symmetry

MDPI

Article

On the Design of Multi-Party Reversible Data Hiding over Ciphered Overexposed Images

Bing Chen, Ranran Yang, Wanhan Fang, Xiuye Zhan and Jun Cai *

School of Cyber Security, Guangdong Polytechnic Normal University, Guangzhou 510665, China; chenbing@gpnu.edu.cn (B.C.); yangranran@gpnu.edu.cn (R.Y.); whfang@gpnu.edu.cn (W.F.); xyzhan@gpnu.edu.cn (X.Z.)
* Correspondence: caijun@gpnu.edu.cn

Abstract: Multi-party reversible data hiding over ciphered images (MRDH-CI) has high restorability since the image is split into multiple ciphered images by secret sharing. However, the MRDH-CI methods either fail to produce satisfied results, or only work well for conventional images. This paper introduces a multi-party reversible data-hiding approach over ciphered overexposed images. First, the pixels of the overexposed images are decomposed into two parts, each of which can be used for secret sharing. Then, the decomposed overexposed images are converted into multiple ciphered overexposed images by using a modified secret sharing method, in which the differences of the ciphered overexposed images are retained. The symmetry of the difference retaining makes the secret data conceal within the ciphered overexposed images such that the marked ciphered overexposed images can be created. Finally, by collecting sufficient marked ciphered overexposed images, it is possible to symmetrically reconstruct the concealed data and primitive overexposed image. Experimental results illustrate that the presented method can efficiently deal with overexposed images while maintaining a low computational overhead.

Keywords: reversible data hiding; multi-party data hiding; ciphered domain; overexposed images

check for updates

Citation: Chen, B.; Yang, R.; Fang, W.; Zhan, X.; Cai, J. On the Design of Multi-Party Reversible Data Hiding over Ciphered Overexposed Images. *Symmetry* **2024**, *16*, 45. https://doi.org/10.3390/sym16010045

Academic Editor: Bingwen Feng

Received: 22 November 2023
Revised: 17 December 2023
Accepted: 26 December 2023
Published: 29 December 2023

1. Introduction

In the era of digital information transmission, privacy and security issues are becoming increasingly prominent in the fields of information processing and transmission [1,2]. Confronted with the challenge of how to effectively hide sensitive information, reversible data hiding (RDH) has garnered significant interest. The feature of this technique is that the secret data are concealed in a cover, and the cover can be recovered nondestructively after the secret data are extracted. RDH has shown broad application prospects in many fields, including but not limited to medical image transmission [3], legal evidence [4], and military communication [5]. Existing RDH schemes are classified as difference expansion [6–8], histogram shifting [9,10], pixel value ordering [11,12], prediction error expansion [13–15], etc. However, traditional RDH schemes tend to embed data in plaintext images, which can be easily detected by unauthorized users, thus reducing covertness and security. To overcome these limitations, reversible data hiding over ciphered images (RDH-CI) has gained prominence during the last few yeas.

RDH-CI enhances the security of secret data by employing encryption algorithms [16], enabling more effective protection of privacy content during the transmission of sensitive data. In [17], Wang et al. introduced an adaptive most significant bit (MSB) prediction-based method for RDH-CI, in which the pixel correlation is remained by block permutation encryption. With the help of the symmetry of the block permutation, the embedding room can be created by MSB prediction. In the method of Gao [18], the cover image underwent encryption by block substitution and bitstream cipher. The ciphered image is then compressed on the basis of adaptive block coding; therefore, the room used for embedding data is vacated. In [19], Sui et al. used a pseudo-random matrix-based symmetric encryption to encrypt a primitive image. The receiver uses the same key matrix to restore the primitive image due to the symmetry of the encryption algorithm. In addition, MSB and the remaining bits of the primitive image are combined to generate hiding room by employing the property of image redundancy. In [20], bitstreams are initially encrypted using the JPEG encryption algorithm. Subsequently, a combination of Huffman code mapping and histogram shifting is employed to conceal secret data. Finally, the receiver extracts the concealed secret data from marked JPEG bitstreams, achieving perfect reconstruction of the primitive bitstreams. In Ge's approach [21], chaotic sequences are generated using chaotic mapping, which are utilized to perform inter-block scrambled operations, and finally secondary encryption is performed by stream cipher to improve security. In the data embedding stage, the detection of all bit planes is achieved by recording smooth and rough bit planes, which yields a high embedding capability.

The homomorphism-based RDH-CI is also presented, which is particularly prominent in scenarios where computations need to be conducted while maintaining data encryption. In Wu's scheme [22], the Pallier algorithm is used to encrypt the preprocessed images, which can realize the extraction of data in both plaintext and ciphertext domains due to the homomorphism of the Paillier algorithm. In addition, Zheng et al. [23] proposed a method to generate a ciphered cover using homomorphic encryption, which enables the data hider to conceal secret data within a ciphered cover by establishing a secret bit mapping and lossless modification. The receiver can successfully retrieve the hidden data from the ciphered domain. Ke et al. [24] proposed a fully homomorphic cryptographic encapsulation differential extension scheme to achieve ciphertext control for homomorphic encryption. By introducing a key-switching technique, the data extraction process can be efficiently achieved by directly retrieving data from the ciphered domain. However, an obvious disadvantage of homomorphic encryption is its high computational overhead, which may lead to performance decline during large-scale data processing.

The mentioned RDH-CI methods are built on a data hider, and when the data hider is compromised, the recovery of the primitive image cannot be realized. To improve the restorability, there has been a rise in the introduction of multi-party reversible data hiding over ciphered images (MRDH-CI) [25,26]. Chen et al. [25] proposed a MRDH-CI method derived from secret sharing, in which multiple ciphered images are generated and assigned to multiple data hiders. Every data hider conceals the secret data into a designated area of the ciphered image through the substitution of the least significant bits. In [26], Hua et al. firstly proposed a cryptographic feedback secret sharing (CFSS) to generate multiple ciphered images. Then, a multi-MSB prediction method is employed to reserve embedding room for data hiding. MRDH-CI methods ensure the lossless restoration of the primitive image through gathering some marked ciphered images from intact data hides.

However, the MRDH-CI methods cannot efficiently deal with overexposed images since there are many pixels that are not directly encrypted into multiple ciphered pixels (called overflow pixels). They either fail to produce satisfactory results, or only work well for conventional images. To address this issue, multi-party reversible data hiding over ciphered overexposed images (MRDH-COI) is proposed, in which the overflow pixels are efficiently processed for data hiding. In the following, the contributions of this paper are encapsulated:

- By decomposing the pixel of the overexposed image into two parts, each of which is suitable for secret sharing, it is thus efficient to handle overflow pixels.
- An encryption algorithm combining group scrambling and modified secret sharing is given for the overexposed image, by which the differences of the groups of ciphered overexposed images are retained. It means that the ciphered overexposed images can be facilely used for data hiding.
- According to the given overexposed image encryption, the overflow pixels can be encrypted without labeling, so the executing time of the overexposed image encryption is reduced.

The subsequent sections of this paper are organized below. A brief analysis of related MRDH-CI works is given in Section 2. Section 3 provides the presented MRDH-COI approach. The experiment and its analysis are demonstrated in Section 4. At last, Section 5 draws our conclusion.

