Hindawi
Security and Communication Networks
Volume 2019, Article ID 6572105, 12 pages
https://doi.org/10.1155/2019/6572105

Research Article

Novel Meaningful Image Encryption Based on Block Compressive Sensing

Chen Pan,[1] Guodong Ye,[1] Xiaoling Huang,[1] and Junwei Zhou[2,3]

[1]*Faculty of Mathematics and Computer Science, Guangdong Ocean University, Zhanjiang 524088, China*
[2]*School of Computer Science and Technology, Wuhan University of Technology, Wuhan 430070, China*
[3]*The Pennsylvania State University, University Park, PA 16802, USA*

Correspondence should be addressed to Xiaoling Huang; xyxhuang@hotmail.com

Received 13 September 2019; Revised 31 October 2019; Accepted 9 November 2019; Published 30 November 2019

Guest Editor: Veljko Milutinovic

This paper proposes a new image compression-encryption algorithm based on a meaningful image encryption framework. In block compressed sensing, the plain image is divided into blocks, and subsequently, each block is rendered sparse. The zigzag scrambling method is used to scramble pixel positions in all the blocks, and subsequently, dimension reduction is undertaken via compressive sensing. To ensure the robustness and security of our algorithm and the convenience of subsequent embedding operations, each block is merged, quantized, and disturbed again to obtain the secret image. In particular, landscape paintings have a characteristic hazy beauty, and secret images can be camouflaged in them to some extent. For this reason, in this paper, a landscape painting is selected as the carrier image. After a 2-level discrete wavelet transform (DWT) of the carrier image, the low-frequency and high-frequency coefficients obtained are further subjected to a discrete cosine transform (DCT). The DCT is simultaneously applied to the secret image as well to split it. Next, it is embedded into the DCT coefficients of the low-frequency and high-frequency components, respectively. Finally, the encrypted image is obtained. The experimental results show that, under the same compression ratio, the proposed image compression-encryption algorithm has better reconstruction effect, stronger security and imperceptibility, lower computational complexity, shorter time consumption, and lesser storage space requirements than the existing ones.

1. Introduction

In the background of rapid development of information networks, emergence of artificial intelligence, big data, 5G cellular communication, and the Internet of Things, technology is imperceptibly changing the way of life for most people, bringing convenience into their lives, while also increasing the exposure of private and personal data. Digital images occupy the major share in information transmission carriers, because of the intuitive nature and large quantity of information they carry. Due to low operation costs, the copying, cropping, and forwarding of images make important information available on unsafe public channels, which seriously infringes on users' data privacy. Therefore, the efficient protection of digital images on unsafe public channels has become a popular field of research for experts and scholars, and a series of image encryption algorithms have been proposed.

The original image encryption algorithms were based on the "confusion-diffusion" encryption framework proposed by Fridrich. With the continuous development of hardware technology and cryptanalysis technology, most of the current image encryption algorithms are designed by integrating various technologies, such as DNA coding [1], optical technology [2], cellular automata [3, 4], and asymmetric cryptosystems [5], which guarantees the security of image transmission and storage on some resource sharing platforms. However, with the rapid development of communication networks, the increasing demand for real-time transmission, and increasing image sizes, ensuring the

security and real-time performance of the transmission of massive images in bandwidth-constrained networks has become an urgent problem that needs to be solved.

This provides the scope for image compression to be used, due to the characteristics of the human visual system (HVS) and the high redundancy of the sampled and quantized digital images. The compressed image has wider applicability and is more efficient in storing and transmitting in a bandwidth-constrained network, which greatly alleviates network congestion. In 2006, the introduction of compressive sensing brought a new perspective on image compression technology [6, 7]. Compressive sensing theory points out that, under the premise that the sampling rate is far less than Nyquist's, the signal can be sampled and compressed simultaneously because of the its sparsity in a transform domain. The process of reconstructing the signal is an optimization problem, and the original signal is reconstructed with high probability from little observations by solving this optimization problem. Following this principle, many image encryption algorithms were developed based on compressive sensing [8–18]. Zhou et al. [8] proposed combining high-dimensional chaotic systems to compress and encrypt the image with 2D compressed sensing and then to reencrypt the image by the cyclic shift operation. This algorithm has higher security, but the original image reconstruction effect is poor. Similarly, Xu et al. [9] designed a new 2D-SLIM chaotic map, which uses compressive sensing to compress and encrypt the image along both row and column directions, which is 2D compressed encryption, and then reencrypt along row and column directions. The proposed algorithm has low complexity and high security, but the robustness of the algorithm is not great, and the reconstruction effect of the original image is poor. Chai et al. [10] used the memristive chaotic system, elementary cellular automata (ECA), and compressive sensing (CS) to encrypt and compress images. This can resist plaintext attacks with high robustness and security. Compressive sensing is suitable not only for ordinary digital images but also for compression and encryption of medical images. Reference [11] applies compressive sensing to medical images, achieving compression and confidentiality for them. Gong et al. [12] used compressive sensing to compress and encrypt images using bitwise XOR operations and pixel scrambling. Compressive sensing greatly improves the efficiency of image compression and encryption, but when large-scale images are observed and reconstructed, the storage space required is large, the computational complexity of the algorithm is high, and the reconstruction time is long. Therefore, Lu Gan proposed "block compressed sensing" [15], in which an image is divided into uniform nonoverlapping blocks. By observing and reconstructing these blocks separately, the computational complexity is greatly reduced, as is the required storage space. Simultaneously, the time taken for image reconstruction is shortened. Reference [16] divides an image into four equal-sized blocks, uses two different measurement matrices to measure and encrypt each of the images, then employs random pixel scrambling, and finally merges them into a single encrypted image. The security of the resulting algorithm is higher, but the block effect of the cipher image after segmentation is more obvious. In [17], block compression sampling is applied to resource-constrained wireless visual sensor networks (WVSNs), which makes the image more robust when transmitted over unreliable channels. In [18], after the plain image is divided into blocks, the discrete cosine transform is applied to it, and the obtained low frequency, high frequency, and intermediate frequency are observed by different measurement matrices. Following that, forward diffusion, disturbance, and backward diffusion operations are applied to it to generate the final encrypted image. The algorithm is highly efficient and requires a short reconstruction time and low storage space.

