Image Enhancement and Cloud Secure Transmission Based on Reversible Image Information Hiding Technology

Zailin Li

(Corresponding author: Zailin Li)

School of 3D Printing, Xinxiang University, Xinxiang 453003, China

Email: lizailin@126.com

(Received Aug. 15, 2023; Revised and Accepted Apr. 24, 2024; First Online June 22, 2024)

Abstract

Image distortion and poor transmission security are the key problems restricting the reversible image information hiding technique. The existing image enhancement algorithms do not consider the restoration problem, failing to obtain the original image after obtaining secret information, and the object of study is usually the gray image in the medical field. This study proposes an adaptive image enhancement algorithm based on gray-level images and constructs a reversible information-hiding algorithm based on a constant tone plane. In addition, a new reversible information-hiding algorithm based on MSB prediction and error embedding is proposed to enhance the security of image transmission. Compared with the traditional algorithms, the gray image and color image enhancement algorithms proposed in this study improve the image quality by 8% and 15%, respectively. The change rate of image pixels encrypted by the cloud security transmission algorithm is more than 99%. The proposed image enhancement and encryption algorithm can significantly improve image quality, providing a development platform for applying reversible information-hiding technology in images.

Keywords: Cloud Secure Transmission; Error Location; Gray Level Histogram; Image Enhancement; Reversible Information Hiding Technology

1 Introduction

Nowadays, Reversible Data Hiding (RDH) was born. This technique can add secret message into various types of data carriers, which can completely extract secret information [18]. The combination of RDH and image enhancement technology has become a hot research direction recently. RDH technology has practical value, so it is required to study key RDH technologies for image enhancement and cloud secure transmission [8]. Scholars focus on the study of grayscale images in the medical and military fields. However, existing algorithms still have the problem of weak contrast of gray image, and there are few researches on algorithms based on color image enhancement and data encryption [12]. Therefore, three innovations are made in this research: first, an adaptive enhancement algorithm based on gray image is presented; secondly, the image enhancement and encryption algorithms of color images are studied, and the RDH algorithm of color image contrast enhancement with constant tone plane is proposed.

Thirdly, to ensure the security of image transmission during cloud transmission, a new encryption image RDH algorithm is proposed. In response to the problem that existing algorithms cannot simultaneously achieve high embedding capacity and good reconstructed image quality, this paper proposes a reversible information hiding algorithm for encrypted images based on the most significant bit prediction and error embedding. On the one hand, the innovation of the research takes into account all types of prediction errors and can correctly recover all pixels with prediction errors; On the other hand, the algorithm in this paper uses error blocks to mark the location of prediction errors, and uses message blocks to embed secret information.

The contribution of this study is to provide reference for the fusion of reversible information hiding algorithms and image enhancement algorithms, while also exploring research on color images. This research mainly analyzes the image RDH technology from four aspects: The first part is the review and discussion of the current RDH algorithm related literature; the second part is to build RDH algorithm based on gray image, color image and cloud security transmission. The third part is the comparative analysis and application test of the results of image enhancement and encryption algorithms. The last part is the conclusion of the full text.

2 Related Work

Recently, RDH developed fast and formed a series of classic frameworks, such as histogram shift, prediction error extension, etc. Based on these classical algorithms, a large number of scholars have explored more optimized image enhancement techniques [5]. Among them, He et al. applied RDH to color images and constructed an image hiding strategy with 2D histogram translation based on the histogram shift framework, which could enhance the image quality by deleting the number of invalid pixels. The scheme processed images with higher PSNR ratio and smaller image files [6]. Wang and Liu proposed a variational histogram equalization framework to adjust image pixel values (PV) through energy functional. This algorithm had higher convergence and feasibility [21]. Chen et al. transformed the encrypted image with the freely selected image. To ensure image conversion's quality, an algorithm based on gray co-occurrence matrix was proposed, which used medical feature extraction to improve model's efficiency and image quality. Under this method, the RMS value was reduced by 5% [2]. Wu et al. constructed a histogram translation algorithm with checkerboard development for prediction optimization of encrypted images. The image output by this enhancement algorithm has better bits per pixel [24]. Based on the cloud-edge model, Chen and Shiu suggested a new technique with distributed encrypted images. This technology takes edge nodes as Bridges, uses XOR secret sharing as cryptographic tags, and imbeds differential extension for image and processing. This algorithm has good applicability in image RDH [3].

To ensure the security of images in RDH technology, scholars in this field studied a large quantity of models with image cloud security transmission. Among them, Anushiadevi and Amirtharajan introduced elliptic curve cryptography to obtain encryption before embedding, and combined the original image with the confidential data through the addition homomorphism property. The image memory after encryption was unchanged by this method, and 100% reversibility was achieved [1]. Wang et al. suggested a new block-based image encryption method. This method hides the encrypted data into each block through Huffman coding, which ensures the image's security while achieving a higher embedding rate [22]. Qu et al. proposed a reversible data hiding method for encrypted images, which enhanced its embedding capacity and security. This method also ensured the embedding content and security of the image [16]. Qian et al. suggested a hiding algorithm for encrypted color images. In this algorithm, the user could decrypt the original bit stream directly by constructing a mark encrypted image bit stream. This method had a higher embedding rate and easier user-oriented operation [15]. Wang et al. suggested an image cloud transmission encryption technology based on quadtree segmentation and integer wavelet transform. The technology encrypted images by 2×2 blocks to ensure higher security, and introduced integer wavelet transform to transform the encrypted images. This scheme improved the embedding rate of encrypted data [23]. Yin et al. proposed a point target policy algorithm based on adaptive Most Significant Bit (MSB) and Haverman coding, and conducted experimental tests. Compared with other algorithms, this algorithm had a higher embedding rate [25].

To sum up, image enhancement and image encryption based on RDH technology have developed so far, and a large number of algorithms have emerged. There are histogram shift and prediction error based on image enhancement, and MSB encryption algorithm based on cloud security transmission. However, the above algorithms still have many shortcomings. To handle the issue of low contrast and low security of gray image, an adaptive enhancement algorithm of gray image is constructed. To handle the issue of uneven color and saturation in color image enhancement and hiding, an RDH algorithm based on constant tone plane is constructed. To handle the issue of low information security in cloud transmission, an encrypted image RDH algorithm is proposed. The aim of this study is to provide better scientific advice for image RDH technology.