2. Related Works

The existing MRDH-CI methods are designed for conventional images. In [25], a MRDH-CI method is given, in which the traditional secret sharing strategy is employed to encrypt the primitive image into multiple ciphered images, and the ciphered images are distributed to multiple data hiders so that they can be used to embed data independently. In the case of a damaged hider, by collecting marked ciphered images from other undamaged hiders, the receiver is able to restore the primitive image in a lossless manner, which significantly improves the security of the image. In [26], a CFSS-based MRDH-CI method is proposed, in which the embedding room is reserved by the content owner. First, the median edge detector is used to predict the image to produce predictable pixels, and the MSB planes are determined based on the proportion of predictable pixels. Then, the predictor error is obtained by predicting the MSB planes, and the embedding room is reserved by encoding the predictor error with Huffman coding. This method provides a feasible and secure encryption protection mechanism for multiple data hiders.

The MRDH-CI methods proposed in [25,26] are constructed over finite field F_p by Shamir secret sharing [27], where p is a prime. For grayscale images with 8 bits, the pixels exceeding 250 are not suitable for secret sharing since p is set to 251. Therefore, the pixels exceeding 250 need to be processed so that they can be used for secret sharing. In [25], a location map (LM) is used to label the pixels exceeding 250 and concealed within the primitive image in a reversible manner. In [26], to label the pixels exceeding 250, the difference between $p-1$ and the pixel value is encoded by introducing reference information. The reference information is embedded into the multiple MSBs of the pixel vacated via prediction error expansion.

However, the methods mentioned above have deficiencies in dealing with overexposed images. Four overexposed images selected from the standard dataset [28] are used for the demonstration as shown in Figure 1. We found that the percentages of pixels exceeding 250 are 51.7%, 61.7%, 59.8%, and 62.4%, respectively. In other words, there are plenty of overflow pixels that are not directly encrypted into multiple ciphered pixels. To deal with these overflow pixels, a lot of auxiliary information is required. For the method in [25], the primitive image may not have enough room to accommodate this auxiliary information. In [26], a lot of auxiliary information will increase the computational overhead since it is implemented by the reserving embedding room technique.

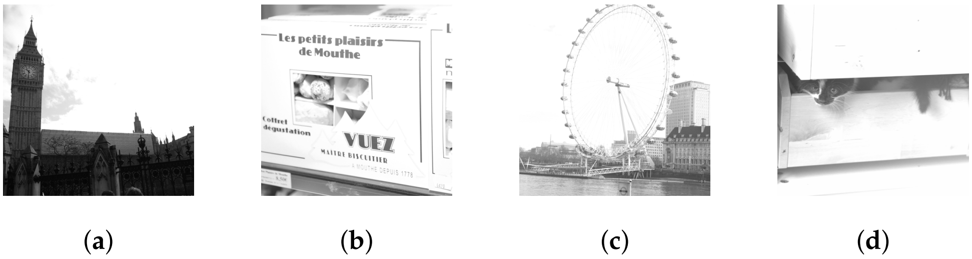


Figure 1. Four overexposed images used for the experiment. (**a**) 1851.pgm, (**b**) 1933.pgm, (**c**) 2025.pgm, and (**d**) 7343.pgm.

Faced with these challenges, we propose a novel MRDH-CI method that focuses on solving the problem of overflow pixels in overexposed images. The challenge posed by overflow pixels is effectively overcome by splitting the pixel of the image into two parts. In addition, by combining group scrambling and modified secret sharing techniques, the grouping differences of overexposed images can be preserved during encryption, thus making the ciphered overexposed images suitable for data hiding. The key to the proposed scheme is the successful fusion of overexposed image processing and encryption algorithms, which achieves the efficient encryption of overflow pixels without labeling. The proposed scheme simplifies the process of overexposed image encryption, thereby significantly reducing the time cost of processing overflow pixels.

3. Presented Approach

Figure 2 shows the given MRDH-COI approach, which involves encrypting the overexposed image, hiding data into ciphered overexposed images, and extracting hidden data and restoring overexposed images. For encrypting the overexposed image, the owner first scrambles an overexposed image to obtain a scrambled overexposed image. Then, the scrambled overexposed image is split into multiple ciphered overexposed images by secret sharing, and the ciphered overexposed images are sent to the associated data hiders, respectively. After that, every data hider conceals the secret data within a ciphered overexposed image, resulting in the creation of a marked ciphered overexposed image. In the step of extracting hidden data and restoring the overexposed image, once a sufficient number of marked ciphered overexposed images are obtained, the receiver first performs data extraction to obtain the embedded secret data. Subsequently, the receiver proceeds with the overexposed image restoration to obtain the primitive overexposed image.

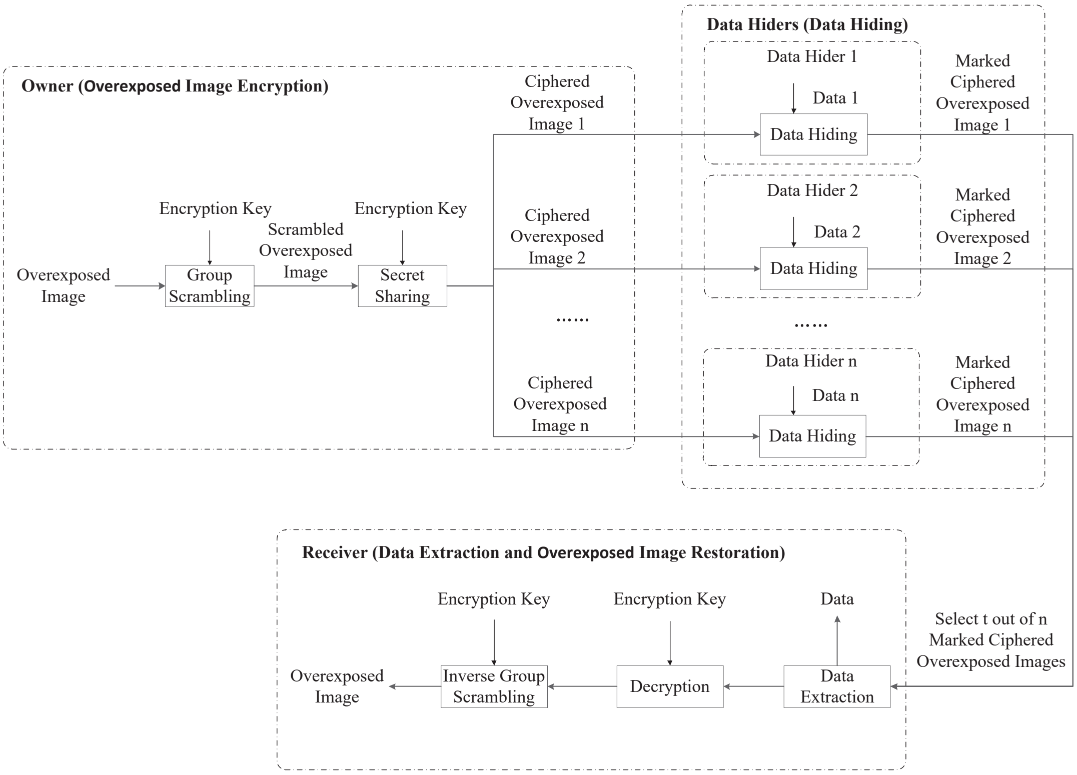

Data Hiders (Data Hiding)
Data Hider 1
Data 1
Data Hiding
Marked Ciphered Overexposed Image 1
Owner (Overexposed Image Encryption)
Ciphered Overexposed Image 1
Data Hider 2
Data 2
Data Hiding
Marked Ciphered Overexposed Image 2
Encryption Key
Scrambled Overexposed Image
Encryption Key
Ciphered Overexposed Image 2
Overexposed Image
Group Scrambling
Secret Sharing
......
......
Data Hider n
Data n
Data Hiding
Marked Ciphered Overexposed Image n
Ciphered Overexposed Image n
Receiver (Data Extraction and Overexposed Image Restoration)
Encryption Key
Encryption Key
Data
Select t out of n Marked Ciphered Overexposed Images
Overexposed Image
Inverse Group Scrambling
Decryption
Data Extraction

Figure 2. The framework of the presented approach, in which there are three parties actively involved.