Reference [19] proposes a new image encryption framework: encrypting images into visually meaningful cipher images. In fact, it combines image encryption with information hiding technology and hides the original image in a carrier image after encryption, so as to achieve a visually meaningful effect. This image encryption method camouflages the existence of the original image, thus reducing the possibility of being attacked to a certain extent. As of now, many meaningful image encryption algorithms have been proposed [20–33]. Inspired by [19], the work of [20] embeds multiple color images into nonessential areas of the carrier image to achieve visually meaningful effects. The algorithm has a large embedding capacity and high robustness. Reference [21] encrypts the original image using zigzag confusion and compressive sensing, and then embeds it into a carrier image. The algorithm is quite robust but suffers from poor real-time performance and long encryption and decryption times. Compared to [21], the paper [22] uses parallel compressive sensing and integer discrete wavelet transform (IWT) to realize meaningful image encryption, which makes the algorithm more applicable and less time-consuming. However, it was pointed out in [23] that the construction of measurement matrices increases the computational complexity and storage requirements. Therefore, combining compressive sensing and DWT, multiple plain images are encrypted and embedded them into the carrier image. Following the HVS model, [25] decomposes the carrier image by lifting wavelet transform (LWT) and then adaptively embeds the preencrypted secret image into the corresponding coefficients of the carrier image to achieve the camouflage. Reference [28] combines DWT and CS to encrypt the image, but the restoration effect of the original image is poor. Reference [31] uses compressive sensing and discrete cosine transform- (DCT-) singular value decomposition (SVD) for medical image steganography. The restoration effect of the algorithm is good, but compressive sensing is performed upon the original image directly. After being attacked on a channel, the restoration effect of the image is observed to be poor and the robustness is not high. Reference [32] embeds the preencrypted secret image into the sparse representation coefficients of the carrier image by dictionary, which has a high embedding rate but poor robustness. In [33], a kind of novel substitution boxes (S-boxes) based on quantum walk is designed, in which LSB algorithm is used to hide the plain image.

In summary, a new image encryption algorithm is proposed in this paper. Firstly, the plain image is divided into four nonoverlapping blocks of equal size, and then the four blocks are rendered sparse by DWT. To reduce the block effect caused by block compression, the sparse plain image is preencrypted by using zigzag confusion before compression, and then each block of the preencrypted image is compressed and combined into the secret image. After the 2-level discrete wavelet transform of the carrier image, the obtained low-frequency and high-frequency coefficients are further subjected to DCT, and the post-DCT coefficients of the secret image are superimposed and restored to obtain the final encrypted image.

The rest of this paper is structured as follows. In Section 2, compressive sensing technology used by the algorithm, chaotic map, and zigzag scrambling are introduced. In Section 3, the encryption algorithm is introduced in detail. In Section 4, the decryption algorithm is introduced in detail. In Section 5, a simulation experiment is presented. In Section 6, the safety analysis and comparison experiments of the algorithm are presented. In Section 6, a conclusion is drawn.

2. Introduction of Related Technologies

2.1. Compressive Sensing. Compressive sensing can sample and compress the signal simultaneously, as long as sampling rate is far less than the Nyquist sampling rate, and recover the original signal with high probability from small observations. The detailed description is as follows.

Suppose that there is an $N \times 1$-dimensional signal x, which can be expressed in some transform domain as follows:

$$x = \sum_{i=1}^{N} \Psi_i \alpha_i = \Psi\alpha, \tag{1}$$

where Ψ represents a set of $N \times N$ orthogonal basis matrices, and α is the coefficient vector of signal x in the transform domain Ψ. When there are K nonzero values in the vector α, $K \ll N$, the signal x is compressible in the transform domain Ψ, which is expressed as follows:

$$y = \Phi x = \Phi\Psi\alpha = \Theta\alpha, \tag{2}$$

where Φ is a measurement matrix with a size of $M \times N$ ($M \ll N$), and $\Theta = \Phi\Psi$ is the associated sensor matrix. To correctly reconstruct the original signal x from the measured value y, the sensor matrix Θ must satisfy the RIP [34]. It has been pointed out in some literatures that an equivalent condition for the sensor matrix Θ to satisfy the RIP is that the measurement matrix Φ is not related to the sparse basis Ψ. Therefore, choosing a suitable measurement matrix is conducive to high-quality image restoration. In this paper, a partial Hadamard matrix is selected as the measurement matrix.

In addition, the signal reconstruction process is an optimization process. When the sensor matrix Θ satisfies the RIP condition, the original signal x can be recovered with high probability from the observed values y by solving the optimization problem presented in

$$\widehat{\alpha} = \arg\min \|\alpha\|_0. \tag{3}$$

As of now, many reconstruction algorithms have been proposed, such as MP, OMP, BP, and SL0. This paper uses OMP for image reconstruction.

2.2. Chaotic Map

2.2.1. The Logistic Map. The logistic map is one of the classical chaotic systems. The mathematical formulae are as follows:

$$x(n+1) = 1 - \lambda x^2(n), \tag{4}$$

where the parameter $\lambda \in (1.40015, 2]$. The logistic map is used to control the generation of the measurement matrix.

2.2.2. The Logistic-Tent System. Compared to a single logistic map or a single tent map, the Logistic-Tent System combines these two chaotic systems as seed maps to form a low-dimensional composite chaotic system [35]. The specific expressions are as follows:

$$\begin{aligned} X_{n+1} &= A_{\mathrm{LT}}(r, X_n) = \left(L(r, X_n) + T((4-r), X_n)\right) \mathrm{mod} 1, \\ &= \begin{cases} \left(rX_n(1-X_n) + (4-r)\dfrac{X_n}{2}\right) \mathrm{mod} 1, & X_i < 0.5, \\ \left(rX_n(1-X_n) + (4-r)\dfrac{(1-X_n)}{2}\right) \mathrm{mod} 1, & X_i \geq 0.5, \end{cases} \end{aligned} \tag{5}$$

where the parameter $r \in (0, 4]$. The Logistic-Tent System has better chaotic characteristics than the logistic map and the tent map. In this paper, we use this map to generate the initial position of zigzag confusion and the scrambling sequence of subsequent scrambling operations.

2.3. Zigzag Confusion. In the image encryption algorithm, zigzag confusion is a common method of scrambling image pixel positions. As shown in Figure 1, starting with the point $(1, 1)$, zigzag confusion scans the elements of the matrix according to a zigzag path and then stores them in a one-dimensional array. It then rearranges them in a certain order into a two-dimensional array, which disturbs the positions of the pixels in the image and reduces the correlation between adjacent pixels. The initial position of zigzag confusion is particularly important. To improve the ability of the algorithm to resist known-plaintext attacks and chosen-plaintext attacks, this paper takes the information of the original image and uses the Logistic-Tent System to generate the initial position of the scrambling, which improves the security of the algorithm.