3 Image Enhancement and Encryption in RDH Technology

Currently, the algorithms for image RDH technology are not perfect, and image distortion and transmission security are two prominent problems. Therefore, an adaptive enhancement algorithm with gray-scale image is constructed. Meanwhile, the image enhancement and encryption algorithms of color images are discussed, and a color image contrast enhancement algorithm based on constant tone plane is suggested. In addition, to ensure the security of image transmission, a new RDH algorithm with MSB Prediction and Error Embedding (MSB-EE) is constructed.

3.1 RDH Technology Based on Image Contrast Enhancement

The existing methods for gray image enhancement are mainly concentrated in the military medical field, but these fields have high requirements for image security and quality, and some traditional algorithms can not meet the needs of both. Therefore, an adaptive gray-scale image enhancement algorithm is proposed in this paper by combining RDH technology and image enhancement. The algorithm enhances contrast by performing Pixel concentration ratio (PCR) segmentation for Regions of interest (ROI) and embedding secret information. The gray value of Regions of non-interest (NROI) is lowered to embed more secret information. The algorithm flow is shown in Figure 1.

First, this study used an adaptive threshold detector to determine the threshold and divide the ROI and NROI.

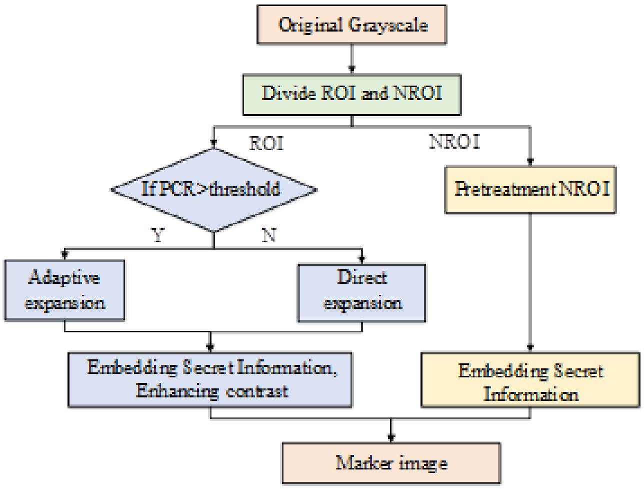


Figure 1: Grayscale enhancement process based on reversible information hiding

The specific partitioning method is as follows: when the PV is greater than the threshold value, it is regarded as the research target, and the unified value is 0, which is displayed in black; when the PV is less than the threshold, the unified value is 255 and is displayed in white. Finally, the outermost PV of 0 is used as the ROI boundary. When histogram stretching and secret information embedding are performed on ROI, PCR needs to be calculated first. The result is the ratio of pixels' number in the target bias [0,127] or [128,255] to the pixels' total number in the ROI. The calculation method of pixel moving distance D_{shift} in ROI region is shown in Equation (1).

$$D_{shift} = \begin{cases} 255 - ROI_{\max}, & PCR_{[0,127]} > r \\ ROI_{\min}, & PCR_{[128,255]} > r \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

In Equation (1), $ROI_{\max}$ and $ROI_{\min}$ are the biggest and smallest PV; r is a ratio between 0 and 1, setting the value to 0.7 based on a large number of calculations. Then you need to stretch the histogram to create more space to add secret message, and the stretching equation is shown in Equation (2).

$$\begin{aligned} ROI_{stretch}(x,y) &= round[(L_{\max} - L_{\min}) \\ &\quad \times \frac{ROI_{shift}(x,y) - ROI'_{\min}}{ROI'_{\max} - ROI'_{\min}} + L_{\min}] \end{aligned} \tag{2}$$

In Equation (2), $ROI_{stretch}(x,y)$ is the PV of the stretched image; $L_{\max}$ and $L_{\min}$ are the upper and lower boundaries of the stretched pixel; $ROI_{shift}(x,y)$ the PV of the picture after moving the corresponding pixel; $ROI'_{\max}$ and $ROI'_{\min}$ are the biggest and smallest values. By stretching the image, more space is gained. By embedding the secret information into the non-empty PV surrounded by the empty PV until there is no non-empty PV inside, the specific calculation method of embedding is shown in Equation (3).

$$k' = \begin{cases} k + b_i, & \text{if } k = k_{peak} \ \& \ k_{peak} \in [0,126] \\ & \quad \& h(k_{peak}+1) = 0 \\ k - b_i, & \text{if } k = k_{peak} \ \& \ k_{peak} \in [129,255] \\ & \quad \& h(k_{peak}-1) = 0 \\ k, & \text{if } k \neq k_{peak} \end{cases} \tag{3}$$

In Equation (3), k is the value of $ROI_{stretch}(x,y)$; b_i denotes the i position, which has a value of 0 or 1. k_{peak} is the peak pixel, that is, it has the biggest number of pixels and the adjacent PV are empty; $h(k_{peak})$ is the number of pixels of the peak pixel. After multiple embeddings, the histogram distribution before and after the algorithm embeddings is shown in Figure 2.

