(2, 6) = 2$ is found, and $D'_{U1} = 1$ because the corresponding frame is Green, according to Equation (6). Transform the derived $D'_{U1} = 1$ and $D'_{U2} = 2$ into binary representations, the hidden secret bits, and one-bit authentication $(01\ 010)_2$.

The pixel pairs of stego image *SI2* are always located at the central point of its corresponding frames. Therefore, with such property, a stego image belonging to *SI2* can be easily identified during the recovery of the cover image and secret data. To enhance the security of the hidden data, a secret key and a random number generator can be used to shuffle the order for pixel pairs of stego images *SI1* and *SI2*. In this case, an RDH scheme without requiring extra information can be adapted to hide the identity of the stego image for later usage. Certainly, the hidden secret data also can be encrypted with a symmetric cryptographic algorithm to enhance its confidentiality.

4. Experimental Results

To demonstrate the performance and the applicability of our proposed matrix-based crossover RDH scheme with dual meaningful image shadows, in this section, several experiments were conducted. The simulations were implemented into Java and Python on the platform of a personal computer with Windows 11 as the operating system. The hardware resources were i5-11400H CPU, RTX 3060 GPU, and 24 GB RAM. Eight standard grayscale images sized 512 × 512 served as the test cover image, as shown in Figure 5. As for the secret data, they were a bitstream randomly generated in advance.

4.1. Measurements

To evaluate the performance of our proposed dual image-based RDH scheme, two criteria were used: one was the visual quality of the stego image and the other was the hiding capacity. The peak-signal-to-noise ratio (PSNR) is defined as:

$$\mathrm{MSE} = \frac{1}{\mathrm{W} \times \mathrm{H}} \sum_{\mathrm{i}=1}^{\mathrm{W}} \sum_{\mathrm{j}=1}^{\mathrm{H}} \left(\mathrm{CI}_{\mathrm{i,j}} - \mathrm{SI}_{\mathrm{i,j}}\right)^2, \tag{7}$$

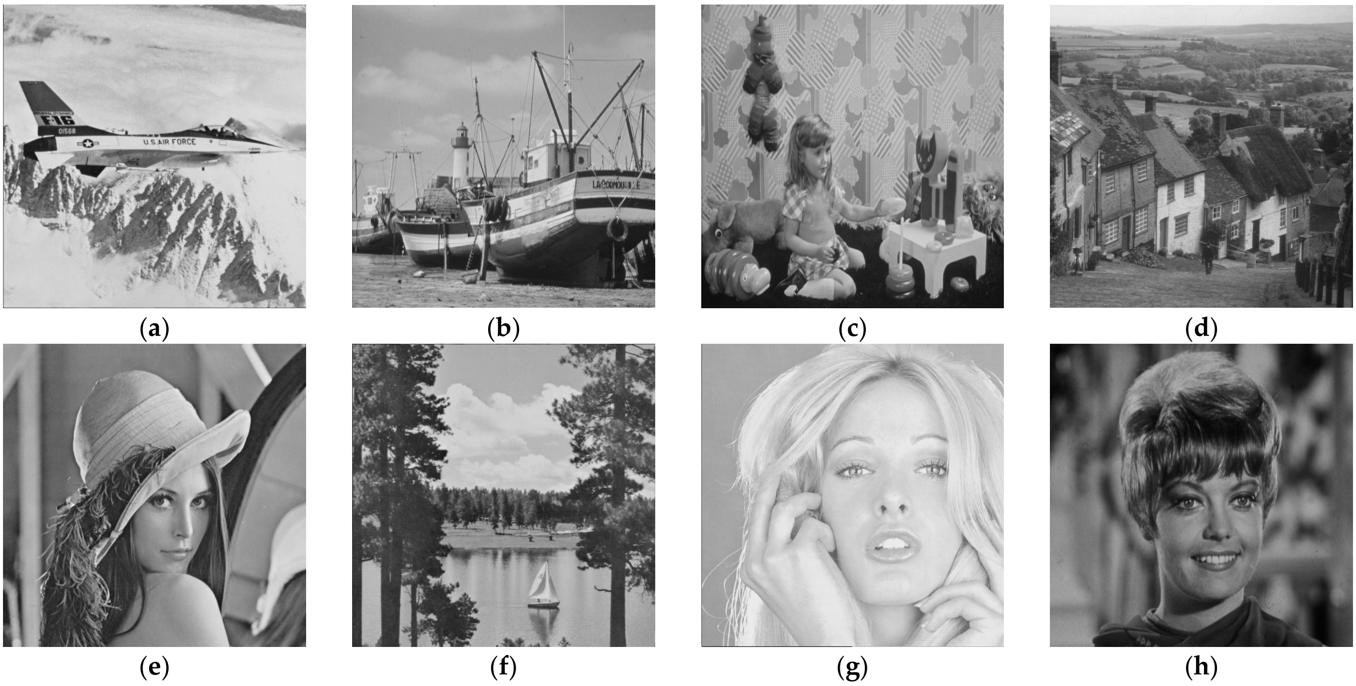
$$\mathrm{PSNR} = 10 \log_{10} \frac{(255)^2}{\mathrm{MSE}} \mathrm{dB} \tag{8}$$

