Hindawi
Advances in Multimedia
Volume 2022, Article ID 8627056, 11 pages
https://doi.org/10.1155/2022/8627056

Research Article

Reversible Data Hiding of Digital Image Based on Pixel Combination Algorithm

Jingmin Zhang

School of Computer Science and Engineering, Guangxi Normal University, Guilin, Guangxi, 541006, China

Correspondence should be addressed to Jingmin Zhang; zjm0247@stu.gxnu.edu.cn

Received 14 May 2022; Revised 9 June 2022; Accepted 22 June 2022; Published 15 July 2022

Academic Editor: Qiangyi Li

In order to improve the security effect of image information, this paper studies the reversible information hiding of the digital images combined with the pixel combination algorithm and proposes an improved simulated annealing algorithm using the incremental calculation method of statistical functions. Moreover, according to the gray gradient information contained in the image, this paper proposes an automatic threshold determination algorithm suitable for the unimodal gray distribution images and uses this algorithm to complete the threshold determination and binary segmentation of all images. In addition, this paper optimizes the model by transforming the isolated pores inside the model and removing the isolated matrix area. Through comparative experiments, it can be seen that the reversible information hiding method for digital images based on the pixel combination algorithm proposed in this paper has a good image information confidentiality effect.

1. Introduction

The embedding process of reversible information hiding based on the digital images can be understood as using a certain processing method to transform the pixel values to generate a redundant space and then embedding the secret information into the obtained redundant space [1]. The size of the redundant space directly affects the hidden capacity of the carrier image. For the embedding algorithm, if there is no certain reversible rule that can be followed in the extraction process, the carrier image cannot be recovered completely lossless while extracting the secret information [2]. From a theoretical point of view, the larger the redundant space, the larger the length of the secret information that can be hidden, the smaller the pixel modification of the carrier image, and the smaller is the distortion of the original carrier image. Therefore, the reversible information hiding algorithms are based on the two aspects of hiding capacity and image quality as the starting point to find an algorithm that can obtain as much redundant space as possible, modify the pixels of the carrier image as little as possible, and minimize the computational complexity [3].

Encryption technology based on cryptography is a widely used information security method [4]. It converts multimedia data such as images, videos, and audios from plaintext to chaotic ciphertext, thereby realizing the protection of multimedia content. Encryption technology protects the multimedia data to a certain extent but it also has the following limitations: first, the ciphertext is easy to attract the attention of attackers and the security of the decrypted multimedia data will not be guaranteed [5]; second, the encryption technology cannot realize copyright tracking and content integrity authentication because the integrity authentication in cryptography is achieved through digital signatures [6], rather than directly embeddeding them in multimedia data. In addition, in application scenarios such as social media, the practicability of encryption technology is not strong because the multimedia data shared by people on social platforms is generally identifiable plaintext, not ciphertext. In order to protect the copyright of multimedia works and the integrity of their contents, information hiding technology has developed rapidly. Information hiding technology is a technology that embeds secret information into multimedia data such as images, audios, videos, and texts without being noticed by people [7]. Due to

the redundancy of the multimedia data itself and the limitations of human vision and hearing, the multimedia data before and after information embedding is not much different, so its use value and sensory effect are not affected. The embedded information can have nothing to do with the multimedia carrier itself. At this time, the information hiding technology realizes the secret communication function [8], focusing on imperceptibility. If the embedded information is related to the multimedia carrier itself (such as the copyright information of the multimedia carrier), the information hiding technology realizes functions such as copyright authentication and integrity authentication [9], focusing on robustness, that is, in the embedded information. The embedded information can still be detected after the multimedia carrier undergoes unintentional or malicious operations such as compression, rotation, and trimming. Whether it is for secret communication or copyright protection, the embedding of the secret information changes the original multimedia data more or less, resulting in a certain degree of distortion. Although this kind of distortion is not easy to be noticed by people, in some special application scenarios, such as medical images, military image, and legal documents, even a small distortion will bring serious consequences [10]. In addition, with the advancement of technology, people have higher and higher requirements for the definition of digital images, audio, video, and other multimedia works, and the distortion caused by information hiding will become more and more easily detected. Therefore, in order to restore the original multimedia carrier after information extraction, researchers propose reversible data hiding (RDH). Reversible information hiding technology is a technology in which the secret information is embedded in the original carrier in a reversible manner, so that after the information is extracted, the original carrier can be recovered without damage [11]. Different from the traditional information hiding technology, the RDH technology requires that the embedded secret information can be extracted losslessly, the original carrier can be restored losslessly [12], and the quality of the embedded information carrier is higher. In recent years, the rapid development of cloud computing has provided convenience for the storage and processing of massive multimedia data. Individual users can store and share a large number of files in the cloud, and enterprise users can use the cloud to process data to save costs. However, data stored in the cloud is also at risk of being exposed and tampered with. Storing digital images in clear text in the cloud has certain risks. In order to protect the privacy for individual users and for business users to protect the business secrets, the encrypted version of the digital image may be uploaded to the cloud server [13]; in order to facilitate the management and retrieval of encrypted images, cloud service managers embed relevant information (such as copyright and abstract) so that RDH technology is facing new challenges; because in traditional RDH technology, the carrier is usually plain text image. However, after encryption, the plaintext image becomes a messy ciphertext, and the statistical characteristics of the original plaintext image and the correlation between the adjacent pixels are lost, and the traditional RDH technology is no longer applicable. In this context, it is of great significance to study the reversible information hiding technology of encrypted images [14]. Reversible data hiding in encrypted image (RDH-EI) technology is a technology that embeds secret information in encrypted images in a reversible way, and after the information is extracted losslessly, the original image can be restored losslessly [15], which is the combination and development of reversible information hiding technology and encryption technology. Based on the original intention of privacy protection, the RDH-EI algorithm applied to cloud storage scenarios should provide users with a simple and secure image encryption method on the user side to protect user privacy; in order to facilitate the management of ciphertext images by cloud service providers, the RDH-EI algorithm should be provided with large hidden capacity; at the receiving end, high-quality decrypted images and restored original images that are completely consistent with the original images are reasonable requirements that the RDH-EI algorithm should meet [16]. Most of the existing encrypted image reversible information hiding algorithms are based on the symmetric encryption domain, use stream cipher to encrypt the original image bitwise XOR, and use the spatial correlation of the image to reconstruct the original image. However, we also found that the RDH-EI algorithm based on the symmetric encryption domain has the following problems: (1) the ciphertext image generated by the existing stream cipher encryption has the risk of information leakage, (2) the quality of the decrypted image is not high, and (3) the information embedding rate is relatively low [17].