3.1. Overexposed Image Encryption

Suppose the overexposed image O is an eight-bit grayscale image sized by $P \times Q$, and $O_{\alpha,\beta}$ is the pixel at location (α, β), where $O_{\alpha,\beta} \in [0, 255]$, $1 \leq \alpha \leq P$, $1 \leq \beta \leq Q$. For simplicity, P and Q are considered even. The overexposed image encryption is comprised of two parts: group scrambling and secret sharing. First, the owner divides the overexposed image into groups with size 1×2. It is easily obtained that there are $PQ/2$ groups. All groups of the overexposed image are scrambled by using an encryption key, then a scrambled overexposed image O' is obtained. It is worth mentioning that by using a pseudorandom number generator with a seed, the encryption key can be created. The key generation process is shown in Figure 3. First of all, the content owner chooses a seed at random and assigns the seed to the state. Secondly, with the state, an encryption key is generated by adopting a 256-bit secure hash algorithm (SHA-256). At the same time, the state is modified to the sum of the encryption key and step m, where m is an integer. Finally, the second step is repeated to generate multiple encryption keys as needed. In general, the encryption key is shared over a covert channel or a public channel with the assistance of a key exchange protocol, such as the Diffie–Hellman key negotiation algorithm.

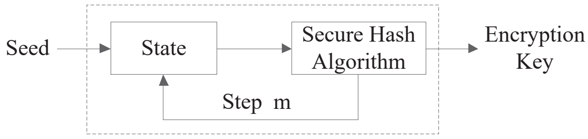


Figure 3. Sketch of the key generation process, where the security level of the secure hash algorithm is 256 bits.

After group scrambling, secret sharing is performed on the scrambled overexposed image O'. Herein, a modified secret sharing method inherited from Shamir secret sharing is used to convert the scrambled overexposed image into multiple ciphered overexposed images. For grayscale images with eight bits, pixels exceeding 250 do not lend themselves to secret sharing. To address this issue, we decompose the pixels of the overexposed image and make a simple modification to (t, n) threshold secret sharing [27], where $2 \leq t \leq n$. Let a group of the scrambled overexposed image be $(O'_{i,j}, O'_{i,j+1})$, where $1 \leq i \leq P$, $j = 1, 3, \ldots, Q-1$. To obtain multiple ciphered overexposed images, a identifier is chosen for each ciphered overexposed image, denoted as x_r, $1 \leq r \leq n$, each of which is distinct from one another. Usually, x_r is determined by the encryption key. When $O'_{i,j} \in [d, 255]$ or $O'_{i,j+1} \in [d, 255]$, a polynomial $f(x)$ with a degree of $t-1$ is formulated via

$$f(x) = \left(a_0 + dx + \sum_{q=2}^{t-1} a_q x^q\right) \bmod p, \tag{1}$$

where $a_0 = O'_{i,j} - d$ or $a_0 = O'_{i,j+1} - d$, $d \geq 5$ is a integer, and $a_2, \ldots, a_{t-1} \in F_p$ are chosen at random. For each specified x_r, a corresponding $f(x_r)$ can be calculated by Equation (1), and $f(x_r)$ is set as the pixel of the ciphered overexposed image. When $O'_{i,j} \in [0, d-1]$ or $O'_{i,j+1} \in [0, d-1]$, another polynomial $f(x)$ with a degree of $t-1$ is formulated via

$$f(x) = \left(a_0 + 0x + \sum_{q=2}^{t-1} a_q x^q\right) \bmod p, \tag{2}$$

where $a_0 = O'_{i,j}$ or $a_0 = O'_{i,j+1}$. Similarly, for each specified x_r, another corresponding $f(x_r)$ can be calculated by Equation (2), and the corresponding $f(x_r)$ is set as the pixel of the ciphered overexposed image. In this way, n ciphered overexposed images are created, and the created ciphered overexposed images are shared among n data hiders for data hiding. Algorithm 1 shows the procedure of the overexposed image encryption.

Next, we will demonstrate that the obtained ciphered overexposed images are suitable for data hiding. An example is given in Figure 4, where $(3, 3)$ modified secret sharing is adopted. Assume that a group of the scrambled overexposed image is $(252, 254)$. With the encryption key, three identifiers 2, 3, and 5 are generated. According to Equation (1), two 2-degree polynomials with $d = 5$ and random integer $a_2 = 10$ are constructed by

$$f(x) = 247 + 5x + 10x^2 \bmod 251, \tag{3}$$

and

$$f(x) = 249 + 5x + 10x^2 \bmod 251, \tag{4}$$

respectively. Three identifiers 2, 3, and 5 are substituted into Equations (3) and (4), and three corresponding groups of ciphered overexposed images $(46, 48)$, $(101, 103)$, and $(20, 22)$, are generated, respectively. As can be seen, the differences of the generated three groups are retained, which means that the ciphered overexposed images can be used for data hiding.

Algorithm 1 Overexposed image encryption.

```
Input: Overexposed Image $O$, Encryption Key.
Output: Ciphered Overexposed Image $CO^r$.
  Divide $O$ into groups with size $1 \times 2$;
  Obtain scrambled overexposed image $O'$ by scrambling the groups;
  for $r \leftarrow 1 : n$ do
    Generate $x_r$ with the encryption key;
    for $i \leftarrow 1 : P$ do
      for $j \leftarrow 1 : Q$ do
        if $O'_{i,j} \geq d$ && $O'_{i,j} \leq 255$ then
          $a_0 \leftarrow O'_{i,j} - d$;
          Construct polynomial $f(x)$ by Equation (1) with $a_0$, $d$ and random integer $a_q$;
        else
          $a_0 \leftarrow O'_{i,j}$;
          Construct polynomial $f(x)$ by Equation (2) with $a_0$ and random integer $a_q$;
        end if
        $CO^r_{i,j} \leftarrow$ Calculate $f(x)$ with $x_r$;
      end for
    end for
  end for
```

For the group belonging to $[0, d-1]$, the difference retaining verification is similar to the group belonging to $[d, 255]$, and thus no description is provided here.

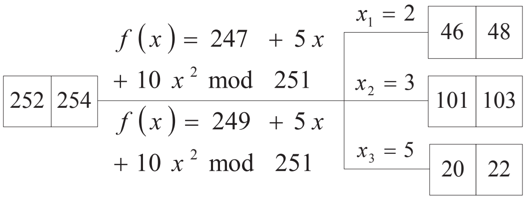

252
254
$f(x) = 247 + 5x + 10x^2 \bmod 251$
$f(x) = 249 + 5x + 10x^2 \bmod 251$
$x_1 = 2$
46
48
$x_2 = 3$
101
103
$x_3 = 5$
20
22

Figure 4. An example of the difference retaining in a group.