where CI is the cover image, SI is the stego image, W is the width of the image, and H is the height of the image. The PSNR is a general criterion to evaluate the visual quality of the generated stego images. As long as the PNSR is above 30 dB, the human vision system cannot distinguish with ease the difference between the cover image and its stego image.

As for evaluating the hiding capacity, the embedding rate (ER) is the general criterion and is defined as:

$$\mathrm{ER} = \frac{\text{Size of secret data S}}{\mathrm{n} \times \mathrm{W} \times \mathrm{H}}, \tag{9}$$

where n is the number of stego images, and n is set as 2 to indicate it is a dual image-based RDH scheme. In addition, W is the width of the image and H is the height of the image. The less hidden secure data, the less distortion that is caused and the higher the PSNR value. The higher the PSNR value, the less likely it is to attract attackers' attention.


(**a**) (**b**) (**c**) (**d**)

(**e**) (**f**) (**g**) (**h**)

Figure 5. The eight test images with the size of 512 × 512 pixels. (**a**) Airplane. (**b**) Boat. (**c**) Girl. (**d**) Goldhill. (**e**) Lena. (**f**) Lake. (**g**) Tiffany. (**h**) Zelda.

4.2. Comparison with Related Schemes Regarding PSNRs and ERs

Table 2 shows the correlation between the PSNR performance of our proposed MRA-VSS and authentication code (*ac*), using eight general test images covering smooth, medium, and complex textures. In Table 2, we compare the PSNR performance of *SI1* and *SI2* with and without an embedded authentication code (*ac*), further verifying the impact of further authentication code embedding on the image quality.

Table 2. The impact of the authentication code (*ac*) on the image quality.

Images	**With *ac***		**Without *ac***	
	SI1	***SI2***	***SI1***	***SI2***
Airplane	45.91	48.13	45.90	48.13
Boat	45.87	48.13	45.90	48.13
Girl	45.90	48.13	45.90	48.13
Goldhill	45.91	48.13	45.92	48.13
Lena	45.89	48.13	45.90	48.13
Lake	45.89	48.13	45.89	48.13
Tiffany	45.89	48.13	45.90	48.13
Zelda	45.94	48.13	45.91	48.13
Average	45.90	48.13	45.90	48.13

As shown in Table 2, the average PSNRs with the authentication code are almost the same as those without the authentication code. This is because each pixel pair only carries a 1-bit authentication code without affecting the visual quality of the generated shares *SI1* and *SI2*. The PSNR performance is comparable to that of images without embedded authentication codes, while effectively enhancing the ability to detect attacks. To further demonstrate the embedding performance offered by our proposed MRA-VSS scheme, Table 3 shows the achievable maximum embedding capacity of seven representative schemes [6,8–11,13,15] and our scheme. From Table 3, we can see that Huynh et al.'s scheme [9] provides the highest ER at 1.99 bpp, the Lin et al.'s scheme [11] and our MRA-VSS scheme provide a relatively high ER of 1.25 bpp =(256 × 512 × 5)/(512 × 512 × 2) = 1.25 because there are five secret bits embedded into each pixel pair. Although the schemes in [9] achieve a higher embedding capacity compared to ours, they lack authentication capabilities. On the other hand, the schemes proposed by Liu et al. [8] and Lin et al. [10] provide authentication but have a maximum capacity of only 1 bpp, which is lower than the 1.25 bpp offered by our MRA-VSS. While the scheme in [13] excels in terms of PSNR and embedding rates (ERs), our MRA-VSS not only achieves an embedding rate of 1.25 bpp and an average PSNR of 47.02 dB, but also boasts a detection accuracy of 0.99%, surpassing the highest accuracy of 0.97% provided by [13]. This superior performance is largely due to the four verification rules outlined in Section 3.4, with the 1-bit accuracy being just one of these rules. Based on the comparisons in Table 3, we conclude that our MRA-VSS effectively embeds data while ensuring the quality and reliability of stego images, consistently maintaining a high detection accuracy under various conditions. This indicates that our MRA-VSS strikes a strong balance between data hiding and authentication, making it particularly well-suited for applications with high-security requirements.