Taking the hidden position as the starting point, reversible information hiding can be divided into spatial domain and transform domain information hiding. Based on the image hiding in the spatial domain, the purpose of hiding the secret information is achieved by modifying the gray value of image pixels. Because human vision is least sensitive to the least significant bits of an image pixel, the secret information is typically embedded in the spatial domain by modifying the least significant bits of a pixel. Based on the image hiding in the transform domain, the purpose of hiding the information is achieved by modifying the coefficients in the transform domain, such as Fourier coefficients, discrete cosine coefficients, and wavelet coefficients [18]. Generally speaking, the reversible algorithm based on the transform domain has high security but the algorithm complexity is relatively high. Starting from the type of carrier data, reversible information hiding techniques can be divided into image-based, video-based, audio-based, or document-based. Image-based reversible information hiding is the most discussed which utilizes the redundant data information of the images and the sensitive characteristics of the human visual system for information hiding [19]. The realization method of the video-based reversible algorithm is not much different from that of the image but it has higher requirements on the real-time performance of the algorithm. The audio-based reversible algorithm mainly uses the data redundancy of audio files and the sensitive characteristics of the human auditory system to hide the secret information. Document-based reversible

algorithm uses its words, lines, or formats to complete the concealment of secret information.

This paper combines the pixel combination algorithm to carry out the research on the reversible information hiding of the digital images to improve the encryption effect of digital images and reduce the information risk in the information age.

2. Pixel Binning Algorithm

2.1. Simulated Annealing Algorithm (SAA). The annealing process of solids belongs to the research field of statistical physics and thermodynamics. According to the existing research results, it can be known that when the temperature of the system is cooled to T, the probability P of particles in the state i inside the equilibrium system is satisfied and the Gibbs regular distribution is satisfied:

$$P_i = \frac{\exp(-E_i/kT)}{\sum_i \exp(-E_i/kT)}. \tag{1}$$

In the formula, E_i is the energy of the particle in the i state, k is the Boltzmann constant, and T is the absolute temperature.

The algorithm uses the random number generation algorithm to generate random numbers in the interval (0,1). If $P > 1$, the change is an important change; otherwise, it is an unimportant change.

$$P_{ij} = \exp\left(-\frac{\Delta E}{kT}\right). \tag{2}$$

In the formula, AE is the difference in energy when the system is in states j and i, respectively, and $\Delta E = E_j - E_i$.

Various types of statistical functions must be considered as much as possible, so that the pore structure features contained in the reference image can be fully characterized. The greater the amount of computation required, the greater the effect on the execution efficiency of the algorithm. The definitions of the three are as follows:

$$\varphi = \langle I(x) \rangle, \tag{3}$$

$$S\langle r \rangle = \langle I(x) I(x+r) \rangle, \tag{4}$$

$$L\langle r \rangle = \langle \prod_{i=s}^{s+r} I(i) \rangle. \tag{5}$$

In the formula, <> represents the average of its internal calculated values, x is the attribute value of the pixel at the x position inside the image, the pore is 1, and the matrix is 0.

In order to correspond to the energy in the solid annealing process, the "energy" of the image system to be reconstructed is taken as the weighed sum of the squares of the differences of different types of statistical values between itself and the reference image and is defined as follows:

$$E = \sum_{r=o}^{R} \alpha \left[S(r) - S_0(r)\right]^2 + \beta \left[L(r) - L_0(r)\right]^2. \tag{6}$$

In the formula, α and β are the weight values corresponding to different types of statistical functions, respectively, and $S(r)$ and $L(r)$ are, respectively, the values of the different types of statistical functions of the image system to be reconstructed. $S_o(r)$ and $L_o(r)$ are the different types of statistical function values of the reference image, respectively, and R is the maximum statistical distance that needs to be calculated between the two pixels.

Analogous to the annealing process of the previous solid, the acceptance probability of the new system is calculated according to the following formula:

$$P = \begin{cases} 1, & \Delta E \le 0, \\ \exp\left(-\dfrac{\Delta E}{T}\right), & \Delta E > 0. \end{cases} \tag{7}$$

In the formula, E_i is the difference between the energy changes before and after the disturbance of the reconstructed system.$\Delta E = E_{\text{new}} - E_{\text{ini}}$ is the temperature used to simulate the solid annealing process, and a larger value is set in the initial state.

Based on the metropolis criteria, the acceptance criteria for rebuilding the system updates are

$$P \ge \text{rand}(0, 1). \tag{8}$$

The conventional simulated annealing algorithm is shown in Figure 1.

That is, after the pixel positions are exchanged, only incremental calculations need to be performed in a specific direction centered on the exchanged pixels.

$$\Delta C = C_{\text{new}} - C_{\text{ini}}. \tag{9}$$

From the definition of the two-point probability function given by formula (4), it can be seen that the contribution value of the matrix pixel (represented by 0 in the reconstructed image matrix) to the statistical function is zero. The relationship is expressed as follows:

$$\begin{aligned} C_{\text{total}} &= 2 \times C_{\text{ind}}, \\ \Delta C &= C_{\text{new}} - C_{\text{ini}} \\ &= 2 \times C_{\text{new}}^{\text{ind}} - 2 \times C_{\text{ini}}^{\text{ind}}. \end{aligned} \tag{10}$$

In the formula, $C_{\text{ini}}^{\text{ind}}$ and $C_{\text{new}}^{\text{ind}}$, respectively, correspond to the values of the pore phase pixel points at the selected positions before and after the exchange of pixel positions.

The sum of the relative linear path function contributions of all pores in the system can be expressed as follows:

$$C_{\text{sum}} = \begin{cases} 2 \times (N - r), & r \le N, \\ 0, & r > N. \end{cases} \tag{11}$$

The matrix pixels are denoted as N_{0-u}, N_{0-d}, N_{0-l}, and N_{0-r} , respectively, and the pore pixels are denoted as N_{1-u}, N_{1-d}, N_{1-l}, and N_{1-r}, respectively. Finally, the total number of consecutive adjacent pores centered on the selected pores and matrix pixels is calculated according to the row and column directions, respectively.