3.2. Data Hiding

To manage the obtained ciphered overexposed images, data hiders conceal secret data into them to create marked ciphered overexposed images without accessing the primitive overexposed image. Based on the analysis in Section 3.1, the differences of the groups of ciphered overexposed images are retained, so data hiding can be achieved using the classic difference expansion algorithm, such as the method in [7]. Let the ciphered overexposed image be CO^r,$1 \leq r \leq n$. The group of the ciphered overexposed image is represented by $(CO^r_{i,j}, CO^r_{i,j+1})$, $1 \leq i \leq P$, $j = 1, 3, \ldots, Q-1$. Specifically, comprehensive description of the data hiding algorithm is provided below.

1. Compute the integer mean and difference of the groups of ciphered overexposed images. For each $(CO^r_{i,j}, CO^r_{i,j+1})$, the integer mean and difference are computed by $l = \left\lfloor \frac{CO^r_{i,j}+CO^r_{i,j+1}}{2} \right\rfloor$ and $h = CO^r_{i,j} - CO^r_{i,j+1}$, respectively, where $\lfloor\cdot\rfloor$ is a floor function.
2. Determine the expandable and non-expandable groups. A group is expandable if its integer mean l and difference h satisfy $\left|2 \times \lfloor \frac{h}{2} \rfloor + b\right| \leq \min(2(255-l), 2l+1)$, where

b is the bit of the secret data; otherwise, it is considered non-expandable. In addition, an LM is created to label expandable and non-expandable groups, and their associated bits are set to 0 and 1, respectively.

3. Embed secret data into the expandable groups. First, for each expandable group, a new difference is generated with the difference h by

$$h' = 2 \times h + b, \tag{5}$$

where $b \in \{0, 1\}$ is the bit of the secret data that is concealed within the ciphered overexposed images. Then, with the new difference h', the pixels of the marked ciphered overexposed image are computed by

$$\begin{cases} COD^r_{i,j} = l + \lfloor \frac{h'+1}{2} \rfloor, \\ COD^r_{i,j+1} = l - \lfloor \frac{h'}{2} \rfloor, \end{cases} \tag{6}$$

where $COD^r_{i,j}$ (resp. $COD^r_{i,j+1}$) is the pixel of the rth marked ciphered overexposed image at location (i, j) (resp. $(i, j+1)$).

By these means, the ciphered overexposed images can accommodate the embedding of secret data, and the marked ciphered overexposed images are generated, denoted as COD^r, $1 \leq r \leq n$. The data hiding procedure is given in Algorithm 2.

Algorithm 2 Data hiding.

```
Input: Ciphered Overexposed Image $CO^r$, Embedded Bit $b$.
Output: Marked Ciphered Overexposed Image $COD^r$.
for $i \leftarrow 1 : P$ do
    for $j \leftarrow 1 : 2 : Q$ do
        $h \leftarrow CO^r_{i,j} - CO^r_{i,j+1}$;
        $l \leftarrow \lfloor (CO^r_{i,j} + CO^r_{i,j+1})/2 \rfloor$;
        if $|2 \times \lfloor h/2 \rfloor + b| \leq \min(2 \times (255 - l), 2 \times l + 1)$ then
            $h' \leftarrow 2 \times h + b$;
            $COD^r_{i,j} \leftarrow l + \lfloor \frac{h'+1}{2} \rfloor$;
            $COD^r_{i,j+1} \leftarrow l - \lfloor \frac{h'}{2} \rfloor$;
        end if
    end for
end for
```

It is noted that the LM has high data redundancy since most groups are expandable. We use run-length coding to compress LM to generate compressed LM. Meanwhile, the compressed LM is required for data retrieval and overexposed image reconstruction, and hence it is embedded into the pixels of the initial few rows of the ciphered overexposed images. The initial few rows of pixels from the ciphered overexposed images will be concealed within the remaining pixels along with the secret data.

3.3. Data Extraction and Overexposed Image Restoration

When having any t marked ciphered overexposed images, the concealed data and the primitive overexposed image can be obtained by the receiver. Assume any t marked ciphered overexposed images are received, represented by $COD^{r_1}, COD^{r_2}, \ldots, COD^{r_t}$, where $\{r_1, r_2, \ldots, r_t\} \subseteq \{1, 2, \ldots, n\}$.

3.3.1. Data Extraction

Extracting concealed secret data is performed on the expandable groups of marked ciphered overexposed images. Denote $(COD^{r_s}_1, COD^{r_s}_2)$ as an expandable group, where $s = 1, 2, \ldots, t$. The data extraction is described in detail as follows:

1. Fix the expandable groups. Extract the compressed LM from the pixels of the initial few rows of marked ciphered overexposed images, and decode it to obtain the associated LM. By the decoded LM, the expandable groups are fixed, that is, if the bit of LM is 0, the corresponding group is expandable.
2. Compute the integer mean and difference of the expandable groups. For an expandable group $(COD_1^{r_s}, COD_2^{r_s})$, the integer mean l' and difference h' are computed by $l' = \left\lfloor \frac{COD_1^{r_s}+COD_2^{r2}}{2} \right\rfloor$ and $h' = COD_1^{r_s} - COD_2^{r_s}$, respectively.
3. Retrieve the secret data by utilizing the difference h'. The embedded secret data are obtained by
$$b = h' \bmod 2, \tag{7}$$
where b is the bit of the secret data.

Algorithm 3 shows the data extraction procedure.

Algorithm 3 Data extraction.

```
Input: Any $t$ Marked Ciphered Overexposed Image $COD^{r_s}$.
Output: Embedded bit $b$.
for $i \leftarrow 1 : P$ do
    for $j \leftarrow 1 : 2 : Q$ do
        if $(COD_{i,j}^{r_s}, COD_{i,j+1}^{r_s})$ is an expandable group then
            $l' \leftarrow \lfloor (COD_{i,j}^{r_s} + COD_{i,j+1}^{r_s})/2 \rfloor$;
            $h' \leftarrow COD_{i,j}^{r_s} - COD_{i,j+1}^{r_s}$;
            $b \leftarrow h' \bmod 2$;
        end if
    end for
end for
```

3.3.2. Overexposed Image Restoration

For overexposed image restoration, we first transform the marked ciphered overexposed images to ciphered overexposed images and then restore the primitive overexposed image from the ciphered overexposed images. In fact, only expandable groups of the ciphered overexposed images are modified for data hiding. Therefore, the non-expandable groups of the marked ciphered overexposed images can be recognized as those of the ciphered overexposed images. On the other hand, with the integer mean l' and the difference h', the expandable groups of the ciphered overexposed images can be obtained by

$$\begin{cases} CO_1^{r_s} = l' + \lfloor \frac{h+1}{2} \rfloor, \\ CO_2^{r_s} = l' - \lfloor \frac{h}{2} \rfloor, \end{cases} \tag{8}$$

where $(CO_1^{r_s}, CO_2^{r_s})$, $1 \leq s \leq t$ is an expandable group of the ciphered image CO^{r_s} and $h = \lfloor \frac{h'}{2} \rfloor$.