Table 3. Comparison of the embedding capacity of our scheme with that of related schemes.

Images	**[6]**	**[8]**	**[9]**	**[10]**	**[11]**	**[13] (*r* = 3, 7)**	**[15]**	**Proposed**
Boat	1.07	1.00	1.99	1.00	1.25	[1.14, 1.82]	1.10	1.25
Goldhill	1.07	1.00	1.98	1.00	1.25	[1.14, 1.82]	1.10	1.25
Lena	1.07	0.99	1.99	1.00	1.25	[1.14, 1.82]	1.10	1.25
Tiffany	1.07	1.00	1.99	1.00	1.25	[1.14, 1.82]	1.10	1.25
Zelda	1.07	1.00	1.99	1.00	1.25	[1.14, 1.82]	1.10	1.25
Average	1.07	1.00	1.99	1.00	1.25	[1.14, 1.82]	1.10	1.25

To further illustrate the average image quality of two stego images generated by six representative schemes [6,8–11,13] alongside ours, Table 4 shows the average PSNR values for these schemes at fixed hiding capacities of 5000, 10,000, and 20,000 bits. Scheme [15] was excluded due to its lack of verifiability and the related discussion in their article. All schemes are classified into two categories: unverifiable and verifiable. The first three rows feature the unverifiable schemes [6,9,11], while the last four rows include the verifiable schemes [8,10,13] and our own. Notably, the PSNR values for stego images embedded with 20,000 bits from our scheme and those from [8,10,11,13] exceed 60 dB, indicating an excellent visual quality even with high-capacity embedding. Only the schemes in [8,10,13] and our scheme ensure both verifiability and integrity, allowing for the detection of any changes to the stego images. While the schemes in [8,10,13] achieve higher PSNR values, they exhibit a relatively lower detection ratio compared to ours. This suggests that our MRA-VSS may be particularly well-suited for applications in healthcare or military contexts, where data integrity and confidentiality are of utmost importance. The performance of the authentication capability of our MRA-VSS scheme will be discussed in detail in Section 4.3.

Table 4. Comparison of the PSNR values of our scheme with those of related schemes under different ERs.

Schemes	**5000 bits**			**10,000 bits**			**20,000 bits**		
	SI1	***SI2***	***Avg***	***SI1***	***SI2***	***Avg***	***SI1***	***SI2***	**Avg**
[6]	65.63	65.6	65.62	62.55	62.54	62.55	59.56	59.55	59.56
[9]	59.35	59.31	59.33	56.33	56.36	56.35	53.34	53.31	53.33
[11]	70.56	66.89	68.73	67.51	63.78	65.65	64.54	60.75	62.65
[8]	71.9	65.96	68.93	68.93	62.91	65.92	65.93	59.87	62.9
[10]	70.36	67.37	68.87	67.36	64.38	65.87	64.35	61.38	62.87
[13]	70.31	70.46	70.39	67.24	67.46	67.35	64.19	64.56	64.38
Proposed	67.06	69.3	68.18	64.05	66.29	65.17	61.04	63.28	62.16

4.3. Authentication and Security Analysis

Based on our hiding strategy, two adjacent pixels are formed as a pair to carry 5-bits secret data. To provide authentication capacity so that the recipient can authenticate the integrity of the received stego images, our proposed MRA-VSS scheme provides the option to conceal the authentication code into the last bit during the pixel pair's embedding. In our proposed scheme, the four rules for integrity verification were designed and are discussed in Section 3.4. If any rule is not satisfied, the corresponding stego pixel pair is determined as having been tampered with. Once all pixel pairs are examined, an integrity map is generated after the verification process. To evaluate the performance of our proposed scheme regarding verification, the detection ratio (DR) is defined as follows, and it is noted that the higher the DR, the better the detection performance.

$$\text{DR} = \frac{\text{number of detected tampered pixel} - \text{pairs}}{\text{the total number of the tampered pixel} - \text{pairs}} \tag{10}$$