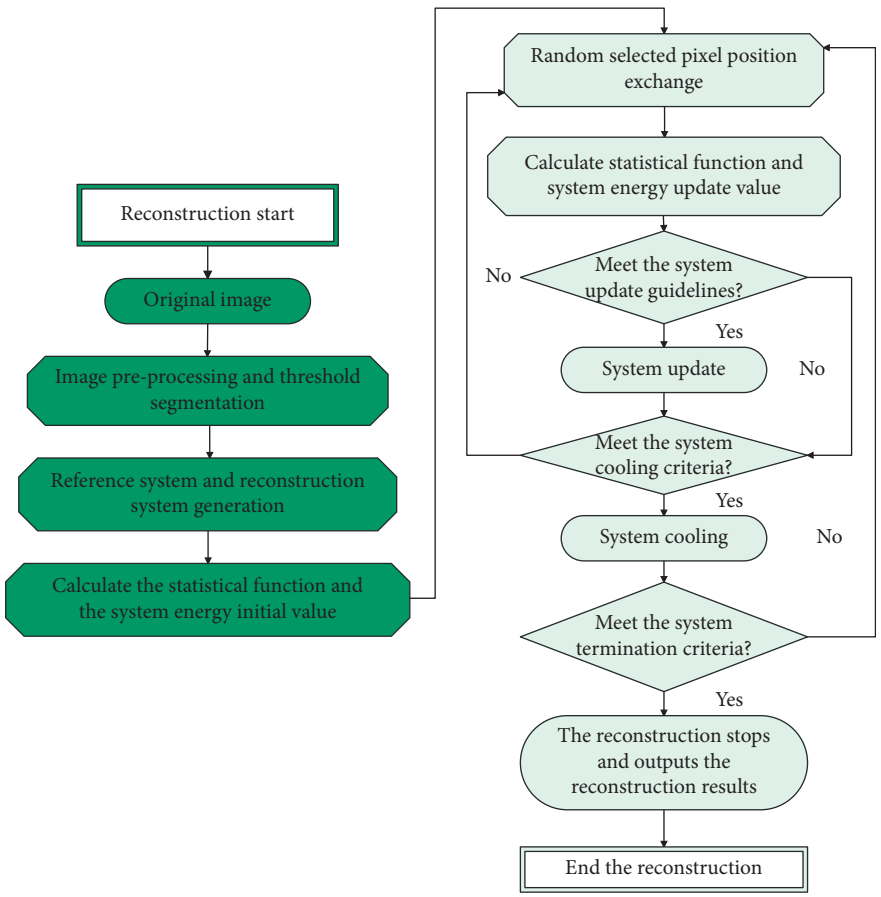


Figure 1: Flowchart of the conventional simulated annealing algorithm.

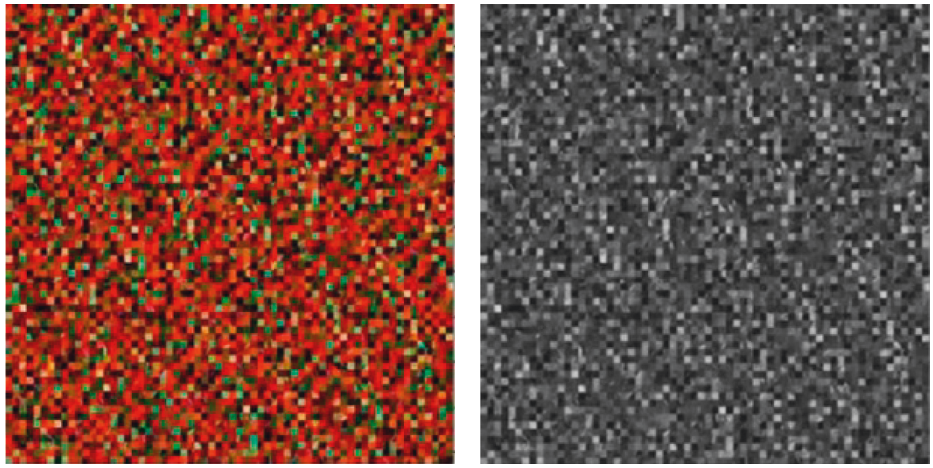
For the initial system before pixel position exchange, the consecutive adjacent pore phases in the row and column directions can be calculated by the following equations, respectively:

$$N_{\text{row}}^{\text{ini}} = \begin{cases} N_{1-l} + N_{1-r} + 1, & \text{Pore}, \\ N_{o-l}, & \text{Matrix}, \\ N_{0-r}, & \text{Matrix}, \end{cases}$$
$$N_{\text{cohmn}}^{\text{ini}} = \begin{cases} N_{1-u} + N_{1-d} + 1, & \text{Pore}, \\ N_{o-u}, & \text{Matrix}, \\ N_{0-d}, & \text{Matrix}. \end{cases} \tag{12}$$

Moreover, for the updated system after pixel position exchange, the initial matrix phase is updated to the pore phase and the pore connectivity may be enhanced. Therefore, it is necessary to modify formula (13) at this time to calculate the total number of continuous adjacent pore phases in the row and column directions of the update system, as follows:

$$N_{row}^{new} = \begin{cases} N_{1-l}, Matrix \\ N_{1-l}, Pore \\ N_{0-l} + N_{0-r} + 1, Pore \end{cases} \quad N_{cohmn}^{new} = \begin{cases} N_{1-u}, Matrix \\ N_{1-d}, Matrix \\ N_{0-u} + N_{0-d} + 1, Pore \end{cases}, \tag{13}$$

$$\begin{aligned} \Delta C &= C_{new} - C_{ini} \\ &= 2 \times \left(N_{row}^{new} - r\right) + 2 \times \left(N_{column}^{new} - r\right) - 2 \times \left(N_{row}^{ini} - r\right) - 2 \times \left(N_{column}^{ini} - r\right) \end{aligned} \tag{14}$$



(a) (b)

Figure 2: Grayscalecolor image. (a) Color image and (b) grayscale image.