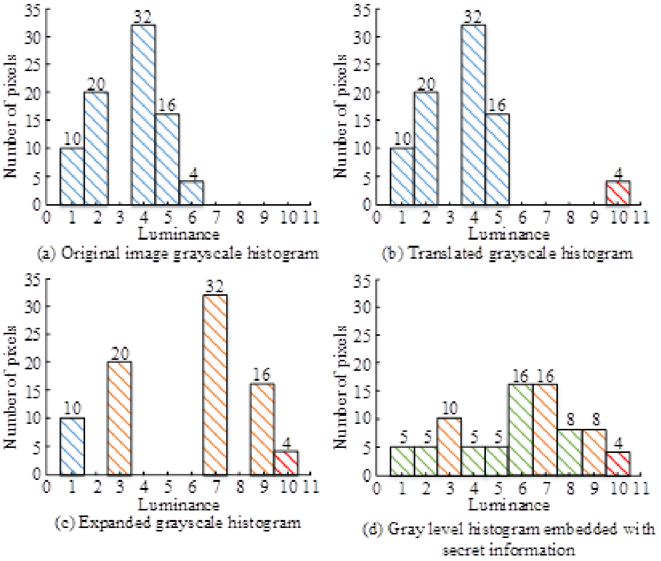


Figure 2: Schematic diagram of histogram distribution before and after embedding

To ensure the quality of the image, the study enhances the internal contrast by reducing the value of NROI pixels.

$$NROI_{preprocess}(x,y) = NROI(x,y) - NROI_{\min} \tag{4}$$

In Equation (4), $NROI_{preprocess}(x,y)$ denotes the background PV after processing; $NROI(x,y)$ refers to the original background PV; $NROI_{\min}$ denotes the minimum PV in the background. When the secret information cannot be fully embedded within the ROI, the remaining information will be embedded in the background. The secret information is replaced by the Least Significant Bit (LSB) of up to three pixels in the background to satisfy that the PV of the background changes within the range of [0,7] after embedding. Use N to denote the number of secret information bits which required to be embedded in the background, and the embedding equation is shown in Equation (5).

$$LB_j = b_i, j \in \{1,2,3\} \tag{5}$$

In Equation (5), LB_j denotes the j-th last bit of NROI. After the user sends the picture with the secret message to the receiver, the user needs to get the secret message and the original picture through image enhancement, which is mainly split into three steps. First, LSB is read to obtain the quantity of secret message bits in NROI, and then Equation (5) is used to reverse solve the secret message in NROI. Secondly, the secret message in ROI is obtained by inverse solution of Equation (3). Finally, Equation (1) and Equation (2) are used to reverse solve the original image.

When encountering the RDH and image enhancement of color images, due to the limitation of hue and saturation in color images, the processing method of gray image is not suitable for this [20]. Therefore, a contrast enhancement and RDH algorithm for color pictures is proposed with constant tone plane. The specific algorithm processing flow is shown in Figure 3.

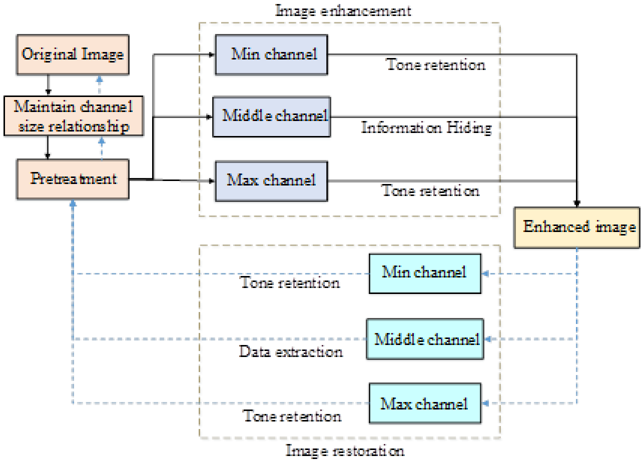


Figure 3: Flowchart of reversible information hiding and enhancement algorithm for color images

In the preprocessing, this study makes space for the secret information hiding by the size relation preserving operation; Then the IP of the pre-processed image is obtained through the mapping relationship, and the mapping method is shown in Equation (6).

$$Value_{mapping} = round[\frac{Value_{maintain}}{255} \times (255 - S \times 2) + S] \quad (6)$$

In Equation (6), $Value_{mapping}$ denotes the PV after mapping; $Value_{maintain}$ denotes the PV maintained after the channel size relationship; S is the PV that needs to be left empty for the secret message. In this paper, the segmsegmed middle channel is selected for secret information hiding, and secret message is added into the picture after preprocessing, as shown in Equation (7).

$$I_{e-mid}(a,b) = \begin{cases} I_{p-mid}(a,b) - 1, & \text{if } I_{p-\min d}(a,b) < f_L \\ I_{p-mid}(a,b) - b, & \text{if } I_{p-\min d}(a,b) = f_L \\ I_{p-mid}(a,b), & \text{if } f_L < I_{p-\min d}(a,b) < f_R \\ I_{p-mid}(a,b) + b, & \text{if } I_{p-\min d}(a,b) = f_R \\ I_{p-mid}(a,b) + 1, & \text{if } I_{p-\min d}(a,b) < f_R \end{cases} \quad (7)$$

In Equation (7), $I_{e-mid}(a,b)$ denotes the median value of embedded pixels; $I_{p-mid}(a,b)$ denotes the median value of pixels separated after preprocessing; b_i denotes the value of i-th secret information; f_L and f_R are the PV with the most pixels, and $f_L < f_R$. To keep the color image hue constant, the research proposed a constant tone plane, as shown in Figure 4. All on the same plane have the same hue [11].

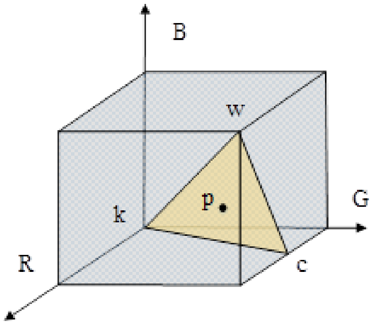


Figure 4: Schematic diagram of a constant tone plane

The value of the same constant tonal plane is set as (p_r, p_g, p_b), then the specific tonal preservation algorithm is shown in Equation (8).

$$\begin{cases} p'_r = p_r + amplitude \\ p'_g = p_g + amplitude \\ p'_b = p_b + amplitude \end{cases} \quad (8)$$

In Equation (8), (p'_r, p'_g, p'_b) denotes the PV after hue preservation; *amplitude* is the value of the color change. After the tone is maintained, the minimum channel and maximum channel PV are adjusted as stated by the change value of the middle channel pixel to avoid image distortion [13]. Then, the receiver first obtains the PV of the three-channel variable recovery channel to obtain the secret information; then Equation (6) is applied to inversely solve the PV of the picture before mapping, and finally the original image is obtained.