After the t ciphered overexposed images are generated, the primitive overexposed image is recovered. According to the encryption key, the identified x_{r_s},$1 \leq s \leq t$, can be obtained. Subsequently, the polynomial $f(x)$ with a degree of $t-1$ is reconstructed via the Lagrange polynomial interpolation technique as represented by

$$f(x) = \sum_{1 \leq v \leq t} \left(CO_{\alpha,\beta}^{r_v} \prod_{1 \leq u \leq t, u \neq v} \frac{x - x_{r_u}}{x_{r_v} - x_{r_u}} \right) \bmod p, \tag{9}$$

where $CO_{\alpha,\beta}^{r_v}$ is the pixel of the ciphered overexposed image CO^{r_v} at location (α, β), $1 \leq \alpha \leq P$, $1 \leq \beta \leq Q$. Obviously, the parameter d is equivalent to the coefficient associated with a term in the function $f(x)$. If $d \neq 0$, the pixel of the scrambled overexposed image is calculated by $O'_{\alpha,\beta} = a_0 + d$ or $O'_{\alpha,\beta+1} = a_0 + d$; otherwise, we have $O'_{\alpha,\beta} = a_0$ or $O'_{\alpha,\beta+1} = a_0$, where a_0 is the constant term of $f(x)$. Finally, the primitive overexposed image is obtained from the scrambled overexposed image according to the inverse operation of the group scrambling with the encryption key. The procedure of overexposed image restoration is provided in Algorithm 4.

Algorithm 4 Overexposed image restoration.

```
Input: Any $t$ Marked Ciphered Overexposed Image $COD^{r_s}$, Encryption Key.
Output: Primitive Overexposed Image $O$.
for $i \leftarrow 1 : P$ do
    for $j \leftarrow 1 : 2 : Q$ do
        if $(COD^{r_s}_{i,j}, COD^{r_s}_{i,j+1})$ is an expandable group then
            $l' \leftarrow \lfloor (COD^{r_s}_{i,j} + COD^{r_s}_{i,j+1})/2 \rfloor$;
            $h' \leftarrow COD^{r_s}_{i,j} - COD^{r_s}_{i,j+1}$;
            $h \leftarrow \lfloor h'/2 \rfloor$;
            $CO^{r_s}_{i,j} \leftarrow l' + \lfloor \frac{h+1}{2} \rfloor$;
            $CO^{r_s}_{i,j+1} \leftarrow l' - \lfloor \frac{h}{2} \rfloor$;
        end if
    end for
end for
Generate $x_{r_s}$ with the encryption key;
for $i \leftarrow 1 : P$ do
    for $j \leftarrow 1 : Q$ do
        Reconstruct $f(x)$ by Equation (9) with $CO^{r_s}_{i,j}$ and $x_{r_s}$;
        $a_0 \leftarrow$ Constant term of $f(x)$;
        $d \leftarrow$ One term of $f(x)$;
        if $d \neq 0$ then
            $O'_{i,j} \leftarrow a_0 + d$;
        else
            $O'_{i,j} \leftarrow a_0$;
        end if
    end for
end for
Obtain $O$ by the inverse operation of the group scrambling with $O'$;
```

4. Experimental Results and Analysis

Herein, the presented method will be evaluated by some experiments, such as effectiveness, security, efficiency, and embedding capacity. Four overexposed images from the common dataset [28] are employed for our experiments, including "1851.pgm", "1933.pgm", "2025.pgm", and "7343.pgm". All the overexposed images possess a 512 × 512 resolution and are in grayscale as shown in Figure 1.

4.1. Experimental Setup

During the experiment, a computer running 64-bit Windows 10 Professional is chosen as the hardware environment. This computer is configured with an Intel Core i5-11600 processor at 2.8 GHz and an 8 GB of Kingston DDR4 memory. The strong hardware platform provides reliable performance and computational resources to ensure efficient execution of our experiments. Matlab 2012a serves as the experimental software tool, which provides comprehensive support for the research conducted in this paper. This software is a professional tool widely used in the fields of scientific computing and engineering, which contributes to the thorough execution of the study. In the numerical processing procedure, all programs are developed by Matlab language and carried out in Matlab

2012a. The built-in plotting tools of Matlab software are utilized to ensure user-friendly visualization of the experimental results.

4.2. Effectiveness of the Presented Scheme

In this experiment, we conduct tests on an overexposed image to demonstrate the effectiveness of the presented scheme. The result of the experiment is given in Figure 5, where (3,4) modified secret sharing is used. According to the proposed overexposed image encryption algorithm, the overexposed image is encrypted into four different ciphered overexposed images as shown in Figure 5b–e. For each ciphered overexposed image, the secret data are concealed into it, and a marked ciphered overexposed image is generated. The generated marked ciphered overexposed images are shown in Figure 5f–i. With any three marked ciphered overexposed images, the concealed secret data are retrieved, and the primitive overexposed image is restored. The restored overexposed images are shown in Figure 5j–m, each of which is identical to the primitive overexposed image. Therefore, the presented approach can efficiently deal with the overexposed image. In [25,26], the overflow pixels are processed by using a labeling technique. In fact, labeling the overflow pixels generates a lot of auxiliary information, especially for overexposed images. As a result, the primitive overexposed image does not have enough room to accommodate it.

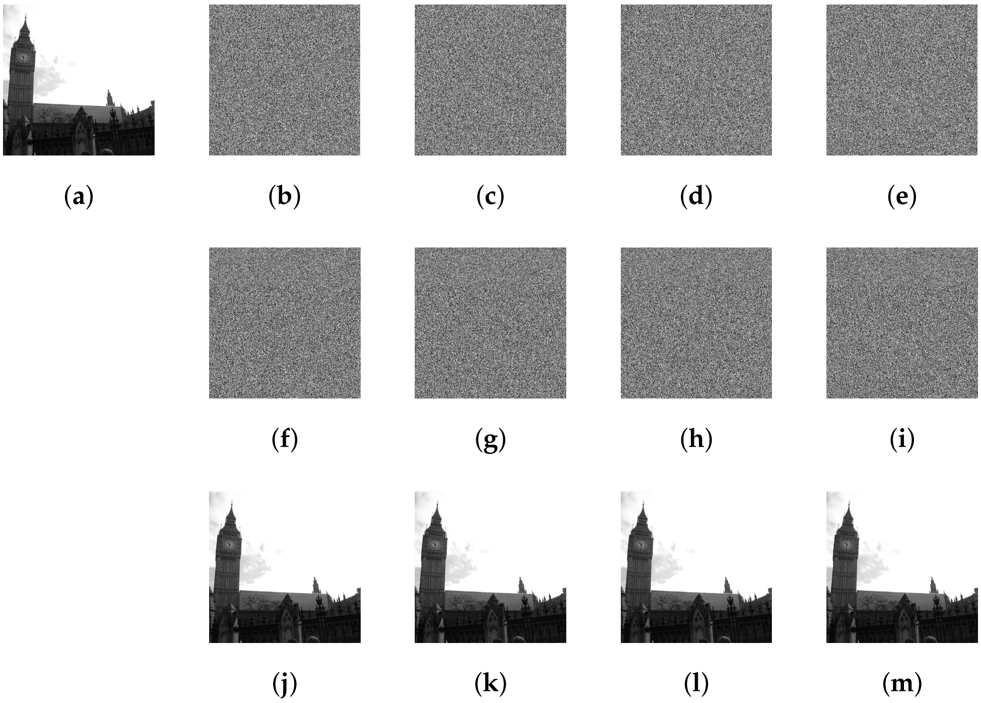


Figure 5. Validate the proposed approach employing (3,4) modified secret sharing. (**a**) The primitive overexposed image, (**b**) the first ciphered overexposed image, (**c**) the second ciphered overexposed image, (**d**) the third ciphered overexposed image, (**e**) the fourth ciphered overexposed image, (**f**) the first marked ciphered overexposed image, (**g**) the second marked ciphered overexposed image, (**h**) the third marked ciphered overexposed image, (**i**) the fourth marked ciphered overexposed image, (**j**) the reestablished overexposed image with (**f**–**h**), (**k**) the reestablished overexposed image with (**f**,**g**,**i**), (**l**) the reestablished overexposed image with (**f**,**h**,**i**), and (**m**) the reestablished overexposed image with (**g**–**i**).