The schemes presented in references [8,10,13] and our proposed scheme are capable of authenticating the integrity of the received stego images. To evaluate the tamper detection performance, we applied a collage attack, where the small image "Cameraman" was inserted into the shared image "Zelda", as illustrated in Figure 6b. Figure 6c displays the detection outcome, revealing that our scheme successfully differentiates malicious alterations and accurately localizes the modifications. The detection results are summarized in Table 5, showing that our MRA-VSS scheme outperforms the detection accuracy of the schemes in [8,10,13]. This improved performance stems from a unique feature of our scheme, where a diagonal relationship is always preserved between the stego pixel pairs (P'_{1i}, P'_{1j}) and (P'_{2i}, P'_{2j}) in the untampered stego images *SI1* and *SI2*, provided that these pixel pairs map to matrix M without overlapping coordinates. This feature enhances the detection rates (DRs) in our MRA-VSS scheme, even though only a 1-bit authentication code is embedded within the pixel pairs across two shares. Therefore, the evaluation results demonstrate that the MRA-VSS scheme effectively identifies the tampering introduced by the collage attack on the stego images.

Table 5. The detection performance for different test images.

Images	**Proposed**	**[8]**	**[10]**	**[13] (r = 3, 7)**
Boat	0.99	0.95	0.94	[0.95, 0.87]
Goldhill	0.99	0.98	0.97	[0.97, 0.94]
Lena	0.99	0.97	0.98	[0.97, 0.93]
Zelda	0.99	0.97	0.97	[0.97, 0.92]
Average	0.99	0.97	0.97	[0.97, 0.92]