3.2 Cloud Security Transmission Algorithm Based on MSB-EE

LSB is used in the above image encryption algorithm to hide information, but the hiding efficiency is lower than MSB algorithm when the hiding quality is the same [9]. Therefore, based on MSB-EE, a more applicable RDH technology for image cloud security transmission is proposed. Figure 5 illustrates the encryption and decryption process.

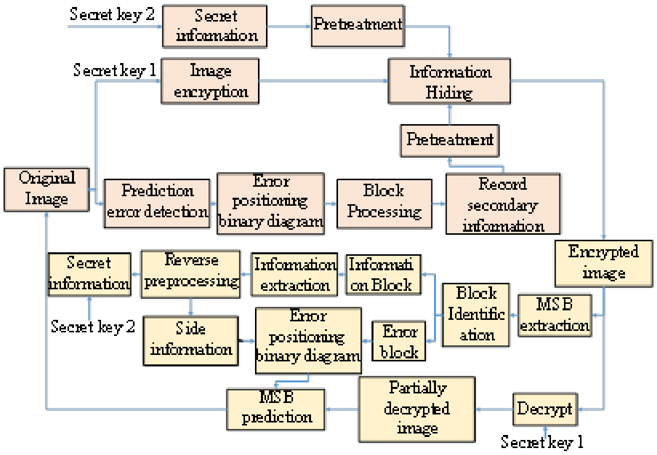


Figure 5: Process of reversible information hiding algorithm for encrypted images based on MSB-EE

First, the prediction error detection is performed on the initial image [7]. By comparing the initial PV, the predicted PV and the inverse MSB PV, the prediction error of the pixel is determined. The MSB is predicted 0 and 1. The calculation method of error location binary graph is shown in Equation (9).

$$M_e(i,j) = \begin{cases} 0, & \text{if } \triangle_I(i,j) < \triangle_{INV}(i,j) \\ 1, & \text{else} \end{cases} \tag{9}$$

In Equation (9), $M_e(i,j)$ denotes the value of each pixel in the error positioning binary graph; $\triangle_I(i,j)$ is the absolute value of the difference between the predicted PV and the initial PV; $\triangle_{INV}(i,j)$ denotes the absolute difference between the inverse MSB PV and the predicted PV. Then, the labeled error location binary graph Mem is obtained by block processing. The specific labeling methods are three kinds of blocks: defining error blocks (including prediction error blocks), message blocks (for embedding information blocks), and marking blocks (distinguishing error blocks and message blocks).

To make the image content unreadable during transmission, the image is encrypted. Then, the pseudo-random sequence and the original image are XOR operation to get the encrypted image, the model is shown in Equation (10).

$$I_e(i,j) = \sum_{k=1}^{8} (I(i,j)_k \oplus S(i,j)_k) \times 2^{k-1} \tag{10}$$

In Equation (10), $I_e(i,j)$ is the PV after encryption; k denotes bit k of the binary stream; $I(i,j)$ denotes the initial PV; $S(i,j)$ denotes a pseudo-random sequence PV. To prevent the receiver from misdiagnosing the content of the marker block after receiving the encrypted image, the study defined the secondary information SI to record the predicted error position, recorded the second piece through Fs, and recorded the last piece with FI. When the value is 0, it means that there is no prediction error in the block, otherwise it is 1. The second part of the secondary information record is the same content as the flag block in the error block. Change the first binary code in the error block to 0 when both are the same. The modified prediction error position was recorded simultaneously by coordinate method and arithmetic coding. The result with the lower median value of the two is taken as the prediction error result SI.

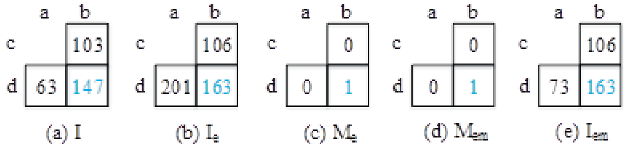
Before embedding secret information and secondary information, the research distinguishes message blocks from marker blocks by preprocessing. Secondary information is processed in the same way as secret information, as shown in Equation (11).

$$T(k) = \begin{cases} 1, & \text{if } k > 5 \text{ and } \sum_{u=0}^{5} SM_e(k-u) = 6 \\ & \quad \text{and } \sum_{u=1}^{5} T(k-u) = 0 \\ 0, & \text{else} \end{cases} \tag{11}$$

In Equation (11), $T(k)$ is the intermediate variable. When it is 1, you need to insert A 0 after bit k of information. When it is 0, no encoding is inserted. SM_e is the embedded secret information with the same value as T. After the initial picture is encrypted, the original MSB value in the picture needs to be replaced with the PV after the secret message is hidden, and the replacement method is shown in Equation (12).

$$I_{em}(i,j) = \begin{cases} I_e(i,j), & \text{if } M_{em}(i,j) \in B_e \\ & \quad \& \triangle_I(i,j) = \triangle_{INV}(i,j) \\ M_{em}(i,j) \times 128 & \\ \quad + \bmod\ (I_e(i,j), 128), & \text{else} \end{cases} \tag{12}$$

In Equation (12), $I_{em}(i,j)$ denotes the PV after marking encryption; $M_{em}(i,j)$ denotes the encrypted PV. The specific replacement process is shown in Figure 6.



	a	b
c		103
d	63	147

(a) I

	a	b
c		106
d	201	163

(b) I$_e$

	a	b
c		0
d	0	1

(c) M$_e$

	a	b
c		0
d	0	1

(d) M$_{em}$

	a	b
c		106
d	73	163

(e) I$_{em}$

Figure 6: The embedding process of prediction error pixel information

When the receiver gets the encrypted image, the initial picture and secret message are obtained through reverse processing. When extracting information, MSB value is obtained by Equation (13).

$$M_{MSB}(i,j) = [I_{em}(i,j)/128] \tag{13}$$

In Equation (13), $M_{MSB}(i,j)$ denotes the MSB value of the corresponding pixel of I_{em}. Then, the reconstructed image is reversely solved according to Equation (10) to get the partially decrypted image PV, and the complete $M_e(i,j)$ is obtained according to Equation (14).

$$M_e(i,j) = \begin{cases} 1, & \text{if } M_{MSB}(i,j) = 1 \\ & \quad \& M_{MSB}(i,j) \in B_e \\ 0, & \text{else} \end{cases} \quad (14)$$

In Equation (14), B_e is sequence M_e. Finally, according to Equation (15), the image is reconstructed and the original image is obtained.