Assuming that the size of the plain image P is $M \times N$, the sum of the pixel values of the image P is total = sum(sum(P)), and the block size of the image P is block_size = $m_b \times n_b$, this paper uses the Logistic-Tent System to generate a chaotic sequence $S = \{s_1, s_2, \ldots, s_{t_1+2+(1/2)M\times N}\}$ with length $t_1 + 2 + (1/2)M \times N$ and discards the first t_1 chaotic values to eliminate the transient effect. Then, the starting position (start_r, start_c) of zigzag confusion is generated according to

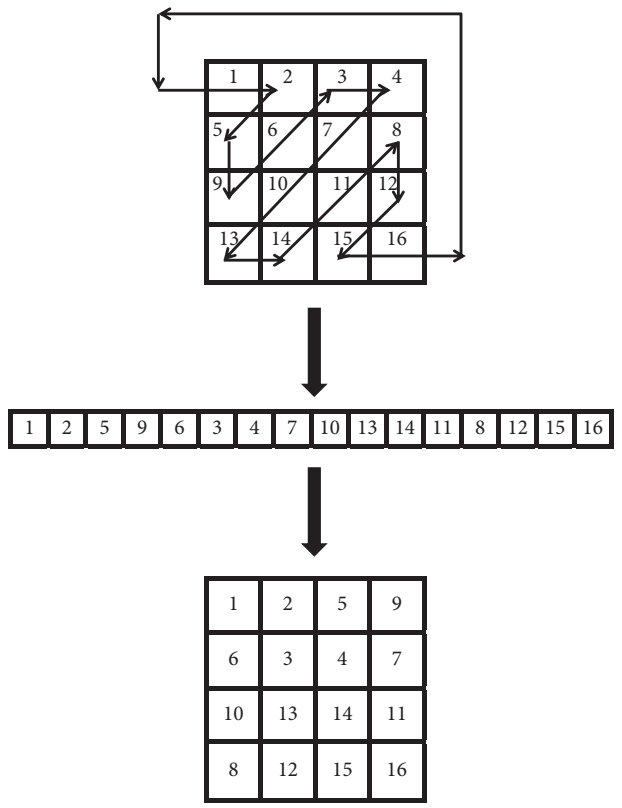


Figure 1: Process of the zigzag confusion.

$$\begin{aligned}\text{start\_}r &= \text{floor}\left[\left(s_1 - \text{floor}\left(s_1\right)\right) \times 10^{14} + \text{total}\right] \text{mod}\left(m_b + 1\right),\\ \text{start\_}c &= \text{floor}\left[\left(s_2 - \text{floor}\left(s_2\right)\right) \times 10^{14} + \text{total}\right] \text{mod}\left(n_b + 1\right).\end{aligned} \tag{6}$$

The remaining chaotic sequence of length $(1/2)M \times N$ is used for subsequent image scrambling operations.

3. The Proposed Image Compression and Encryption Algorithm

Referring to the idea of block compressed sensing, the obtained secret image is embedded into the carrier image using DWT and DCT after plain image block compression. The flow chart of the encryption algorithm is shown in Figure 2. The detailed encryption steps are as follows.

3.1. Block Compression-Encryption Process. The detailed steps are as follows:

Step 1: assuming that the size of the plain image P is $M \times N$, the plain image P is first divided into equal and nonoverlapping blocks, each of which has block_size $= m_b \times n_b$. Considering the subsequent embedding operations, the plain image P is divided into four blocks $B = \{\text{block}_1, \text{block}_2, \text{block}_3, \text{block}_4\}$, i.e., $m_b = (1/2)M$, $n_b = (1/2)N$.

Step 2: a sparse base Ψ of size $n_b \times n_b$ is constructed, and DWT is applied separately to each block to render them sparse:

$$B1_i = \Psi B_i \Psi', \quad i = 1, 2, 3, 4. \tag{7}$$

Step 3: to reduce the block effect caused by block compression and improve the robustness of the algorithm, the preencrypted block $B2_i$ is obtained by scrambling the sparse plain image as described in Section 2.3:

$$B2_i = \text{ZigZag}\left(B1_i\right), \tag{8}$$

where $i = 1, 2, 3, 4$.

Step 4: the dimension reduction observation is carried out. Partial Hadamard matrix is constructed by the logistic map to be used as the measurement matrix. The specific construction process is shown in Algorithm 1.

3.2. Embedding Process of the Secret Image. The detailed steps are as follows: (Algorithm 1)

Step 1: after applying 2-level DWT to the carrier image carrier, the low-frequency component $LL2$ and the high-frequency component $HH2$ are obtained. Then, a discrete cosine transform (DCT) is performed on $LL2$ and $HH2$ to obtain the corresponding DCT coefficients LL_dct and HH_dct.

Step 2: to facilitate the embedding of the secret image, it is divided into two blocks, C_left and C_right, of size $(1/2)M \times (1/2)N$. Similarly, a discrete cosine transform (DCT) is also used to obtain left_dct and right_dct.

Step 3: the DCT coefficients of low-frequency and high-frequency components of the secret image blocks are embedded into the DCT coefficients of carrier images with a certain embedding strength, as shown in

$$\begin{cases} CSL\text{\_dct} = LL\text{\_dct} + \beta \times \text{left\_dct}, \\ CSH\text{\_dct} = HH\text{\_dct} + \gamma \times \text{right\_dct}, \end{cases} \tag{12}$$

where β, γ are the embedding intensity factors, both of which take the value 0.1.

Step 4: the final encrypted image C is obtained by IDCT and IDWT.

Step 5: observe the preencrypted block $B2_i$ by generating the partial Hadamard matrix HM:

$$B3_i = \text{HM} \times B2_i. \tag{9}$$

Here, the measured value image $B3_i$ has a size of $m \times n_b$, $i = 1, 2, 3, 4$.

Step 6: considering the subsequent embedding process, we set cr = 0.5 and then merge the four blocks mentioned above to get a block $P1$ of size $M_p \times N_p$, where $M_p = (1/2)M$, $N_p = N$.