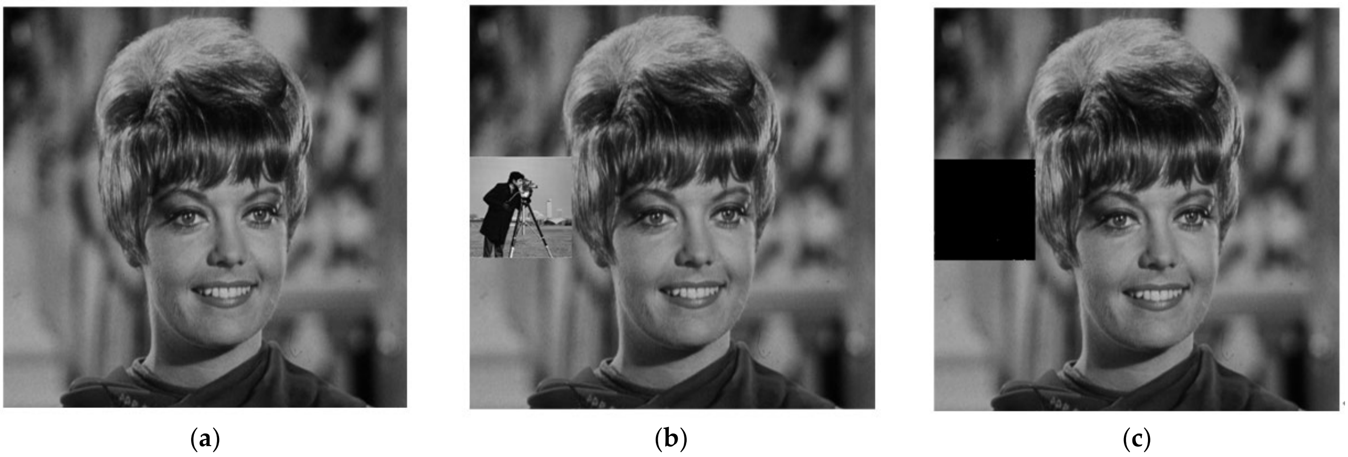
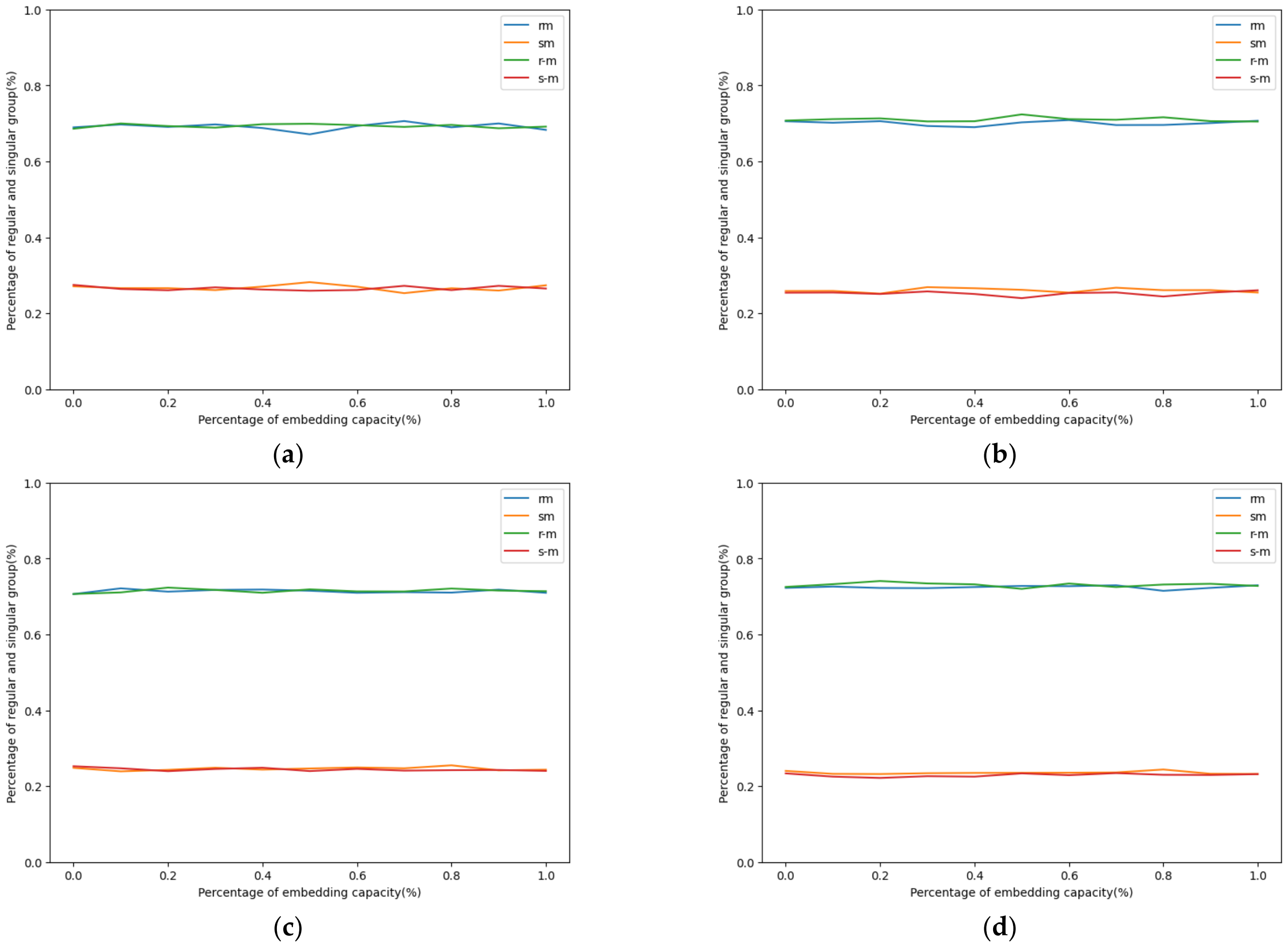


Figure 6. Detection results of the collage attack with the share "Zelda": (**a**) Original share "Zelda"; (**b**) tampered "Zelda"; and (**c**) identified tampered region.

To prove both the hidden secret bits and the concealed 1-bit authentication code do not leak any information to the malicious attackers, RS analysis [18], which is a powerful tool used to judge whether the stego image withstands the LSB-steganalysis attack, was used to analyze the shares generated by our proposed MRA-VSS scheme. In general, the RS analysis first groups four continuous pixels in an image as a unit and assesses them at the same time. Then, the RS analysis classifies the pixel units of an image into three types: regular, singular, and unchanged ones. To evaluate if certain patterns remain and leak extra information to malicious attackers, A flipping operation was conducted on the pixels belonging to the same unit according to the mask M (or $-M$). After the flipping operation, the properties of the pixels in the unit may be changed to regular or singular. R_M and S_M (or R_{-M} and S_{-M}) indicate the percentages of regular and singular units with the mask M (or $-M$), respectively. Based on the characteristics of RS analysis, $R_M \cong R_{-M}$ and $S \cong S_{-M}$ remain when the stego images do not carry any secret. Note that the difference between R_{-M} and S-$_M$ may increase if the stego images carry secrets. In other words, malicious attackers can use the results from the RS analysis to determine whether any secrets are hidden in the LSB portions of the generated stego images. In our RS analysis, we used two different masks, [1, 0, 0, 1] and [0, 1, 1, 0], to conduct the RS analysis. The results are similar; therefore, the related RS analysis with [1, 0, 0, 1] for the stego images of "Boat" and "Lena" by using our proposed MRA-VSS scheme was selected and is demonstrated in Figure 7.