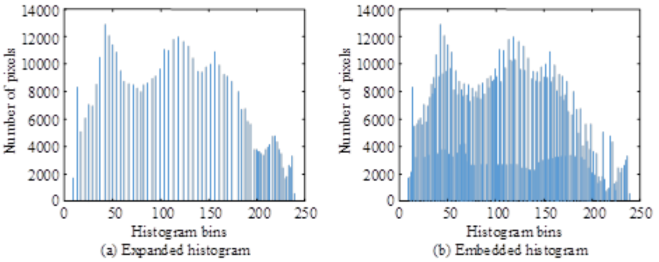
$$I(a,b) = \begin{cases} I'(a,b)_{MSB=0}, & \text{if } (\triangle_0(a,b) < \triangle_1(a,b) \\ & \&M_e(a,b) = 0) \\ & \text{or } (\triangle_0(a,b) > \triangle_1(a,b) \\ & \&M_e(a,b) = 1) \\ I'(a,b)_{MSB=1}, & \text{if } (\triangle_0(a,b) > \triangle_1(a,b) \\ & \&M_e(a,b) = 0) \\ & \text{or } (\triangle_0(a,b) < \triangle_1(a,b) \\ & \&M_e(a,b) = 1) \\ I'(a,b), & \text{else} \end{cases} \quad (15)$$

In Equation (15), $I'(a,b)$ denotes the PV of partially decrypted image; $\triangle_0(a,b)$ denotes the absolute value of the predicted PV and $I'(a,b)_{MSB=0}$; $\triangle_1(a,b)$ denotes the absolute value of the predicted PV and $I'(a,b)_{MSB=1}$. The encrypted image completed by this method can embed more secret information, and it is not easy to steal information by non-recipients.

4 Performance Analysis of Image Enhancement and Encryption Algorithms based on RDH Technology

Firstly, the performance of adaptive enhancement algorithm based on gray image is tested in gray image database. The effect of image quality enhancement is judged by comparing the histogram and visual vision before and after image embedding information, and compared with other popular algorithms. Different image quality evaluation indexes are applied to assess the performance of the proposed algorithm for picture information hiding and quality enhancement. Figure 7 shows the histogram comparison of grayscale images before and after embedding information.

In Figure 7, the expanded histogram leaves more space for secret information to be embedded. After information embedding, the distribution trend is still the same as the initial picture, so as to avoid the situation of picture distortion, and the secret information embedding is more uniform. At the same time, the suggested method is compared with three other methods, including the RDH algorithm based on Receding horizon control Reversible data hiding. RHCRDH), (Automatic Color Equalization Reversible data hiding, ACERDH and Reversible data hiding Multi-box pruning (RDHMBP) algorithm to enhance contrast and maintain original image brightness. The experiments were compared when the embedded secret information was 0.1 bit/pixel, 1 bit/pixel and 2 bit/pixel respectively, and the results were shown in Figure 8.



(a) Expanded histogram
(b) Embedded histogram

Figure 7: Comparison of Histograms after Expansion and Embedding

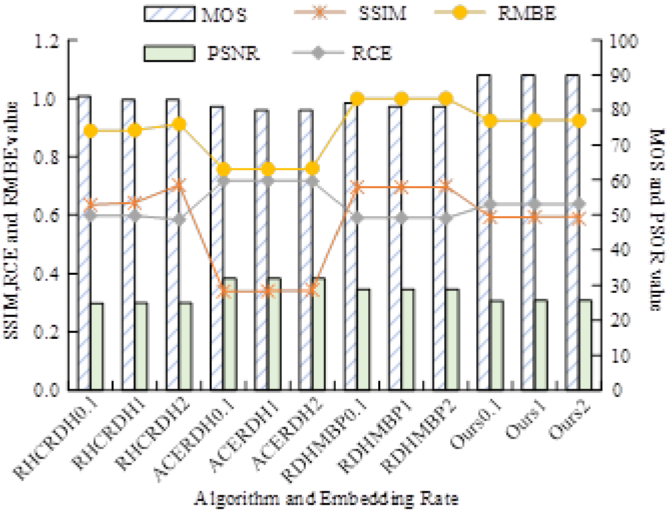


Figure 8: Evaluate results using indicators from different algorithms

In Figure 8, to compare the performance of different algorithms, five indicators are introduced to evaluate image quality, namely MOS and PSNR, SSIM, RCE and RMBE. It can be found that the algorithm proposed in this study has the highest MOS score, and has better image enhancement effect. And the RCE value is greater than 0.6, which indicates that the processed picture's quality is enhanced and the effect is better than that of the initial picture.

To assess the effect of the RDH for color image contrast enhancement based on constant tonal plane proposed in this study, three new indexes are added to the indexes selected for gray image. Hueand Lightness Dependent Correction to Industrial Colour Difference Evaluation, Hu1eand lightness dependent correction to industrial colour difference Evaluation, CIEDE2000 and No reference image spatial quality evaluator (BRISQUE). It is compared with the current popular color image enhancement algorithms, including the contrast enhancement model with deep learning to handle the issue of low illumination image. Contrast limited adaptive histogram equalization, Contrast limited adaptive histogram equalization, CLAHE and Multi-Scale Retinex with Color Restoration (MSRCR). Figure 9 shows the results after processing with four algorithms respectively.