4.3. Security Analysis

The security of the presented approach is evaluated in the following aspects.

4.3.1. Key Strength

According to the key generation process shown in Figure 3, a 256-bit secure hash algorithm (SHA-256) is adopted to generate the encryption key. The security of the encryption key is based on the SHA-256. Thus, the length of the encryption key is 256 bits, and the space of the encryption key is 2^{256}. In order to recover a certain pixel, the adversary needs to obtain parameter x_{r_s}, $1 \leq s \leq t$, $2 \leq t \leq n$. This means that the adversary can break the certain pixel by exploiting A^t_{p-1} attacks, where $p = 251$ for 8-bit overexposed image. On the other hand, the encryption key can be used to encrypt 32 pixels at a time since it is of a 256-bit length. For 32 pixels, the adversary needs $(A^t_{p-1})^{32}$ attacks. Therefore, the strength of the encryption key is $32log_2^{A^t_{p-1}}$.

4.3.2. Imperceptibility

The analysis of the imperceptibility security is illustrated in Figure 6. Figure 6a shows the primitive overexposed image, while Figure 6b presents the image after group scrambling. From Figure 6b, it can be seen that after the first stage of encryption, the image takes on a noise-like appearance and does not show any information about the primitive image. To further improve security, we perform a second round of encryption via modified secret sharing. The scrambled image is segmented into multiple ciphered images (only the effect of one ciphered image is shown here) as shown in Figure 6c. Upon closer examination of these images, we observe that after the second round of encryption, the images exhibit more randomized noise characteristics. More importantly, a sufficient number of ciphered images must be collected if the primitive overexposed image is to be successfully recovered. Figure 6d,e show the marked ciphered images at different embedding rates, respectively. From these two images, we do not obtain any information about the primitive overexposed image and the embedded data, which means that different embedding capacities do not affect the imperceptibility security. Therefore, the presented approach effectively obfuscates the visual characteristics of the image and provides reliable imperceptibility security for the primitive overexposed image.

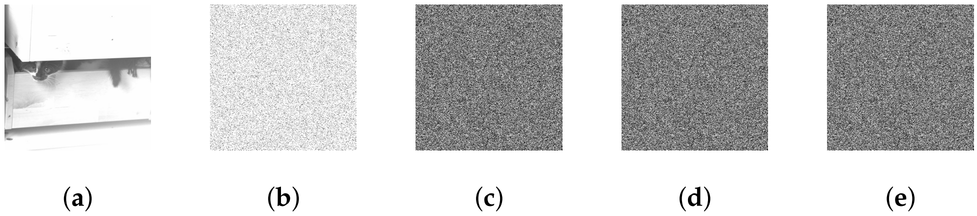
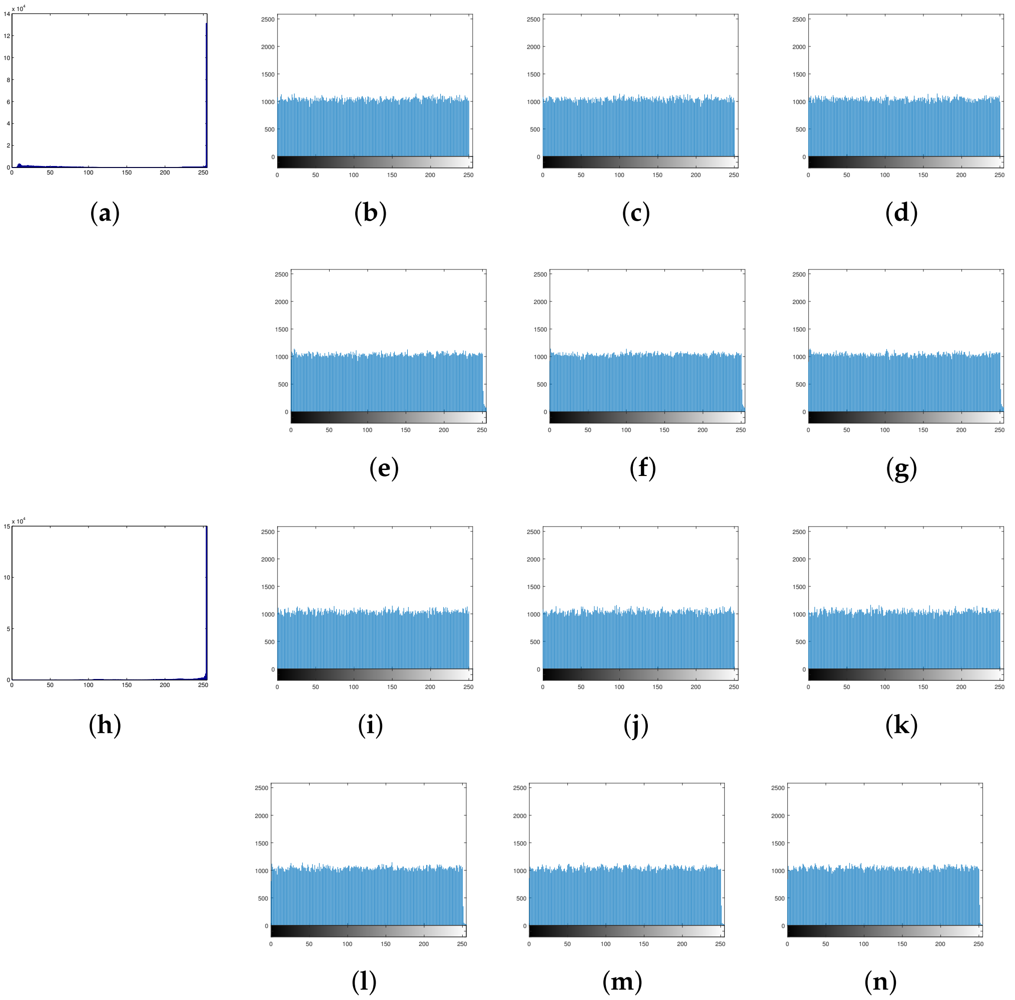


Figure 6. Imperceptibility of the presented approach. (**a**) Primitive overexposed image, (**b**) the scrambled overexposed image, (**c**) the ciphered overexposed image, (**d**) the marked ciphered overexposed image with an embedding rate of 0.2 bpp, and (**e**) the marked ciphered overexposed image with an embedding rate of 0.4 bpp.