Figure 7 presents the RS analysis results of our proposed MRA-VSS scheme. Figure 7a,b show the detection results for "Boat", while Figure 7c,d correspond to the test image "Lena". As the embedding rate varies, the R_M and R-$_M$ curves remain highly similar, and the S_M and S_{-M} curves also display a consistent similarity, indicating a minimal impact on the "regular" and "singular" ratios during the embedding process for both the "Boat" and "Lena" images. This consistency reduces the noticeable differences between the stego and cover images, achieving the intended concealment effect. This result arises because the test images "Boat" and "Lena" share similar statistical properties, such as grayscale distribution, edge structure, and detail variation. These similarities naturally lead to analogous "regular" and "singular" group distributions in the RS analysis, despite content differences. Such statistical consistency highlights the MRA-VSS scheme's robustness across diverse images, a critical factor in data hiding. In network transmission, this stability reduces anomaly detection risks, making it difficult for attackers to identify hidden information based solely on pixel variations, thereby enhancing the security and undetectability of the embedded data.



(**a**) (**b**) (**c**) (**d**)

Figure 7. RS analysis for the dual stego images of "Boat" and "Lena". (**a**) The stego image *SI1* of "Boat". (**b**) The stego image *SI2* of "Boat". (**c**) The stego image *SI1* of "Lena". (**d**) The stego image *SI2* of "Lena".

With the RS analysis [19], we can see that our proposed MRA-VSS scheme preserves the natural cover images' features. Additionally, a pixel-value differencing histogram (PDH) analysis [20] was also conducted to compute the difference value of successive pixels within an image and then analyze the frequencies of the pixels' difference values. It is noted that the basic assumption of PDH is that a given natural image usually has a high peak near the pixel values of "0", "1", or "−1"; this is because the neighboring pixels always share a high correlation, as shown in Figure 8. The frequency distributions of the stego images from the PDH analysis indicate whether they carry secret data. The more similar the frequency distributions of the stego images to that of the cover image, the less attention that draws the malicious attackers. The results of the two stego images and their corresponding cover image with the four test images, Boat, Goldhill, Lena, and Zelda, from the PDH analysis are depicted in Figure 8. In Figure 8, we can see the distributions of the two stego images are almost overlapped with that of the cover image in most cases and remain the peak features at the pixel differences around "0", "−1", or "1". Such phenomena confirm that the pixels' modifications with our matrix-based data hiding strategy retain the neighboring relationship between two successive pixels and without modifying the cover pixel pairs too much.