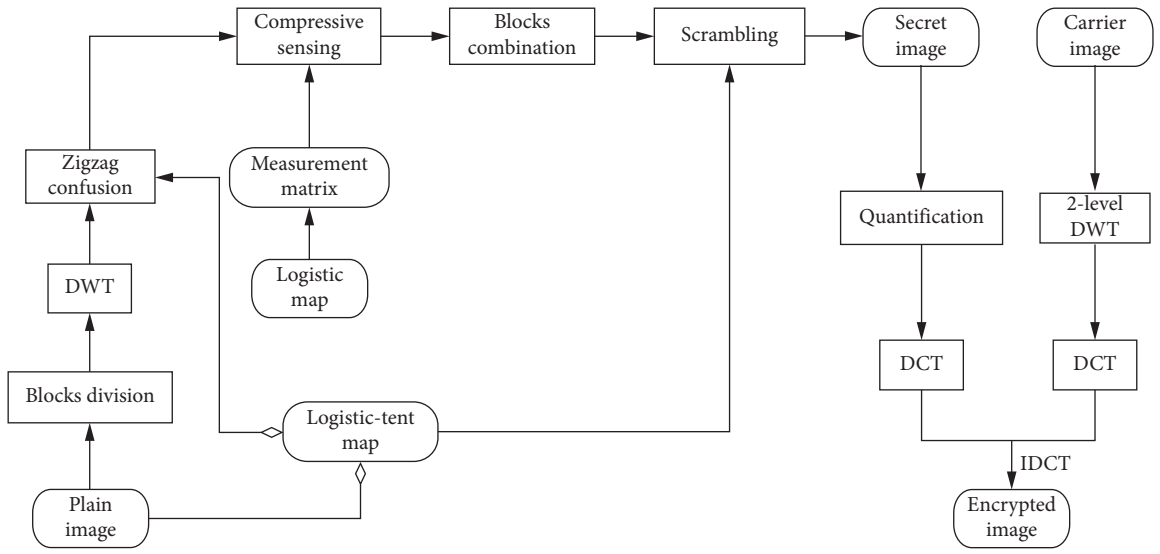


Figure 2: Flow chart of the encryption algorithm.

Input: The secret key pairs (x_1, λ_1), (x_2, λ_2), compression ratio cr.
Output: Measurement matrix Φ.

(1) Iterate logistic map $l = t_2 + \max(m_b, n_b)$ times with the initial parameter (x_1, λ_1) and (x_2, λ_2); the first t_2 chaotic values are discarded, and two chaotic sequences $SS1$ and $SS2$ of length $l' = \max(m_b, n_b)$ are obtained.

(2) $E = \text{sort}(SS1)$. The index sequence $E = \{e_1, e_2, \ldots, e_{l'}\}$ is generated. Similarly, $Z = \text{sort}(SS2)$, and the index sequence $Z = \{z_1, z_2, \ldots, z_{l'}\}$ is generated.

(3) Generate l'−order Hadamard matrix H and disturb Hadamard matrix row by row based on index Sequence E, i.e.,

$$H_r = \begin{pmatrix} H(e_1, :) \\ H(e_2, :) \\ \vdots \\ H(e_m, :) \end{pmatrix},$$

where $m = \text{cr} \times l'$, and cr is the compression rate of the image.

(4) Then, disturb Hadamard matrix H_r column by column based on index Sequence Z, i.e., $\text{HM} = \begin{pmatrix} H_r(:, z_1) & H_r(:, z_2) & \ldots & H_r(:, z_{l'}) \end{pmatrix}$, where $n = l'$. Finally, measurement matrix $\Phi = \text{HM}$ is obtained.

Algorithm 1: The construction process of measurement matrix Φ.

Step 7: considering the restoration effect of the encrypted image, each image block is quantized uniformly, so that the element value is mapped to the range $[0, 255]$:

$$P2 = \text{floor}\left[\frac{255(P1 - P1_{\min})}{(P1_{\max} - P1_{\min})}\right], \tag{10}$$

where $P1_{\max}$ and $P1_{\min}$ are the maximum and minimum values in the image $P1$, and floor( ) represents the rounding down operation.

Step 8: considering the security and robustness of the algorithm, the merged quantized image $P2$ is rescrambled. According to the residual chaotic sequence S obtained in Section 2.3, the scrambling operation is performed by equation (11) to obtain the secret image Secret:

$$\text{Secret}(k) = P2(S(k)), \tag{11}$$

where $k = 1, 2, \ldots, M_p \times N_p$.

4. Process of Image Decryption

The decryption flow chart is shown in Figure 3. The specific operation is as follows:

Step 1: after 2-level DWT is applied to the encrypted image C and the carrier image carrier, C_left and C_right, left_dct, and right_dct are obtained, respectively.

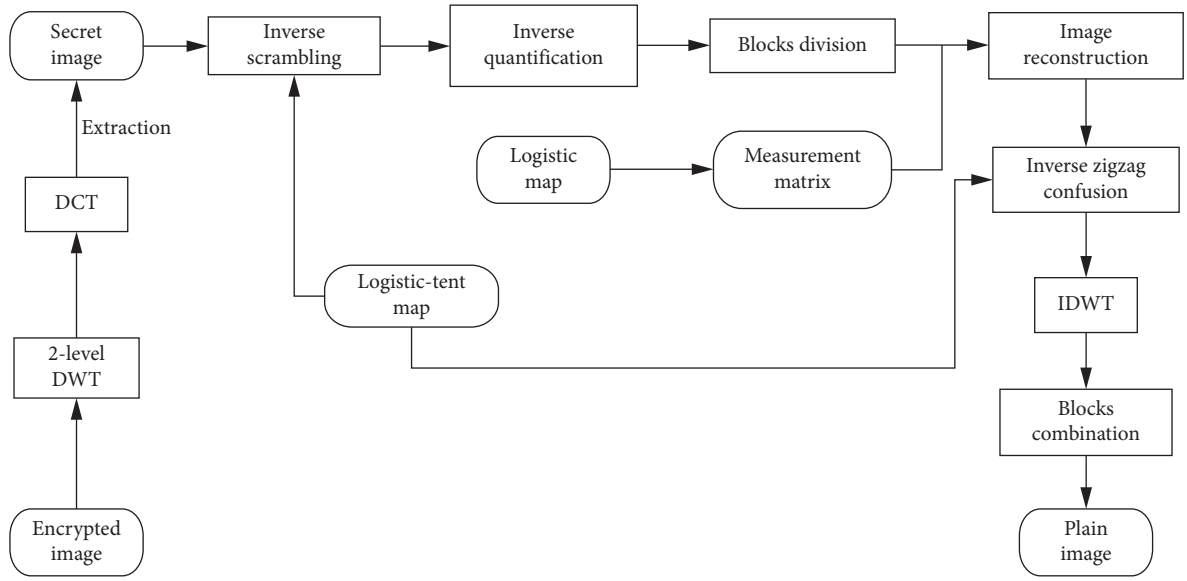


Figure 3: Flow chart of the decryption algorithm.

Step 2: DCT coefficients of the secret image Secret are restored by

$$\text{left\_dct} = \frac{CSL\_\text{dct} - LL\_\text{dct}}{\beta},$$
$$\text{right\_dct} = \frac{CSH\_\text{dct} - HH\_\text{dct}}{\gamma}. \tag{13}$$

Step 3: after the inverse DCT, the left and right image blocks are merged to obtain the secret image Secret.