4.3.3. Statistical Security

In the proposed scheme of this paper, we adopt a modified secret sharing strategy to share the scrambled overexposed image. This scheme fully utilizes the characteristics of the secret sharing, providing excellent fault tolerance for the overexposed image. To assess the statistical properties of image encryption and data hiding, we plot the histograms of the ciphered and marked ciphered images of two overexposed images, respectively, as shown in Figure 7. The histogram distributions of these two images are shown in Figure 7a,h. Observing the histogram reveals that the pixel values of the primitive image are unevenly distributed. Figure 7b–d,i–k show the histogram distribution of the ciphered image through secret sharing. As can be seen from these histogram distributions, the pixel values of the ciphered images are evenly distributed, thereby effectively improving the statistical security. In addition, Figure 7e–g,l–n show the histogram distributions of the marked ciphered images with embedding rates of 0.1 bpp, 0.2 bpp, and 0.3 bpp, respectively. Observing these six histograms, it is evident that despite different embedding rates, the pixel distribution of the marked ciphered images remains uniform. This indicates that the proposed scheme is effective in protecting image content, whether for different embedding rates of the same image or similar embedding rates for different images.



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

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

(**h**) (**i**) (**j**) (**k**)

(**l**) (**m**) (**n**)

Figure 7. Histograms of the overexposed images for statistical security analysis. (**a**) Primitive overexposed image "1851.pgm", (**b**–**d**) the three ciphered overexposed images of (**a**), (**e**–**g**) the three marked ciphered overexposed images with respect to (**b**–**d**), (**h**) primitive overexposed image "7343.pgm", (**i**–**k**) the three ciphered overexposed images of (**h**), and (**l**–**m**) the three marked ciphered overexposed images with respect to (**i**–**k**).

4.3.4. Occlusion Attack

In the presented scheme, by sharing the primitive overexposed image into *n* ciphered overexposed images with a modified secret sharing method, we enhance the resistance of the image to occlusion attack. An adversary may attempt to hinder the understanding of the image by obscuring or disrupting it. However, due to the adoption of secret sharing, the information of the primitive overexposed image is distributed among multiple marked ciphered overexposed images. Thus, even if a portion of the marked ciphered overexposed images are subjected to an occlusion attack, it is still possible to recover the primitive overexposed image by collecting a sufficient number of marked ciphered overexposed images. This fault tolerance enables the effective restoration of the primitive overexposed image, thereby enhancing the robustness of the proposed scheme against occlusion attacks.

4.4. Discussion on Parameter d

Parameter d is one of the important factors for effectively handling overflow pixels in the presented method. The trend of embedding capacity with the variation of parameter d is illustrated in Figure 8. It can be observed from waveform diagrams that the variation of parameter d has a very small effect on the embedding capacity. It is interesting to note that the optimal choice of parameter d may vary due to the introduction of random numbers in the polynomials. This implies that the embedding capacity exhibits randomness and uncertainty for different values of parameter d. This randomness plays a positive role in improving the security and attack resistance of the scheme. Specifically, in these four images, the fluctuation range of the embedding capacity remains between 0.0018 and 0.0039 as d changes. This variation may be related to the smoothness or randomness of the image. For the image "7343.pgm", the embedding capacity fluctuates the least, showing a relatively stable behavior. Also, the experimental results show that the embedding capacity of "7343.pgm" is higher compared to the other three images. Overall, the effect of the parameter d on the embedding capacity is very small, while the introduced randomness effectively improves the security of the proposed scheme.

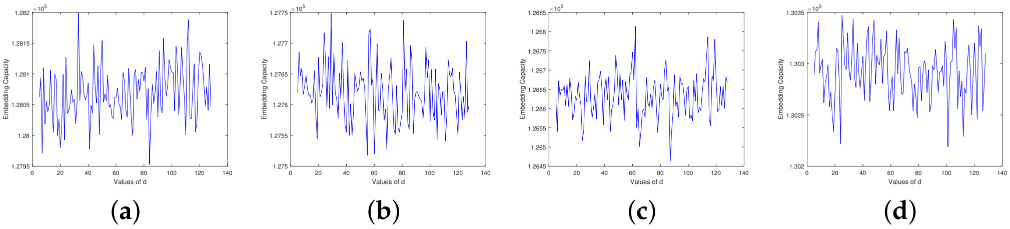


Figure 8. Effect of the parameter d changes on embedding capacity for different overexposed images. (**a**) 1851.pgm, (**b**) 1933.pgm, (**c**) 2025.pgm, and (**d**) 7343.pgm.

4.5. Efficiency Comparison

Efficiency is a key metric of the MRDH-CI method. In this context, we consider the executing time to demonstrate efficiency. Table 1 shows the comparison of the average executing time of the overexposed image encryption phase between the proposed approach and the approach in [26] under various encryption strategies for different overexposed images. For the image encryption of the presented approach, the overexposed image is directly ciphered by the group scrambling and modified secret sharing. Instead, for the image encryption of the method in [26], reserving the embedding room is performed first, and then the image is encrypted by secret sharing. It is known that the presented approach gains a faster processing speed in the image encryption phase by increasing parameters t and n. It means that reserving embedding room increases the extra computational overhead.

Table 1. Comparison of executing time (in second) between the presented approach and the approach in [26] under different encryption strategies for overexposed images.

Schemes	**Overexposed Images**	**Encryption Strategies**				
		(3,4)	**(3,5)**	**(4,5)**	**(3,6)**	**(4,6)**
Hua et al. [26]	1851.pgm	13.53	15.28	11.82	17.06	12.39
	1933.pgm	12.61	14.23	10.38	16.01	12.16
	2025.pgm	15.09	16.07	12.17	18.58	14.05
	7343.pgm	9.95	11.48	8.75	12.77	9.58
Proposed	1851.pgm	6.28	7.76	7.65	8.89	9.24
	1933.pgm	7.15	8.21	7.70	9.17	9.89
	2025.pgm	6.33	9.31	8.07	9.22	9.83
	7343.pgm	6.51	7.47	8.05	9.44	9.53

4.6. Embedding Capacity Analysis

The embedding rate is used to assess embedding performance. The embedding rate (bpp) is the proportion of the total embedded bits to the total pixels of each ciphered overexposed image. For the method in [25], the maximum embedding rate is approximately 3.5 bpp since 7 bits can be embedded into one pixel when sharing two ciphered images. At the same time, the embedding rate does not vary with the distribution of images. However, the embedding rate decreases rapidly as more ciphered images are shared. For the method in [26], it is also possible to achieve a high embedding rate since the hiding room is created from the primitive image during the image encryption stage. But vacating the embedding room from the primitive image requires more computational overhead. As discussed in Section 4.5, the method in [26] has a longer executing time in the image encryption phase. In the proposed scheme, a bit is embedded into a group, and a embedding rate with 0.5 bpp is obtained. Obviously, the presented approach cannot produce a satisfactory embedding capacity due to conservative hiding. To improve the embedding capacity, multi-level hiding is introduced, that is, hiding the data into an expandable group multiple times until the expandable group becomes a non-expandable group.

5. Conclusions

Recently, there has been growing interest in the MRDH-CI approach. This approach ensures the ability to restore the primitive image, even when some data hiders are damaged. However, the MRDH-CI cannot efficiently deal with overexposed images since there are plenty of overflow pixels that are not directly encrypted into multiple ciphered pixels. This paper proposes a MRDH-COI, in which the overflow pixels can be efficiently processed. First of all, the pixels of the group of the overexposed image are decomposed into two parts so that they can be encrypted by secret sharing. In order to encrypt the overexposed image into multiple ciphered overexposed images, the overexposed image is first scrambled by group scrambling and then converted by modified secret sharing. The obtained ciphered overexposed images have the ability to facilitate data hiding since their differences are retained. With the symmetry of the difference retaining, the difference expansion algorithm can be exploited to conceal the secret data within ciphered overexposed images to generate marked ciphered overexposed images. When any sufficient marked ciphered overexposed images are authorized, the primitive overexposed image and the concealed data are retrieved symmetrically. Finally, an experiment and its analysis are provided to illustrate the effectiveness and efficiency of the presented approach.