Formulas (13) and (14) should be replaced by formulas (18) and (19), respectively.

$$N_{row}^{ini} = \begin{cases} 0, Pore \\ N_{o-l}, Matrix \\ N_{0-r}, Matrix \end{cases} N_{cohmn}^{ini} = \begin{cases} N_{1-u} + N_{1-d} + 1, Pore \\ N_{o-u}, Matrix \\ N_{0-d}, Matrix \end{cases}, \tag{15}$$

$$N_{row}^{new} = \begin{cases} N_{0-l} + (Col_1 - Col_0), Matrix \\ N_{0-l} - (Col_1 - Col_0), Pore \\ 0, Pore \end{cases} N_{cohmn}^{new} = \begin{cases} N_{1-u}, Matrix \\ N_{1-d}, Matrix \\ N_{0-u} + N_{0-d} + 1, Pore \end{cases}, \tag{16}$$

$$N_{row}^{ini} = \begin{cases} N_{1-l} + N_{1-r} + 1, Matrix \\ N_{o-l}, Matrix \\ N_{0-r}, Pore \end{cases} N_{cohmn}^{ini} = \begin{cases} 0, Pore \\ N_{o-u}, Matrix, \\ N_{0-d}, Matrix \end{cases} \tag{17}$$

$$N_{row}^{new} = \begin{cases} N_{1-l}, Matrix \\ N_{1-l}, Pore \\ N_{0-l} + N_{0-r} + 1, Pore \end{cases} N_{cohmn}^{new} = \begin{cases} N_{0-u} + (Row_1 - Row_0), Matrix \\ N_{0-d} + (Row_1 - Row_0), Matrix. \\ 0, Pore \end{cases} \tag{18}$$

In the formula, Row_0, Col_0 and Row_1, Col_1 are the row and the column numbers of the selected matrix phase and pore phase, respectively.

2.2. Image Preprocessing. Image grayscale is mainly used for color images. Color images contain more information. In order to improve the efficiency of the subsequent image processing, it is necessary to convert them into grayscale images for processing.

The grayscale of the color image is mainly realized by weighing the average processing of the three color components in the color image and finally converting them into a gray value. In order to make the grayscaled image more in line with the visual effect of the human eye, formula (20) is usually used to calculate the converted grayscale value of each pixel in the color image.

$$Gray = 0.399 \times R + 0.587 \times G + 0.114 \times B. \tag{19}$$

In the formula, Gray is the converted grayscale value and R, G, and B are the red, green, and blue components of a pixel, respectively.

As an example, Figure 2 shows the result of a color image grayscaled using the above method. In fact, the above method cannot completely retain all the detailed information in the color image and the grayscale effect of the above method is acceptable if the requirements are not strict.

Image enhancement mainly improves the image quality through the grayscale mapping of images. Grayscale

mapping is to directly convert the grayscale value of each pixel in the original image into another new grayscale value according to a certain mapping rule, thereby improving the quality of the image. Specifically, it can be explained by the following formula:

$$g_t = E(g_s). \tag{20}$$

In the formula, g_s and g_t are the grayscale values before and after the pixel point mapping at a certain position of the image and E is the grayscale mapping function.

It is suggested that the brightness adjustment of the image is only suitable for the case where the gray value of the image after the brightness adjustment does not exceed its display range; that is, the gray range of the original image itself is a subset of the range that can be displayed.

$$\begin{aligned} g_t &= E(g_s) = g_s \pm a, \\ g_t &= \begin{cases} 0, & g_t < 0, \\ 255, & g_t > 255. \end{cases} \end{aligned} \tag{21}$$

In the formula, a is a constant. The FIB/SEM reference image used by the improved simulated annealing algorithm in the previous section is taken as an example, and the brightness is adjusted. The result is shown in Figure 3. It can be seen that the brightness adjustment is just a shift of the grayscale histogram of the image to the left or right, without any change in the shape of the histogram. Therefore, the brightness adjustment of the image only improves the display effect of the image visually and has no effect on the subsequent image processing, so all the images used in this study are not adjusted for brightness.

The mean filter operates on the image based on template convolution. It selects an $n * n$ template (where $n = 2k + 1$ and k is a positive integer) to move it over the entire area and uses formula (23) to calculate the average value of the neighborhood of a certain pixel. It is used as the gray value of the pixel.

$$g(x, y) = \frac{1}{n^2} \sum_{(s,t) \in N(x,y)} f(s, t). \tag{22}$$

In the formula, $N(x, y)$ corresponds to the $n \times n$ neighborhood of the image $f(x, y)$ at the position (x, y).

Different coefficients can be selected according to the distance from the center point, and the weighted average of the neighborhood is used to determine the pixel value of the center point. The specific calculation form is as follows:

$$g(x, y) = \frac{\sum_{(s,t) \in N(x,y)} w(s, t) f(s, t)}{\sum_{(s,t) \in N(x,y)} w(s, t)}. \tag{23}$$

In the formula, $w(s, t)$ is the weight of pixels at different distances from the center point.

The specific calculation form can be expressed as

$$g_{\text{median}}(x, y) = \underset{(s,t) \in N(x,y)}{\text{median}} [f(s, t)]. \tag{24}$$

In essence, the median filtering is a special case of percentage filtering; that is, the gray value at the 50% position of each pixel sequence in the template is selected as the output result. By changing the gray values at different positions of the selection sequence, such as the 0% position or the 100% position, we will get the minimum and maximum filtering, respectively. The specific form is as follows:

$$\begin{aligned} g_{\min}(x, y) &= \min_{(s,t) \in N(x,y)} [f(s, t)], \\ g_{\max}(x, y) &= \max_{(s,t) \in N(x,y)} [f(s, t)]. \end{aligned} \tag{25}$$

According to the above processing results of mean filter and median filter, take the average value of the minimum filter and maximum filter results as the result output of the new filter, that is, midpoint filter. The specific form is as follows:

$$\begin{aligned} g_{\text{mid}} &= \frac{1}{2} \left\{ \min_{(s,t) \in N(x,y)} [f(s, t)] + \max_{(s,t) \in N(x,y)} [f(s, t)] \right\} \\ &= \frac{1}{2} [g_{\min}(x, y) + g_{\max}(x, y)]. \end{aligned} \tag{26}$$

Midpoint filtering combines the advantages of two image denoising methods, average filtering and sorting filtering. The specific processing results are shown in Figure 4.