Step 4: inverse quantization is performed after the secret image Secret is inversely scrambled:

$$P1 = \frac{P2 \times (P1_{\max} - P1_{\min})}{255} + P1_{\min}. \tag{14}$$

Step 5: the inverse quantized image is divided, and each block is reconstructed using the reconstruction algorithm OMP, followed by the application of the inverse zigzag confusion and the inverse wavelet transform. Finally, the parts are merged again to obtain the original image P.

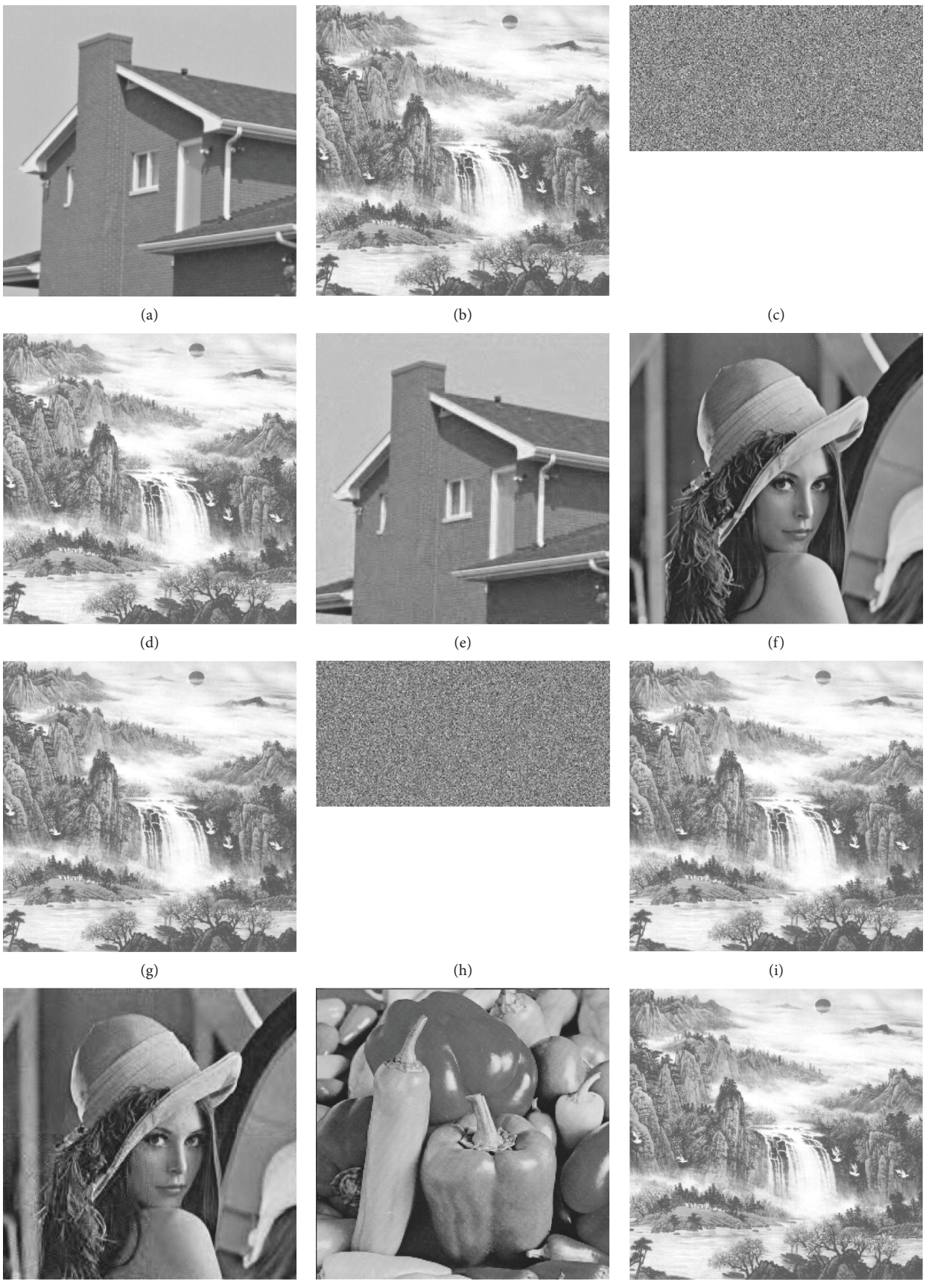
5. Experimental Results

The encryption algorithm used in this paper is based on the Windows 10 platform using Matlab R2016a. The experiment randomly selects two plain images of size 256×256 for algorithm testing. The size of the carrier image is taken to be 512×512 and uniformly selected as a landscape painting. Both chaotic systems are iterated 100 times to eliminate transient effects. The starting position of the zigzag confusion is determined by the pixel sum of the plain image and that of the Logistic-Tent System, which ensures that the algorithm resists known-plaintext attacks and chosen-plaintext attacks. The initial state values are $x_1 = 0.37$ and $x_2 = 0.70$, the parameters of the logistic map are $\lambda_1 = \lambda_2 = 2.000$, the initial state value is $x_3 = 0.6825$, and the parameter of the Logistic-Tent System is $r = 3.999$. Following that, the DWT chooses the Haar wavelet, and the reconstruction algorithm chooses the OMP because of low complexity and high recovery quality.

Figure 4 shows the encryption and decryption effects for different plain images. Generally, for meaningful image encryption frameworks, peak signal-to-noise ratio (PSNR) or normalized correlation (NC) coefficient are used to evaluate the imperceptibility of the encrypted images or the restoration quality of decrypted images. The unit of PSNR is dB. The PSNR is positively correlated with the imperceptibility of the encrypted image and the restoration quality of the decrypted image and is negatively correlated with image distortion. Similarly, as the NC value increases, the similarity between the two images increases as well. The specific formulae are as follows: if we assume that the size of the plain image $P(i, j)$ is $M \times N$ and that the encrypted image or the decrypted image is denoted by $C(i, j)$, then

$$\text{PSNR} = 10 \log_{10}\left[\frac{255^2}{1/MN \sum_{i=1}^{M} \sum_{j=1}^{N} [P(i, j) - C(i, j)]^2}\right],$$
$$\text{NC} = \frac{\sum P(i, j) C(i, j)}{\sqrt{\sum (P(i, j))^2} \sqrt{\sum (C(i, j))^2}}. \tag{15}$$

A landscape painting is chosen as the carrier image in this experiment. Landscape paintings have a characteristic hazy beauty. As the carrier image, it hides the existence of secret image to a certain extent and achieves an effect of camouflage, increasing the security of the secret image. The compression ratio taken here is 0.5. Figures 4(a), 4(f), and 4(k) are three different plain images and Figures 4(d), 4(i), and 4(n) are the corresponding encrypted images. Their PSNRs are 34.5665 dB, 34.9369 dB, and 34.8205 dB,



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

(j) (k) (l)

Figure 4: Continued.