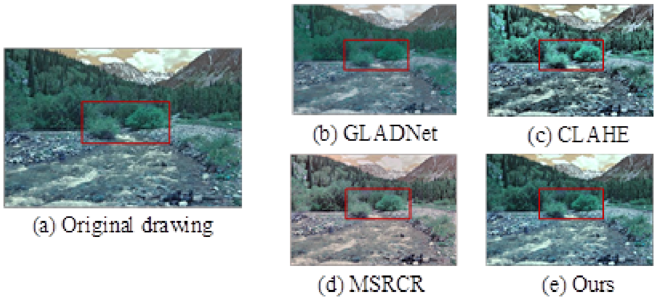
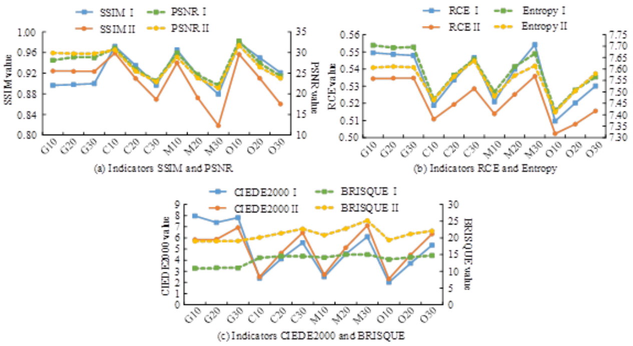

(a) Original drawing
(b) GLADNet
(c) CLAHE
(d) MSRCR
(e) Ours

Figure 9: Comparison of Detail Visibility of Different Algorithms

In Figure 9, the detail enhancement result of the suggested model is better. After GLADNet algorithm is used to enhance the image, the retention effect of the details such as leaves is poor. After CLAHE algorithm enhancement, the brightness of the image has been optimized, but the color conversion is rather stiff, resulting in the loss of the original color of the enhanced object. The image distortion is obvious and does not conform to human visual sense. After MSRCR algorithm enhancement, the overall color of the image changes, the red part deepens, and the color distortion occurs. There is a wide range of color distortion, and the overall effect has a large deviation from the initial picture. After the enhancement of color image by the proposed method, it not only ensures the relative balance of the original image hue, contrast and brightness, but also increases the details in the leaves and water, which has a better enhancement effect on the image. At the same time, the above image quality index is applied to assess the effect of the model objectively. Two commonly used color image datasets were selected, denoted by I and II respectively. By controlling the number of empty PV at both ends of the image histogram, the index values of various algorithms are used.

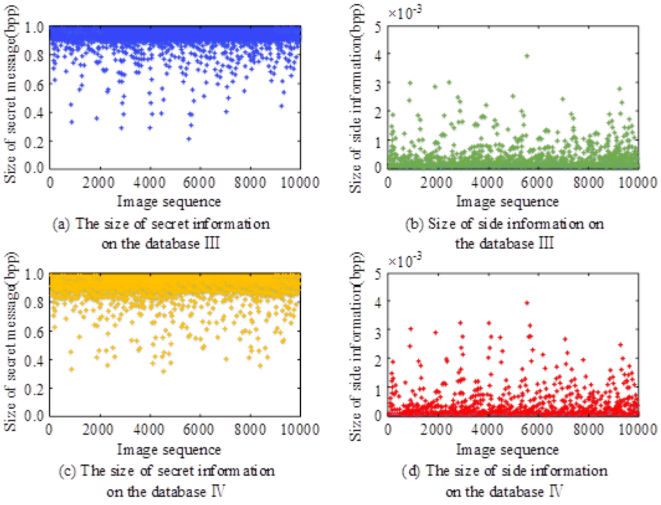


(a) Indicators SSIM and PSNR
(b) Indicators RCE and Entropy
(c) Indicators CIEDE2000 and BRISQUE

Figure 10: Comparison of indicators of different algorithms on datasets

The comparison of SSIM and PSNR is included in Figure 10. When the empty PV is 10, the SSIM and PSNR results of suggested model are the highest. The SSIM value is about 0.96, and the PSNR value is also above 30, indicating that the enhanced image quality is better than other algorithms. Figure 10(b) contains a comparison of RCE and Entropy. The higher the Entropy value, the more evenly distributed the grayscale histogram of the encrypted image is. Although the RCE result of the algorithm in this paper is only between 0.5 and 0.52, it still means that the image information is more abundant and the image distortion is avoided. As the number of empty PV increases, both the RCE and Entropy of the proposed method tend to rise. A comparison of CIEDE2000 and BRISQUE is included in Figure 10(c). A smaller CIEDE2000 value indicates a smaller difference between the original and the processed graph. The CIEDE2000 of the research method has the smallest value, which reaches 2, 3 and 5 respectively when the empty PV is 10, 20 and 30. The highest BRISQUE value is MSRCR algorithm, followed by the suggested model, which indicates that the picture enhancement quality is better.

Finally, to assess the effectiveness of the RDH with MSB-EE, a large number of images from two famous image libraries were selected for experiments. The two picture databases were replaced with Roman numerals III and IV respectively. Figure 11 respectively shows the size of the secret information and sub-information of the algorithm in the two image libraries.



(a) The size of secret information on the database III
(b) Size of side information on the database III
(c) The size of secret information on the database IV
(d) The size of side information on the database IV

Figure 11: The size of information in the database

Figure 11(a) and Figure 11(b) respectively illustrates the distribution of secret information and secondary information on database III after using the proposed algorithm. Figure 11(c) and Figure 11(d) respectively show the distribution of secret information and secondary information on database IV after calculating by the suggested model. The size of the sub-information ranges from 10-3. To assess the safety of the suggested model, the experiment is based on the above indicators. Two indexes, NPCR (the number of pixels change rate) and UACI (the unified average changing intensity), were added to assess the security of encrypted images. The correlation between horizontal direction and vertical direction is compared to judge the intensity of the algorithm encryption.