2.3. Thresholding Image Segmentation. The basic principle of thresholding image segmentation is very simple. That is, by comparing the gray value of each pixel in the image with the selected threshold, the category of the pixel is determined according to the result of the comparison into target (foreground) or background.

$$g(x, y) = \begin{cases} 1, f(x, y) > T, \\ 0, f(x, y) \le T. \end{cases} \tag{27}$$

In the formula, T is the selected image segmentation threshold, $f(x, y)$ and $g(x, y)$ are the gray values of the pixels at the position (x, y) before and after segmentation, respectively, and 1 and 0 are the labels assigned to each category of the segmented image.

The optimal threshold for image segmentation can generally be expressed in the following form:

$$T = T[x, y, f(x, y), p(x, y)]. \tag{28}$$

In this paper, we consider an m-level grayscale image $f(x, y)$ with a size of $M \times N$ (where, for an 8 bit grayscale image, $m = 2^8$), $G = \{0, 1, \ldots, (m - 1)\}$ is the gray value set of $f(x, y)$ and N_i is the number of pixels with gray value i in $f(x, y)$. Based on the above description, the distribution probability of pixels with gray value i in the gray image $f(x, y)$ can be expressed as follows:

$$p_t = \frac{N_i}{M \times N}. \tag{29}$$

Now, we assume that a given threshold T is selected and the pixels in $f(x, y)$ are divided into two categories by formula (28): target C and background C. Among them, the gray value interval included in C is [0, T] and the gray value interval included in C is [T. +1, m − 1]. The total distribution

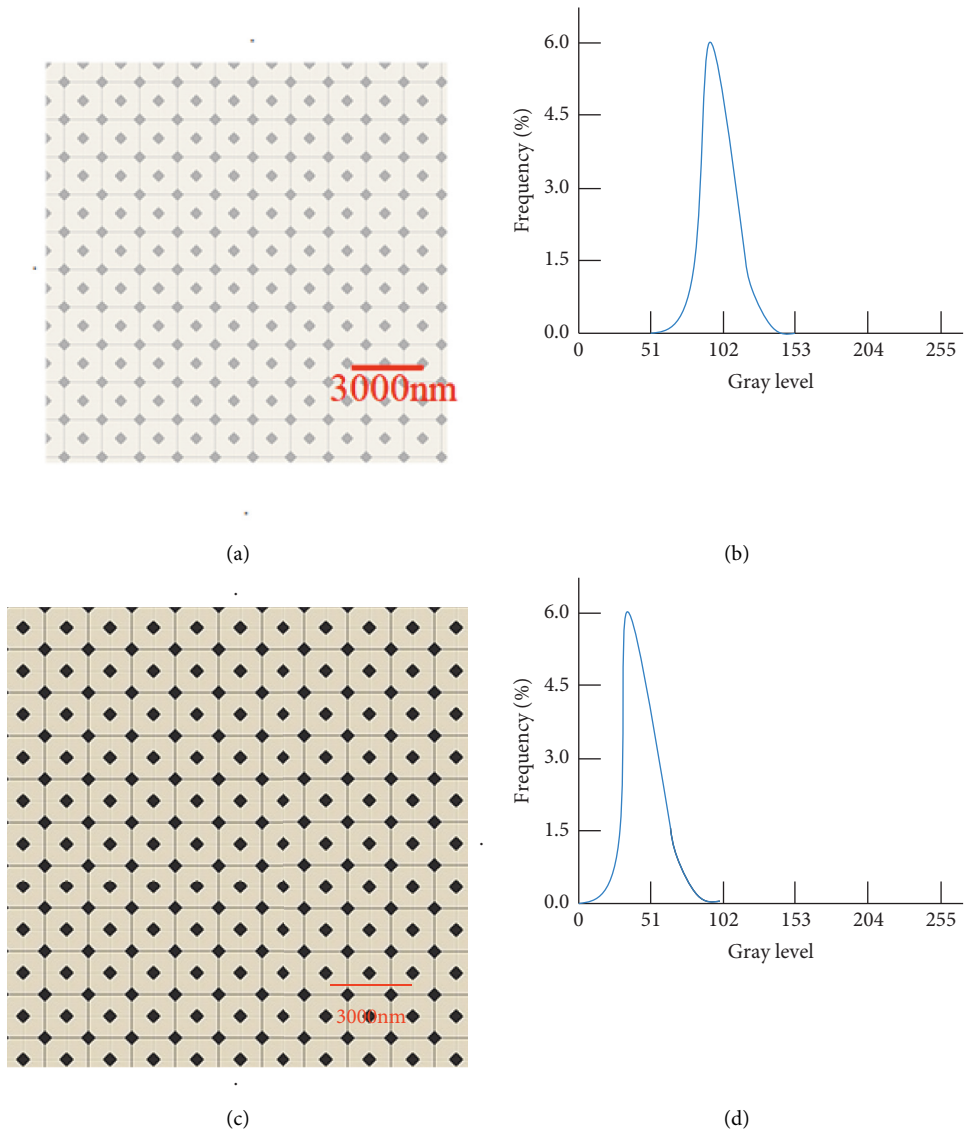


FIGURE 3: Imagebrightness adjustment. (a) Original image, (b) original grayscale histogram, (c) image after the brightness adjustment, and (d) the brightness-adjusted grayscale histogram.

probabilities of the pixels included in the background C are as follows:

$$\omega_0 = \sum_{i=0}^{T} p_i,$$
$$\omega_1 = \sum_{i=T+1}^{m-1} p_i. \tag{30}$$

The average grayscale values of the pixels contained in the target C_0 and the background C_1 are