(m) (n) (o)

Figure 4: Test result: (a) plain image of house, (b) carrier image of landscape, (c) secret image of house, (d) encrypted image of house, (e) reconstructed image of house, (f) plain image of Lena, (g) carrier image of landscape, (h) secret image of Lena, (i) encrypted image of Lena, (j) reconstructed image of Lena, (k) plain image of peppers, (l) carrier image of landscape, (m) secret image of peppers, (n) encrypted image of peppers, and (o) reconstructed image of peppers.

respectively. Figures 4(e), 4(j), and 4(o) are the corresponding decrypted images, and the corresponding PSNRs are 34.5722 dB, 30.0233 dB, and 29.8787 dB, respectively.

Table 1 shows the hiding effect and recovery quality of different plain images. PSNR1 shows the peak signal-to-noise ratio (PSNR) for the carrier image before and after hiding while PSNR2 shows recovery effect. So, it can be seen that the proposed method has good imperceptibility and recovery effect.

Table 1: PSNR for different images.

	PSNR1 (dB)	PSNR2 (dB)
House	34.5665	34.5772
Lena	34.9369	30.0233
Peppers	34.8205	29.8787

6. Security Analysis

6.1. Key Space Analysis. A secure and efficient encryption algorithm should have a key space of at least 2^{100}. In this paper, the initial state values x_1, x_2, the parameters λ_1, λ_2 of the logistic map which control the generation of the measurement matrix, the initial state value x_3, and the parameter r of the Logistic-Tent System are used to generate the initial position of the zigzag confusion and the subsequent disturbance operation; that is, the key to the encryption algorithm is key $= \{x_1, x_2, x_3, \lambda_1, \lambda_2, r\}$. When the precision reaches 10^{-14}, the key space of the proposed encryption algorithm is $10^{14} \times 10^{14} \times 10^{14} \times 10^{14} \times 10^{14} = 10^{70} \approx 2^{233} > 2^{100}$. Therefore, the key space of the encryption algorithm proposed in this paper is large enough to resist brute-force attacks.

6.2. Key Sensitivity Analysis. Key sensitivity is an important index to evaluate the security of an encryption algorithm. If the decrypted images are significantly different when the key changes slightly, it shows that the proposed algorithm is sensitive to the key. This paper mainly tests the decryption key sensitivity of the algorithm, as shown in Figure 5. Figure 5(a) is a plain image, Figure 5(b) is the encrypted image, and Figure 5(c) is the decrypted image. In this experiment, $\lambda_1 = \lambda_2$, and so Figures 5(d)–5(h) modify one of the decrypted keys, while the other keys remain unchanged. It can be seen that when the decryption key changes slightly, the image cannot be restored at all. So the key sensitivity of the algorithm is strong.

6.3. Histogram Analysis. The encryption algorithm proposed in this paper is based on a meaningful image encryption framework. So, our main purpose is to prove the similarity between encrypted image and carrier image by comparing their histograms, i.e., measure the imperceptibility and the difference between the plain image and the encrypted image to establish the security of the algorithm. Thus, the histogram analysis reflects the reliability and security of the algorithm. As shown in Figure 6, the histogram of the carrier image is similar to that of the encrypted image, which shows that the plain image is well camouflaged and that the histograms of the plain image and the encrypted image are quite different, which shows that the algorithm is highly secure.

6.4. Comparison. This paper draws on the idea of block compressed sensing and then compresses and encrypts the plain image and embeds it in a carrier image. Therefore, image reconstruction is less time-consuming than in the case of a general image encryption algorithm based on compressive sensing. The reconstruction algorithm OMP is chosen. Here, [21] and [31] were selected for experimental comparison. The size of the plain image "Lena" is 256×256, and the carrier image uniformly selects the landscape painting. Since the internal structure of each algorithm is different, the sizes of the carrier images and the compression ratio of the images will be inconsistent. The carrier image size proposed in the algorithm described in