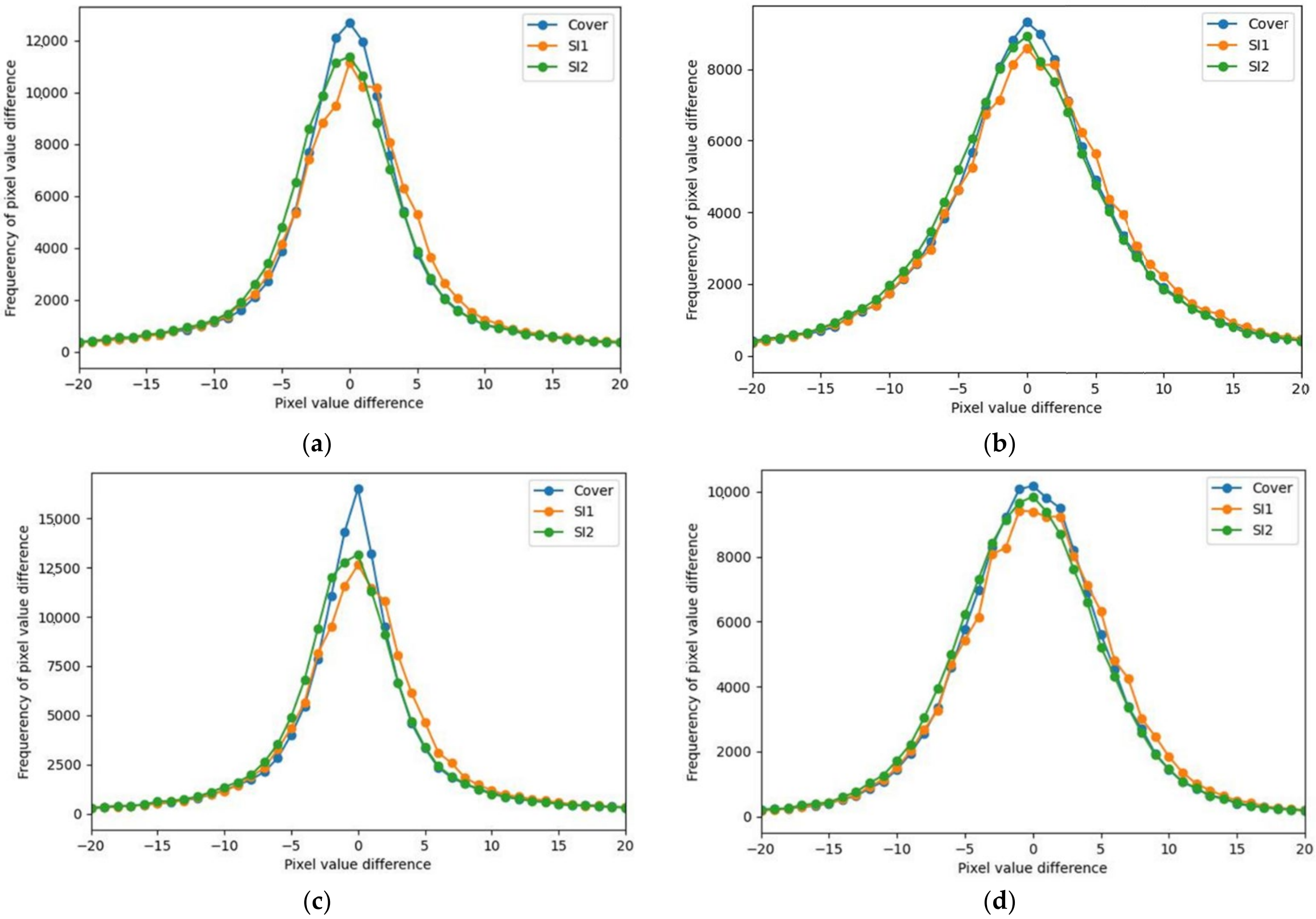


Figure 8. PDH analysis results of four cover images and their stego images. (**a**) Boat. (**b**) Goldhill. (**c**) Lena. (**d**) Zelda.

5. Conclusions

In this paper, we propose a matrix-based reversible and authenticable visual secret-sharing scheme using dual meaningful images. After the construction of two stego images, not only are two stego pixel pairs derived from the corresponding cover pixel pair, besides the one-bit authentication code (*ac*); but also there are two unique features that can be found if two stego pixel pairs are mapped to the matrix M_{ref}: (a) If two pixel pairs are not located at the same coordinate in the matrix M_{ref}, then, there is always a straight line that can pass through these two-pixel coordinates, and the straight line maintains an included angle lower than 90 degrees and greater than 0 degrees with the horizontal line. (b) The Euclidean distance between the two-pixel coordinates is never longer than 4.3. With the exception of the above two features, a refinement mechanism is also designed to determine a pixel as having been tampered with as long as its adjacent pixels have been judged as having been tampered with.

With these unique features and the refinement mechanism, the experiments confirmed that the detection performance of our dual image matrix-based data hiding strategy successfully provides the competitive results compared to the schemes in [8,10,13]. They also indicated that each pixel pairs of stego images can fully support the carrying of confidential data, increasing the hiding capacity of our scheme up to 1.25 bpp. The original cover image is completely restored with our dual image matrix-based RDH scheme, and the integrity of the reconstructed cover image can be verified with our detection rules and refinement mechanism with a simple check of the Euclidean distance and relative position between two stego pixel pairs. Moreover, the reversibility and low complexity of the recovery and verification procedures make our MRA-VSS scheme ideal for high-confidentiality and real-time applications. This is especially valuable in network transmission scenarios, where the receiver must verify the image's authenticity and integrity using the verification code after transmission—a feature rarely available in other methods.