Table 1: The evaluation results of image indicators for the algorithm in this article

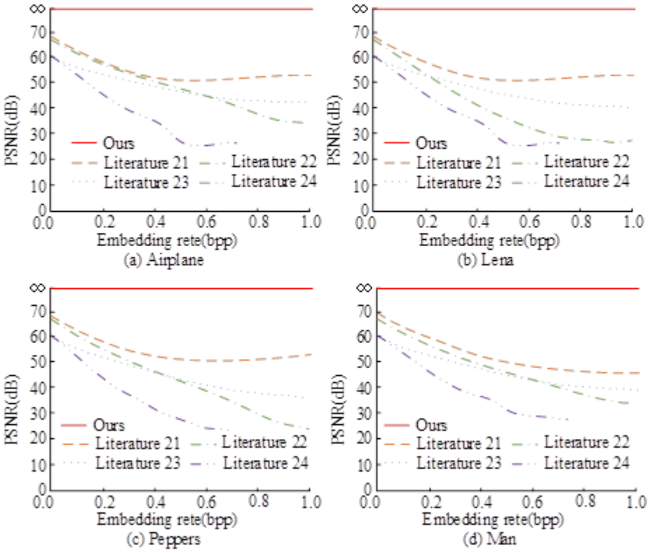
Index	Database III	Database IV
SSIM	0.008	0.007
PSNR (dB)	8.576	7.986
Entropy (bpp)	8.004	8.003
NPCR	99.548(%)	99.339(%)
UACI	33.567(%)	32.952(%)
Horizontal correlation	0.005	0.00
3 Vertical correlation	0.006	0.007

In Table 1, the NPCR value is above 99%, indicating that the safety of the encrypted picture is guaranteed. The correlation between horizontal direction and vertical direction is weak, indicating that the image encrypted by the suggested model is strong. Meanwhile, the research algorithm was compared with other encryption algorithms, and the PSNR values of these five algorithms were calculated respectively in Airplane, Lena, Peppers and Man, and other algorithms included in literature [14], literature [10], literature [4] and literature [19], as shown in Figure 12.

As shown in Figure 12, PSNR values of the four algorithms all decrease when the embedding rate increases. The most obvious decline is in the algorithm proposed in reference [19]. When the embedding rate reaches 0.8, the PSNR has dropped to 20dB. Compared with other algorithms, the suggested model achieves greater embedding rate and security, and less distortion in the image, and the result of image reconstruction is better.

In order to verify the image encryption effect of the research method, this experiment used ideal value deviation analysis to generate the encoding and decoding effects of seven images in BOWS-2. The specific experimental results are shown in Table 2. Seven images from BOWS-2 contain different texture information, with the main body being colored tiles, colored bricks, houses, mountains, lakes, sky, and crowds. The Dobbed values in the experiment are calculated as $D = \sum_{i=0}^{2} 55|H(C_i) - H(C)|/(M \times N)$, $H(C_i)$, and $H(C)$ representing the histograms of the ideal password image and the obtained password image, respectively. The lower the D value, the better the image encryption effect [17]. The table shows that the D value of most images is less than 0.05, indicating the superior image encryption effect of the research method.

In addition, to verify the effectiveness of the indicators NPCR and UACI, in this experiment, the pixel values of coordinates (20,30) were changed from 12 to 13,



(a) Airplane

(b) Lena

(c) Peppers

(d) Man

Figure 12: Performance comparison of different algorithms

Table 2: Ideal value deviation analysis

Image	Number and proportion of error marker blocks	Dobbed values
Colored tiles	2209 (6.7413%)	0.04805
Colored bricks	1418 (4.3274%)	0.04937
House	5467 (16.6840%)	0.04835
Mountains	244 (0.7446%)	0.05141
Lake	299 (0.9125%)	0.04864
Sky	107 (0.3265%)	0.04876
Crowds	948 (2.8931%)	0.04911

Table 3: Sensitivity analysis of NPCR indicators and UACI

Evaluating indicator	P(20,30)	P(155,100)	P(200,300)	P(512,512)
NPCR (%)	99.6223	99.6169	99.6169	99.6140
UACI (%)	33.4851	33.4004	33.4051	33.4312

coordinates (155,100) were changed from 14 to 15, coordinates (200,300) were changed from 169 to 170, and coordinates (512,512) were changed from 65 to 66. Analyze the changes in NPCR and UACI under pixel changes, as shown in Table 3. From the table, it can be seen that with minor changes to the pixel values of a coordinate point in the plaintext image, the NPCR and UACI values calculated using the algorithm in this paper are close to or higher than the calculated values of 99%, indicating that the algorithm in this paper has good differential attack resistance performance.

5 Conclusion

To realize better image enhancement and image encryption in image RDH technology, image enhancement and image hiding algorithms based on image RDH are proposed respectively. In this study, a variety of evaluation indexes are used to evaluate the image quality after the algorithm processing. The suggested model is compared with other commonly used models: In the algorithm to achieve gray level image enhancement, the histogram distribution of gray level distribution of the enhanced image is more uniform after information embedding. The suggested model has the highest MOS score and better image enhancement effect. Among the color image enhancement models, the suggested model has better detail enhancement performance. It not only ensures the relative balance between the original image hue and contrast, brightness, etc., but also increases the details in the picture, and has a better enhancement effect on the picture. When the empty PV is 10, the SSIM obtained by the proposed algorithm reaches about 0.96. PSNR value is also above 30; the RCE results were only between 0.5 and 0.52. The CIEDE2000 of the research algorithm has the minimum value. When the empty PV is 10, 20 and 30, it reaches 2, 3 and 5 respectively. The BRISQUE value is between 15 and 25. When assessing the effectiveness of the suggested cloud transmission model, the NPCR value is above 99%. The correlation between horizontal direction and vertical direction is weak, indicating that the proposed algorithm can encrypt images with high intensity. However, there are still some shortcomings in the research. MSB is used in the algorithm to encrypt images, which limits the capacity of embedded information. Therefore, a way is needed to expand the embedding capacity of secret message in the future.

References

[1] R. Anushiadevi, and R. Amirtharajan, “Reversible data hiding in an encrypted image using the homomorphic property of elliptic curve cryptography,” *Journal of Intelligent & Fuzzy Systems*, vol. 41, no. 5, pp. 5583-5594, 2021.