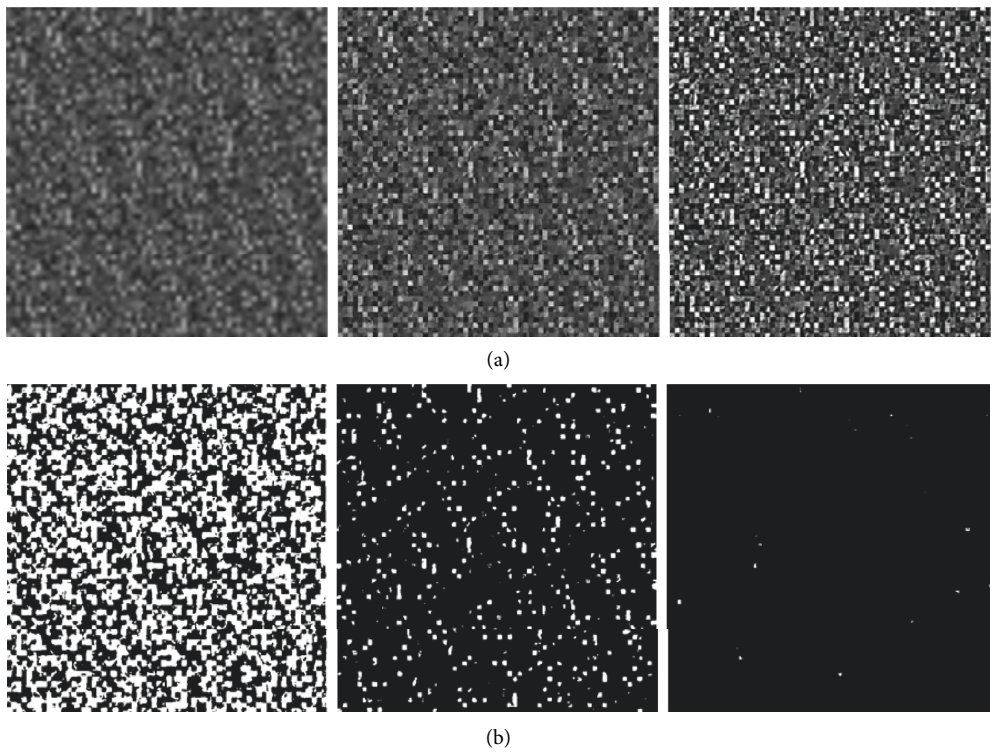
$$\mu_0 = \frac{1}{\omega_0} \sum_{i=0}^{T} i p_i,$$
$$\mu_1 = \frac{1}{\omega_1} \sum_{i=T+1}^{m-1} i p_i. \tag{31}$$

The average gray value of all pixels in the image $f(x, y)$ is

$$\mu = \sum_{i=0}^{m-1} i p_i = \omega_0 \mu_0 + \omega_1 \mu_1. \tag{32}$$

Based on the above-obtained pixel gray mean and its corresponding distribution frequency, we briefly introduce several currently widely used global threshold determination algorithms and give the specific calculation methods of the threshold used.

2.3.1. Huang Algorithm. Huang algorithm mainly determines the optimal threshold by minimizing the fuzzy measure of the image. The specific calculation form is as follows:



(a)

(b)

Figure 4: Comparisonof midpoint filtering results of images under different template sizes. (a) SEM image: from left to right, filter mask sizes are 3×3, 5×5, and 7×7, respectively, and (b) FIB/SEM images: from left to right, the filter mask sizes are 3×3, 5×5, and 7×7, respectively.

$$E(T^*) = \min_{T\in G} E(T),$$

$$E(T) = -\frac{1}{\ln 2}\sum_{i=0}^{m-1}\{\eta(i)\ln[\eta(i)] + [1-\eta(i)]\ln[1-\eta(i)]\}p_i,$$

$$\eta(i) = \begin{cases} \dfrac{C}{C+|i-\mu_0|}, & i \le T, \\ \dfrac{C}{C+|i-\mu_1|}, & i > T. \end{cases} \tag{33}$$

In the formula, C is a constant, which usually selects the difference between the maximum gray value and the minimum gray value of the pixel in the image, that is, $C = i_{\max} - i_{\min}$.

2.3.2. MaxEntropy Algorithm. The MaxEntropy algorithm determines the optimal threshold by maximizing the total amount of information about the target and the background in the image. The specific calculation form is as follows:

$$H(T^*) = \max_{T\in G} H(T)$$

$$H(T) = \ln(\omega_0\omega_1) - \frac{1}{\omega_0}\sum_{i=0}^{T} p_i \ln p_i - \frac{1}{\omega_1}\sum_{i=T+1}^{m-1} p_i \ln p_i. \tag{34}$$

2.3.3. Otsu Algorithm. The Otsu algorithm is also known as the maximum interclass variance algorithm. The specific calculation form of the optimal threshold is as follows:

$$\sigma_B^2(T^*) = \max_{T\in G} \sigma_B^2(T),$$
$$\sigma_B^2(T^*) = \omega_0\omega_1(\mu_0 - \mu_1)^2. \tag{35}$$

2.3.4. Yen Algorithm. The Yen algorithm determines the optimal threshold by maximizing the total correlation between the target and the background in the image. The specific calculation form is as follows:

$$C(T^*) = \max_{T\in G} c(T)$$
$$C(T) = 2\ln(\omega_0\omega_1) - \ln\left(\sum_{i=0}^{T} p_i^2 \sum_{i=T+1}^{m-1} p_i^2\right) \tag{36}$$

2.3.5. Valley-Emphasis Algorithm. The Valley-Emphasis algorithm uses different thresholds to segment the image, so that the corrected interclass variance value reaches the maximum and then determines the optimal threshold. The specific calculation form is as follows:

$$VE(T^*) = \max_{T\in G} VE(T)$$
$$VE(T) = (1 - p_T)\sigma_B^2(T). \tag{37}$$

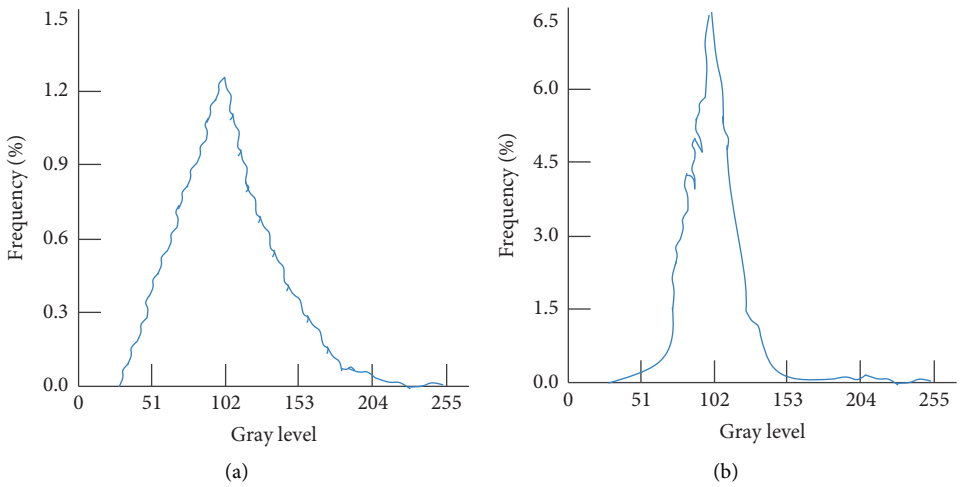


Figure 5: Pixelgray distribution histogram. (a) SEM image and (b) FIB/SEM image.