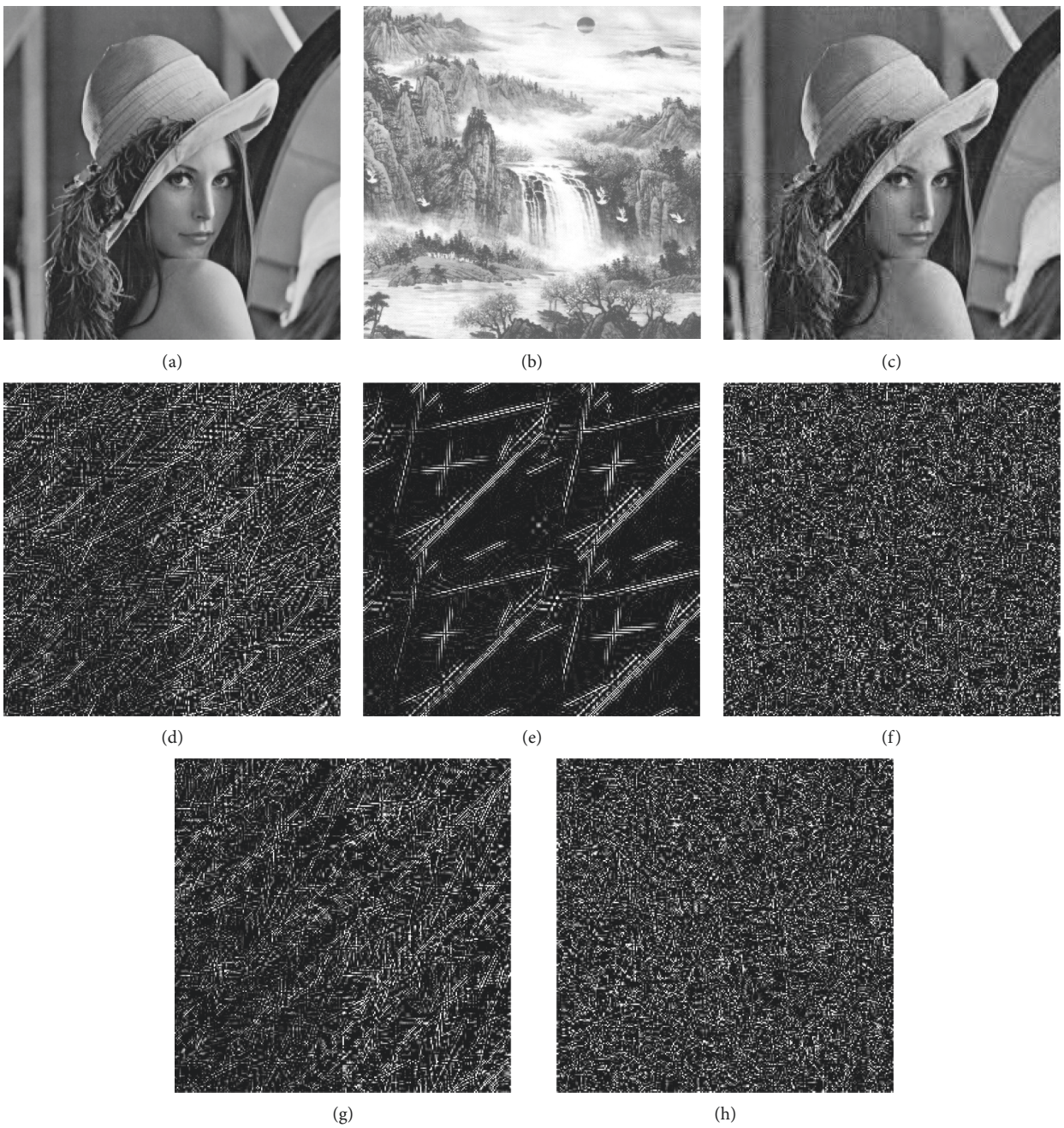


FIGURE 5: Key sensitivity test: (a) plain image, (b) encrypted image, (c) decrypted image, (d) decrypted image with $x_1 + 10^{-14}$, (e) decrypted image with $x_2 + 10^{-14}$, (f) decrypted image with $x_3 + 10^{-14}$, (g) decrypted image with $\lambda_1 + 10^{-14}$ or $\lambda_2 + 10^{-14}$, and (h) decrypted image with $r + 10^{-14}$.

this paper is 512×512, and the carrier image size in [21] and [31] is 256×256. The compression ratio of [21] is fixed at 0.25, that of [31] is fixed at 1.0, and that of the algorithm proposed in this paper is 0.5. To ensure the validity of the experimental data, the encryption and decryption time of each image is averaged over multiple experiments. The encryption and decryption time for different plain images is shown in Table 2. Table 3 gives the results of normalized correlation test.

According to the data shown in Tables 2 and 3, the compression ratio of the proposed algorithm is twice as large as that of [21], so the decryption time is a little longer, but the encryption time is relatively shorter. NC value of the decrypted image is also larger than [21]. The reason is that [21] uses SHA-256 algorithm to generate the key which increases the transmission burden. Compared with [31], the compression ratio of the proposed algorithm is half that of [31], although the encryption time is relatively longer, but

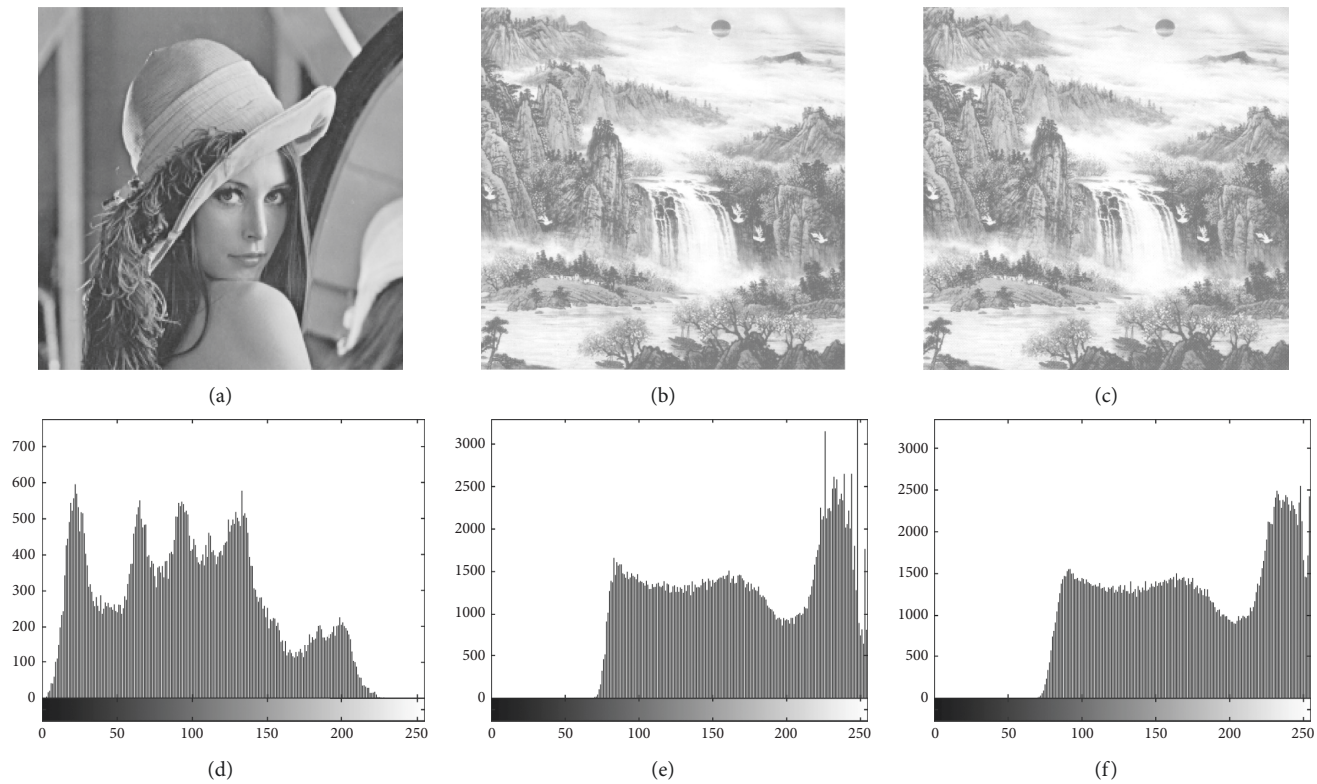


Figure 6: Histogram test: (a) plain image, (b) carrier image, (c) encrypted image, (d) histogram of the plain image, (e) histogram of the carrier image, and (f) histogram of the encrypted image.

Table 2: Comparison of the time cost.

	Encryption Time (s)			Decryption Time (s)		
	Reference [21]	Reference [31]	Proposed algorithm	Reference [21]	Reference [31]	Proposed algorithm
Lena	0.7828	0.0617	0.1146	1.7378	8.7035	2.0058
Barbara	0.7886	0.0558	0.1157	1.7244	8.6632	1.9957
House	0.7885	0.0579	0.1183	1.7393	8.6463	1.9983
Peppers	0.7958	0.0702	0.1251	1.7266	8.7137	1.9926

Table 3: Comparison of normalized correlation.