Author Contributions: Conceptualization, B.C. and J.C.; methodology, B.C. and R.Y.; software, R.Y., W.F. and X.Z.; validation, B.C. and J.C.; formal analysis, R.Y. and J.C.; investigation, W.F. and X.Z.; writing—original draft preparation, B.C. and R.Y.; writing—review and editing, B.C. and R.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China (No. 62102101) and the Doctoral Scientific Research Foundation of Guangdong Polytechnic Normal University (No. 2021SDKYA101).

Data Availability Statement: Data will be made available on request.

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

References

1. Mathivanan, P.; Balaji Ganesh, A. QR code based color image stego-crypto technique using dynamic bit replacement and logistic map. *Optik* **2021**, *225*, 165838.
2. Mathivanan, P.; Balaji Ganesh, A. ECG steganography using Base64 encoding and pixel swapping technique. *Multimed. Tools Appl.* **2023**, *82*, 14945–14962. [CrossRef]
3. Yang, Y.; Xiao, X.; Cai, X.; Zhang, W. A Secure and Privacy-Preserving Technique Based on Contrast-Enhancement Reversible Data Hiding and Plaintext Encryption for Medical Images. *IEEE Signal Process. Lett.* **2020**, *27*, 256–260. [CrossRef]
4. Peng, Y.; Zhao, Y.; Mao, N.; Wang, J.; Fang, Y.; Zhang, T.; Shi, F. Color image reversible data hiding based on multi-channel synchronized histogram. *J. King Saud Univ. Comput. Inf. Sci.* **2023**, *35*, 101804. [CrossRef]

5. Weng, S.; Zhou, Y.; Zhang, T.; Xiao, M.; Zhao, Y. Reversible data hiding for JPEG images with adaptive multiple two-dimensional histogram and mapping generation. *IEEE Trans. Multimed.* **2023**, *25*, 8738–8752. [CrossRef]
6. Mandal, P.C.; Mukherjee, I.; Chatterji, B.N. High capacity reversible and secured data hiding in images using interpolation and difference expansion technique. *Multimed. Tools Appl.* **2021**, *80*, 3623–3644. [CrossRef]
7. Tian, J. Reversible data embedding using a difference expansion. *IEEE Trans. Circuits Syst. Video Technol.* **2003**, *13*, 890–896. [CrossRef]
8. Sahu, A.K.; Swain, G. High fidelity based reversible data hiding using modified LSB matching and pixel difference. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 1395–1409. [CrossRef]
9. Qi, W.; Li, X.; Zhang, T.; Guo, Z. Optimal Reversible Data Hiding Scheme Based on Multiple Histograms Modification. *IEEE Trans. Circuits Syst. Video Technol.* **2020**, *30*, 2300–2312. [CrossRef]
10. Weng, S.; Tan, W.; Ou, B.; Pan, J.S. Reversible data hiding method for multi-histogram point selection based on improved crisscross optimization algorithm. *Inf. Sci.* **2021**, *549*, 13–33. [CrossRef]
11. Pan, Z.; Gao, X.; Gao, E.; Fan, G. Adaptive Complexity for Pixel-Value-Ordering Based Reversible Data Hiding. *IEEE Signal Process. Lett.* **2020**, *27*, 915–919. [CrossRef]
12. Zhang, T.; Li, X.; Qi, W.; Guo, Z. Location-Based PVO and Adaptive Pairwise Modification for Efficient Reversible Data Hiding. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2306–2319. [CrossRef]
13. He, W.; Cai, Z. Reversible Data Hiding Based on Dual Pairwise Prediction-Error Expansion. *IEEE Trans. Image Process.* **2021**, *30*, 5045–5055. [CrossRef]
14. Yu, C.; Zhang, X.; Wang, D.; Tang, Z. Reversible data hiding with pairwise PEE and 2D-PEH decomposition. *Signal Process.* **2022**, *196*, 108527. [CrossRef]
15. Kouhi, A.; Sedaaghi, M.H. Reversible data hiding based on high fidelity prediction scheme for reducing the number of invalid modifications. *Inf. Sci.* **2022**, *589*, 46–61. [CrossRef]
16. Dragoi, I.C.; Coltuc, D. On the Security of Reversible Data Hiding in Encrypted Images by MSB Prediction. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 187–189. [CrossRef]
17. Wang, Y.; He, W. High Capacity Reversible Data Hiding in Encrypted Image Based on Adaptive MSB Prediction. *IEEE Trans. Multimed.* **2022**, *24*, 1288–1298. [CrossRef]
18. Gao, K.; Horng, J.H.; Chang, C.C. High-capacity reversible data hiding in encrypted images based on adaptive block encoding. *J. Vis. Commun. Image Represent.* **2022**, *84*, 103481. [CrossRef]
19. Sui, L.; Li, H.; Liu, J.; Xiao, Z.; Tian, A. Reversible Data Hiding in Encrypted Images Based on Hybrid Prediction and Huffman Coding. *Symmetry* **2023**, *15*, 1222. [CrossRef]
20. Qian, Z.; Xu, H.; Luo, X.; Zhang, X. New Framework of Reversible Data Hiding in Encrypted JPEG Bitstreams. *IEEE Trans. Circuits Syst. Video Technol.* **2019**, *29*, 351–362. [CrossRef]
21. Ge, B.; Ge, G.; Xia, C.; Duan, X. High-Capacity Reversible Data Hiding in Encrypted Images Based on 2D-HS Chaotic System and Full Bit-Plane Searching. *Symmetry* **2023**, *15*, 1423. [CrossRef]
22. Wu, H.T.; Cheung, Y.M.; Yang, Z.; Tang, S. A high-capacity reversible data hiding method for homomorphic encrypted images. *J. Vis. Commun. Image Represent.* **2019**, *62*, 87–96. [CrossRef]
23. Zheng, S.; Wang, Y.; Hu, D. Lossless Data Hiding Based on Homomorphic Cryptosystem. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 692–705. [CrossRef]
24. Ke, Y.; Zhang, M.Q.; Liu, J.; Su, T.T.; Yang, X.Y. Fully Homomorphic Encryption Encapsulated Difference Expansion for Reversible Data Hiding in Encrypted Domain. *IEEE Trans. Circuits Syst. Video Technol.* **2020**, *30*, 2353–2365. [CrossRef]
25. Chen, B.; Lu, W.; Huang, J.; Weng, J.; Zhou, Y. Secret Sharing Based Reversible Data Hiding in Encrypted Images With Multiple Data-Hiders. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 978–991. [CrossRef]
26. Hua, Z.; Wang, Y.; Yi, S.; Zhou, Y.; Jia, X. Reversible Data Hiding in Encrypted Images Using Cipher-Feedback Secret Sharing. *IEEE Trans. Circuits Syst. Video Technol.* **2022**, *32*, 4968–4982. [CrossRef]
27. Shamir, A. How to Share a Secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
28. The Bossbase 1.01 Image Database, 2023. Available online: http://dde.binghamton.edu/download/ (accessed on 20 November 2023).

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.