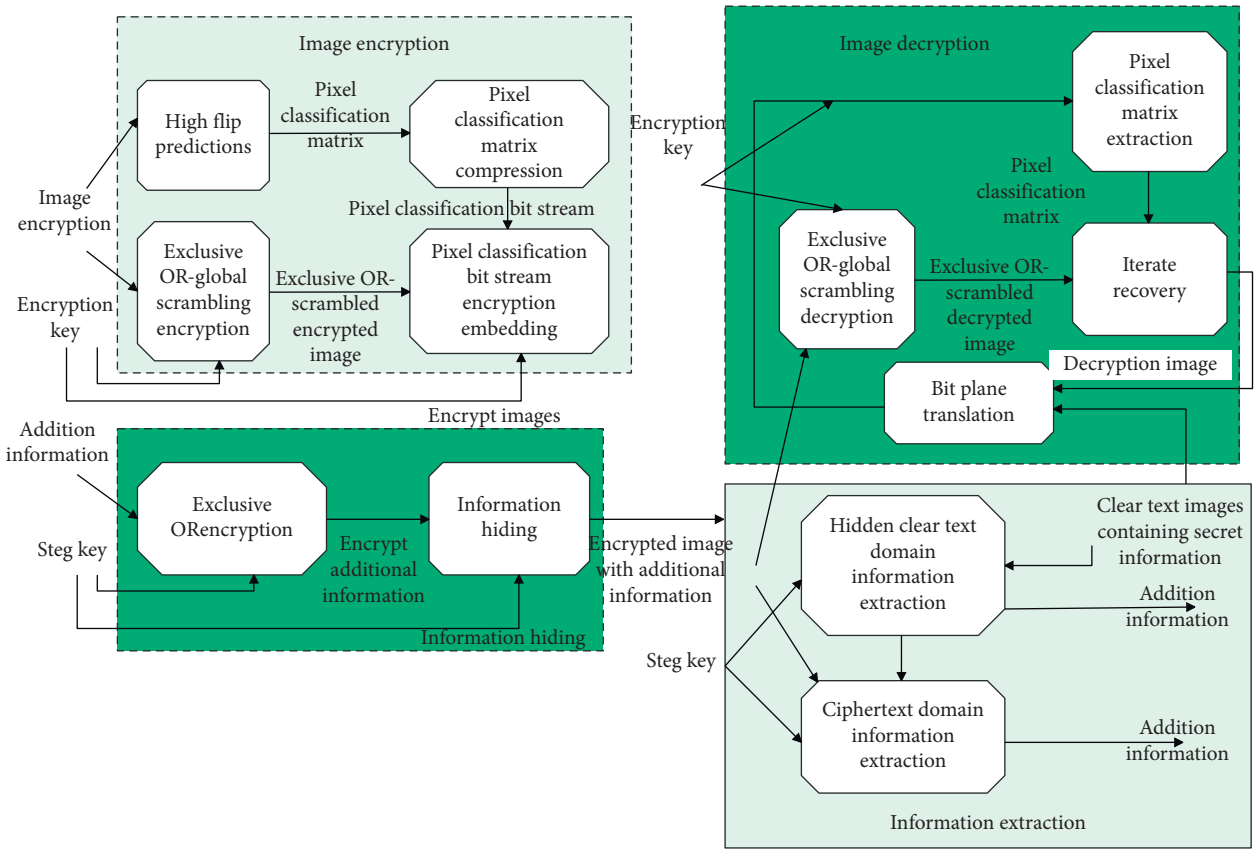


Figure 6: Astructure block diagram of image reversible information hiding algorithm.

Figure 5 shows its corresponding gray distribution histogram.

3. Reversible Information Hiding in Digital Images

This paper proposes a reversible information hiding algorithm for the encrypted images based on the pixel combination algorithm. It includes four parts and they are image encryption, information hiding, image decryption, and information extraction. The algorithm framework is shown in Figure 6.

In order to verify the performance of the algorithm in this paper, the algorithm in this paper is compared with the literature [1] and literature [2]. Table 1 presents a comparison of the net embedding rates of the three algorithms. The results are shown in Table 1 and Figure 7.

It can be seen from the comparative experiments that the reversible information hiding method for digital images

Table 1: Effectevaluation of the digital image reversible information hiding method based on the pixel combination algorithm.

	The method of this paper	The method of literature [1]	The method of literature [2]
Lena	0.9797	0.3131	0.6969
Airplane	0.9393	0.3636	0.7272
Camera	0.9797	0.4848	0.6666
Man	0.9595	0.2727	0.6161
Tiffany	0.9797	0.3232	0.6565
Peppers	0.9494	0.2525	0.7272
Lake	0.9191	0.2121	0.6767
Baboon	0.6161	0.1111	0.3232

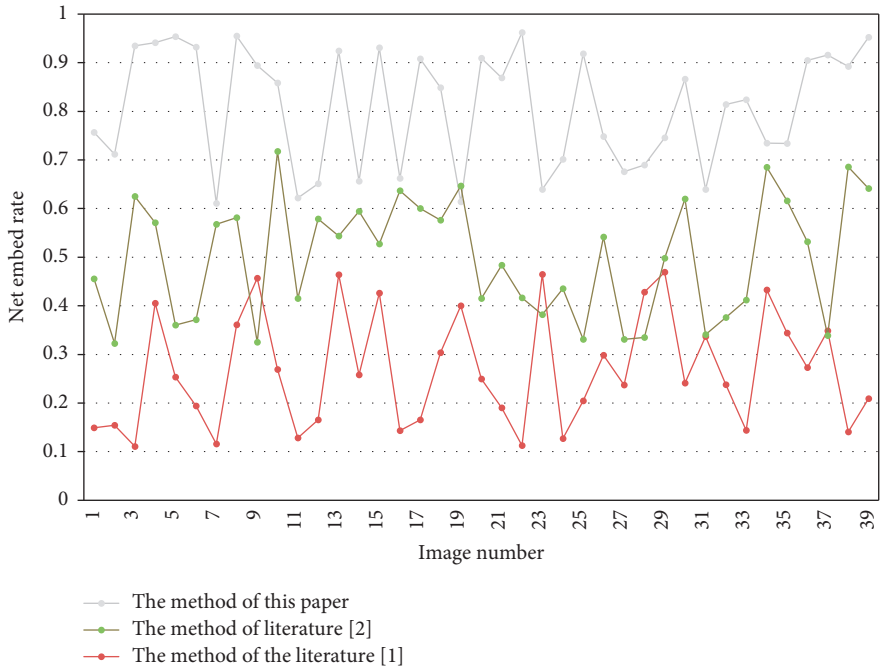


Figure 7: Statisticsof the comparative test data.

based on the pixel combination algorithm proposed in this paper has a good image information confidentiality effect.