Author Contributions: Conceptualization, C.-C.L. and E.E.; Methodology, C.-C.L.; Validation, C.-C.L. and Y.-F.C.; Formal analysis, C.-C.L. and E.-T.C.; Writing—original draft, E.-T.C.; Writing—review and editing, C.-C.L. and Y.-F.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Science and Technology Council, under the grant NSTC 113-2410-H-167-012-MY3.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

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

References

1. Rivest, R.; Shamir, A.; Adleman, L.M. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
2. Tian, J. Reversible data embedding using a difference expansion. *IEEE Trans. Circuits Syst. Video Technol.* **2003**, *13*, 890–896. [CrossRef]
3. Ni, Z.; Shi, Y.Q.; Ansari, N.; Su, W. Reversible data hiding. *IEEE Trans. Circuits Syst. Video Technol.* **2006**, *16*, 354–362.
4. Chang, C.C.; Kieu, T.D.; Chou, Y.C. Reversible data hiding scheme using two steganographic images. In Proceedings of the IEEE Region 10 International Conference (TENCON 2007), Taipei, Taiwan, 30 October–2 November 2007.
5. Zhang, X.; Wang, S. Efficient steganographic embedding by exploiting modification direction. *IEEE Commun. Lett.* **2006**, *10*, 781–783. [CrossRef]
6. Lee, C.F.; Huang, Y.L. Reversible data hiding scheme based on dual stegano-images using orientation combinations. *Telecommun. Syst.* **2013**, *52*, 2237–2247. [CrossRef]
7. Chang, C.C.; Chou, Y.C.; Kieu, T.D. An information hiding scheme using Sudoku. In Proceedings of the 2008 3rd International Conference on Innovative Computing Information and Control, Dalian, China, 18–20 June 2008.
8. Liu, Y.; Chang, C.C. A turtle shell-based visual secret sharing scheme with reversibility and authentication. *Multimed. Tools Appl.* **2018**, *77*, 25295–25310. [CrossRef]
9. Huynh, N.T.; Bharanitharan, K.; Chang, C.C. Quadri-directional searching algorithm for secret image sharing using meaningful shadows. *J. Vis. Commun. Image Represent.* **2015**, *28*, 105–112. [CrossRef]
10. Lin, J.Y.; Horng, J.H.; Chang, C.C. A reversible and authenticable secret sharing scheme using dual images. *Multimed. Tools Appl.* **2022**, *81*, 17527–17545. [CrossRef]
11. Lin, J.Y.; Liu, Y.; Chang, C.C. A real-time dual-image-based reversible data hiding scheme using turtle shells. *J. Real-Time Image Proc.* **2019**, *16*, 673–684. [CrossRef]
12. Chang, C.C.; Su, G.D.; Lin, C.C.; Li, Y.H. Position-aware guided hiding data scheme with reversibility and adaptivity for dual images. *Symmetry* **2022**, *14*, 509. [CrossRef]
13. Lin, J.Y.; Horng, J.H.; Chang, C.C.; Li, Y.H. Asymmetric orientation combination for reversible and authenticable data hiding of dual stego-images. *Symmetry* **2022**, *14*, 819. [CrossRef]
14. Solak, S.; Tezcan, G. A new dual image based reversible data hiding method using most significant bits and center shifting technique. *Appl. Sci.* **2022**, *12*, 10933. [CrossRef]
15. Kim, C.; Cavazos-Quero, L.; Jung, K.H.; Leng, L. Advanced dual reversible data hiding: A focus on modification direction and enhanced least significant bit (LSB) Approaches. *Appl. Sci.* **2024**, *14*, 2437. [CrossRef]
16. Lee, C.F.; Chan, K.C. A novel dual image reversible data hiding scheme based on vector coordinate with triangular order coding. *IEEE Access* **2024**, *12*, 90794–90814. [CrossRef]
17. 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. [CrossRef]
18. Chen, C.C.; Chang, C.C.; Lin, C.C.; Su, G.D. TSIA: A novel image authentication scheme for AMBTC-based compressed images using turtle shell based reference matrix. *IEEE Access* **2019**, *7*, 149515–149526. [CrossRef]

19. Fridrich, J.; Goljan, M. Practical steganalysis of digital images: State of the art. In Proceedings of the SPIE 4675, Security and Watermarking of Multimedia Contents IV, San Jose, CA, USA, 29 April 2002.
20. Zhang, X.; Wang, S. Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. *Pattern Recognit. Lett.* **2004**, *3*, 331–339. [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.