[2] X. Chen, H. Zhong, and Z. Bao, “A GLCM-feature-based approach for reversible image transformation,” *Computers, Materials and Continua*, vol. 59, no. 1, pp. 239-255, 2019.

[3] Y. Chen, and C. Shiu, “Distributed encrypted image-based reversible data hiding,” *Journal of Internet Technology*, vol. 22, no. 1, pp. 101-107, 2021.

[4] A. Durdu, “Nested two-layer RGB based reversible image steganography method,” *Information Technology and Control*, vol. 50, no. 2, pp. 264-283, 2021.

[5] Y. Fu, P. Kong, H. Yao, Z. Tang, and C. Qin, “Effective reversible data hiding in encrypted image with adaptive encoding strategy,” *Information Sciences*, vol. 494, no. 1, pp. 21-36, 2019.

[6] B. He, Y. Chen, Y. Zhou, Y. Wang, and Y. Chen, “A novel two-dimensional reversible data hiding scheme based on high-efficiency histogram shifting for JPEG images,” *International Journal of Distributed Sensor Networks*, vol. 18, no. 3, pp. 354-362, 2022.

[7] M. S. Hwang, E. F. Cahyadi, Y. C. Chou, C. Y. Yang, “Cryptanalysis of Kumar’s Remote User Authentication Scheme with Smart Cards,” in *14th International Conference on Computational Intelligence and Security (CIS’18)*, Hangzhou, China, pp. 416-420, 2018.

[8] J. A. Kaw, N. A. Loan, S. A. Parah, K. Muhammad, J. A. Sheikh, and G. M. Bhat, “A reversible and secure patient information hiding system for IoT driven e-health,” *International Journal of Information Management*, vol. 45, no. 4, pp. 262-275, 2019.

[9] L. H. Liu and J. Cao, “Analysis of One lightweight authentication and key agreement scheme for internet of drones,” *International Journal of Electronics and Information Engineering*, vol. 13, no. 4, pp. 142-148. 2021.

[10] Z. Liu, and C. Pun, “Reversible image reconstruction for reversible data hiding in encrypted images,” *Signal Processing*, vol. 161, no. 8, pp. 50-62, 2019.

[11] F. Masood, J. Masood, H. Zahir, K. Driss, N. Mehmood, and H. Farooq, “Novel approach to evaluate classification algorithms and feature selection filter algorithms using medical data,” *Journal of Com-*

putational and Cognitive Engineering, vol. 2, no. 1, pp. 57-67, 2023.

[12] Q. Mo, H. Yao, F. Cao, Z. Chang, and C. Qin, "Reversible data hiding in encrypted image based on block classification permutation," *Computers, Materials, and Continuum*, vol. 59, no. 1, pp. 119-133, 2019.

[13] M. M. Nabi and F. Nabi, "Cybersecurity mechanism and user authentication security methods," *International Journal of Electronics and Information Engineering*, vol. 14, no. 1, pp. 1-9, 2022.

[14] M. Navetha, "Survey on secured reversible image data hiding techniques," *Research Journal of Engineering and Technology*, vol. 10, no. 1, pp. 4-10, 2019.

[15] Z. Qian, H. Xu, X. Luo, and X. Zhang, "New framework of reversible data hiding in encrypted jpeg bitstreams," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, no. 2, pp. 351-362, 2019.

[16] L. Qu, H. He, S. Zhang, and F. Chen, "Reversible data hiding in encrypted images based on prediction and adaptive classification scrambling," *Computers, Materials, and Continuum*, vol. 63, no. 3, pp. 2623-2638, 2020.

[17] D. Ravichandran, S. Fathima, V. Balasubramanian, A. Banu, Anushiadevi and R. Amirtharajan, "DNA and chaos based confusion-diffusion for color image security," in *International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN'19)*, Vellore, India, pp. 1-6, 2019.

[18] M. Shah, W. Zhang, H. Hu, X. Dong, and N. Yu, "Prediction error expansion based reversible data hiding in encrypted images with public key cryptosystem," *IET Image Processing*, vol. 13, no. 10, pp. 1705-1713, 2019.

[19] F. H. Shajin, and P. Rajesh, "FPGA realization of a reversible data hiding scheme for 5G MIMO-OFDM system by chaotic key generation-based paillier cryptography along with LDPC and its side channel estimation using machine learning technique," *Journal of Circuits, Systems and Computers*, vol. 31, no. 5, pp. 2250093, 2021.

[20] J. Wang, Z. Sun, and G. Li, "High capacity reversible data hiding algorithm based on parabolic interpolation space," *Tien Tzu Hsueh Pao/Acta Electronica Sinica*, vol. 47, no. 1, pp. 137-144, 2019.

[21] W. Wang, and R. Liu, "A saturation-value histogram equalization model for color image enhancement," *Inverse Problems and Imaging*, vol. 17, no. 4, pp. 746-766, 2023.

[22] X. Wang, C. Chang, and C. Lin, "Reversible data hiding in encrypted images with block-based adaptive MSB encoding," *Information Sciences*, vol. 567, no. 8, pp. 375-394, 2021.

[23] X. Wang, C. Chang, C. Lin, and C. Chang, "Privacy-preserving reversible data hiding based on quad-tree block encoding and integer wavelet transform," *Journal of Visual Communication & Image Representation*, vol. 79, no. 8, pp. 103203, 2021.

[24] M. Wu, T. Chang, H. Chen, Z. Yang, and S. Liu, "Reversible information hiding in images based on histogram shift method," *Sensors and Materials: An International Journal on Sensor Technology*, vol. 34, no. 7, pp. 2555-2566, 2022.

[25] Z. Yin, Y. Xiang, and X. Zhang, "Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding," *IEEE Transactions on Multimedia*, vol. 22, no. 4, pp. 874-884, 2020.

Biography

Zailin Li obtained his BE in Electronic Information Engineering from Southwest normal university in 2005. He obtained a Master's degree in Electronic and Communication Engineering from Nanjing University of Science and Technology in 2012. Presently, he is working as an associate professor in the school of 3D printing, Xinxiang University. His areas of interest are computer communication technology, electronic information, image processing and network security.