4. Conclusion

With the continuous development of reversible digital steganography technology, it has attracted the attention of many researchers. Although the research on reversible digital steganography originated from lossless image authentication, the data embedded in digital images does not necessarily have to be traditional authentication information such as digital signatures. For example, the management and the legal use of military secret maps, the authorized use of military secret images, and the retrieval and labeling of medical image information can all use the reversible digital image technology for data embedding. At the same time, the original carrier data is restored when needed, while the embedded data is extracted. This paper combines the pixel combination algorithm to carry out the research on the reversible information hiding of the digital images. Through comparative experiments, it can be seen that the reversible information hiding method for digital images based on pixel combination algorithm proposed in this paper has a good image information confidentiality effect.

Data Availability

The labeled dataset used to support the findings of this study is available from the corresponding author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

Acknowledgments

This study was sponsored by Guangxi Normal University.

References

[1] J. Anitha Ruth, H. Sirmathi, and A. Meenakshi, "Secure data storage and intrusion detection in the cloud using MANN and dual encryption through various attacks," *IET Information Security*, vol. 13, no. 4, pp. 321–329, 2019.

[2] V. Prabhakaran and A. Kulandasamy, "Integration of recurrent convolutional neural network and optimal encryption scheme for intrusion detection with secure data storage in the cloud," *Computational Intelligence*, vol. 37, no. 1, pp. 344–370, 2021.

[3] L. Deng, D. Li, X. Yao, H. Wang, and H. Wang, "Retracted article: mobile network intrusion detection for IoT system based on transfer learning algorithm," *Cluster Computing*, vol. 22, no. S4, pp. 9889–9904, 2019.

[4] B. Wahyudi, K. Ramli, and H. Murfi, "Implementation and analysis of combined machine learning method for intrusion detection system," *International Journal of Communication Networks and Information Security*, vol. 10, no. 2, pp. 295–304, 2018.

[5] D. Li, Z. Cai, L. Deng, X. Yao, and H. H. Wang, "Information security model of block chain based on intrusion sensing in the IoT environment," *Cluster Computing*, vol. 22, no. S1, pp. 451–468, 2019.

[6] H. Parveen Sultana, N. Shrivastava, D. D. Dominic, N. Nalini, and J. M. Balajee, "Comparison of machine learning algorithms to build optimized network intrusion detection system," *Journal of Computational and Theoretical Nanoscience*, vol. 16, no. 5, pp. 2541–2549, 2019.

[7] V. Pham, E. Seo, and T. M. Chung, "Lightweight convolutional neural network based intrusion detection system," *Journal of Communications*, vol. 15, no. 11, pp. 808–817, 2020.

[8] V. Subbarayalu, B. Surendiran, and P. Arun Raj Kumar, "Hybrid network intrusion detection system for smart environments based on internet of things," *The Computer Journal*, vol. 62, no. 12, pp. 1822–1839, 2019.

[9] B. Molina-Coronado, U. Mori, A. Mendiburu, and J. Miguel-Alonso, "Survey of network intrusion detection methods from the perspective of the knowledge discovery in databases process," *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2451–2479, 2020.

[10] P. Suri, J. Sengupta, and P. Sharma, "Survey of intrusion detection techniques and architectures in cloud computing," *International Journal of High Performance Computing and Networking*, vol. 13, no. 2, p. 184, 2019.

[11] R. Gifty, R. Bharathi, and P. Krishnakumar, "Privacy and security of big data in cyber physical systems using Weibull distribution-based intrusion detection," *Neural Computing & Applications*, vol. 31, no. S1, pp. 23–34, 2019.

[12] G. Stergiopoulos, G. Chronopoulou, E. Bitsikas, N. Tsalis, and D. Gritzalis, "Using side channel TCP features for real-time detection of malware connections," *Journal of Computer Security*, vol. 27, no. 5, pp. 507–520, 2019.

[13] Q. Hu and F. Luo, "Review of secure communication approaches for in-vehicle network," *International Journal of Automotive Technology*, vol. 19, no. 5, pp. 879–894, 2018.

[14] M. Safaldin, M. Otair, and L. Abualigah, "Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 2, pp. 1559–1576, 2021.

[15] A. M. Viswa Bharathy and A. Mahabub Basha, "A multi-class classification MCLP model with particle swarm optimization for network intrusion detection," *Sādhanā*, vol. 42, no. 5, pp. 631–640, 2017.

[16] G. Spathoulas, G. Theodoridis, and G. P. Damiris, "Using homomorphic encryption for privacy-preserving clustering of intrusion detection alerts," *International Journal of Information Security*, vol. 20, no. 3, pp. 347–370, 2021.

[17] C. Young, J. Zambreno, H. Olufowobi, and G. Bloom, "Survey of automotive controller area network intrusion detection systems," *IEEE Design & Test*, vol. 36, no. 6, pp. 48–55, 2019.

[18] M. Z. Liu, Y. H. Xu, Y. J. Wu, and Y. N. Xu, "Research of authenticated encryption security protocol for FlexRay in-vehicle network," *International Journal of Computer Theory and Engineering*, vol. 10, no. 5, pp. 175–179, 2018.

[19] M. Mazhar Rathore, A. Ahmad, A. Paul, and S. Rho, "Exploiting encrypted and tunneled multimedia calls in high-speed big data environment," *Multimedia Tools and Applications*, vol. 77, no. 4, pp. 4959–4984, 2018.