	NC (Normalized correlation)		
	Reference [21]	Reference [31]	Proposed algorithm
Lena	0.9821	0.9989	0.9974
Barbara	0.9846	0.9991	0.9979
House	0.9929	0.9995	0.9995
Peppers	0.9861	0.9989	0.9980

Table 4: Comparison of block compression and nonblock compression.

	Encryption time (s)		Decryption time (s)	
	Block compression	Whole compression	Block compression	Whole compression
Lena	0.1742	0.1236	2.0058	3.7097
Barbara	0.1773	0.1312	1.9957	3.7758
House	0.1769	0.1264	1.9983	3.7024
Peppers	0.1783	0.1315	1.9926	3.7232

the decryption time is greatly shortened. However, NC values in Table 3 are little lower, but it is also acceptable. Table 4 displays the better performance of block method than nonblock.

7. Conclusions

In conclusion, this paper invokes the idea of block compressed sensing, divides the plain image into blocks, and makes compressive sensing observations. To reduce the block effect caused by this division, zigzag confusion is used to scramble the pixel positions in each block, after each part is rendered sparse. Considering the security of the algorithm and the convenience of subsequent embedding operations, the processed images are merged, then quantized, and scrambled again to obtain the secret image. They are then combined via the 2-level DWT and DCT, and the secret image is embedded into the carrier image. The experimental results prove the efficiency and security of the proposed

algorithm. In addition, the size of the measurement matrix is smaller because of the image block operation. Under the same compression ratio, the proposed algorithm needs less storage space and lower computational complexity and achieves faster image reconstruction speeds and better reconstruction effects than the existing ones. Therefore, it has bright prospects in practical applications.

There are three contributions of our method, i.e., (1) generating Hadamard matrix and confusing it with chaotic sequence to form a measurement matrix, (2) using scrambling operation zigzag to sparse the plain image in order to enhance a good recovery effect, and (3) encrypting the quantized image after compressive sensing to achieve a secret image before embedding process.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundations of China (nos. 61972103 and 61702116), the Natural Science Foundation of Guangdong Province of China (no. 2019A1515011361), the Science and Technology Planning Project of Guangdong Province of China (no. 2017A010101025), the Program for Scientific Research Start-up Funds of Guangdong Ocean University of China (no. R17037), the Special Funding Program for Excellent Young Scholars of Guangdong Ocean University of China (no. HDYQ2017006), and the Project of Enhancing School with Innovation of Guangdong Ocean University of China (Q18306).

References

[1] S. Sun, "A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling," *IEEE Photonics Journal*, vol. 10, no. 2, pp. 1–14, 2018.

[2] C. Wu, K.-Y. Hu, Y. Wang, J. Wang, and Q.-H. Wang, "Scalable asymmetric image encryption based on phase-truncation in cylindrical diffraction domain," *Optics Communications*, vol. 448, pp. 26–32, 2019.

[3] M. Li, D. Lu, W. Wen, H. Ren, and Y. Zhang, "Cryptanalyzing a color Image encryption scheme based on hybrid hyperchaotic system and cellular automata," *IEEE Access*, vol. 6, pp. 47102–47111, 2019.

[4] B. Mondal, S. Singh, and P. Kumar, "A secure image encryption scheme based on cellular automata and chaotic skew tent map," *Journal of Information Security and Applications*, vol. 45, pp. 117–130, 2019.

[5] Y. Liu, S. Tang, R. Liu, L. Zhang, and Z. Ma, "Secure and robust digital image watermarking scheme using logistic and RSA encryption," *Expert Systems with Applications*, vol. 97, pp. 95–105, 2018.

[6] D. L. Donoho, "Compressed sensing," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[7] E. J. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 489–509, 2006.

[8] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Optics & Laser Technology*, vol. 82, pp. 121–133, 2016.

[9] Q. Xu, K. Sun, C. Cao, and C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map," *Optics and Lasers in Engineering*, vol. 121, pp. 203–214, 2019.

[10] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Processing*, vol. 148, pp. 124–144, 2018.

[11] L. Wang, L. Li, J. Li, J. Li, B. B. Gupta, and X. Liu, "Compressive sensing of medical images with confidentially homomorphic aggregations," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1402–1409, 2019.

[12] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Optics & Laser Technology*, vol. 115, pp. 257–267, 2019.

[13] Y. Luo, J. Lin, J. Liu et al., "A robust image encryption algorithm based on Chua's circuit and compressive sensing," *Signal Processing*, vol. 161, pp. 227–247, 2019.

[14] R. Ponuma and R. Amutha, "Encryption of image data using compressive sensing and chaotic system," *Multimedia Tools and Applications*, vol. 78, no. 9, pp. 11857–11881, 2019.

[15] L. Gan, "Block compressed sensing of natural images," in *15th International Conference on Digital Signal Processing*, pp. 403–406, Cardiff, UK, July 2007.

[16] N. Zhou, A. Zhang, F. Zheng, and L. Gong, "Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing," *Optics & Laser Technology*, vol. 62, pp. 152–160, 2014.

[17] Z. Chen, X. Hou, X. Qian, and C. Gong, "Efficient and robust image coding and transmission based on scrambled block compressive sensing," *IEEE Transactions on Multimedia*, vol. 20, pp. 1610–1621, 2018.

[18] L. Zhu, H. Song, X. Zhang, M. Yan, L. Zhang, and T. Yan, "A novel image encryption scheme based on nonuniform sampling in block compressive sensing," *IEEE Access*, vol. 7, pp. 22161–22174, 2019.

[19] L. Bao and Y. Zhou, "Image encryption: generating visually meaningful encrypted images," *Information Sciences*, vol. 324, pp. 197–207, 2015.

[20] L. D. Singh and K. M. Singh, "Visually meaningful multi-image encryption scheme," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 7397–7407, 2018.

[21] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Processing*, vol. 134, pp. 35–51, 2017.

[22] H. Wang, D. Xiao, M. Li, Y. Xiang, and X. Li, "A visually secure image encryption scheme based on parallel compressive sensing," *Signal Processing*, vol. 155, pp. 218–232, 2018.

[23] R. Ponuma, R. Amutha, S. Aparna, and G. Gopal, "Visually meaningful image encryption using data hiding and chaotic compressive sensing," *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 25707–25729, 2019.

[24] H. Yao, X. Liu, Z. Tang, Y.-C. Hu, and C. Qin, "An improved image camouflage technique using color difference channel transformation and optimal prediction-errore expansion," *IEEE Access*, vol. 6, pp. 40569–40584, 2018.

[25] H. Yao, X. Liu, Z. Tang, C. Qin, and Y. Tian, "Adaptive image camouflage using human visual system model," *Multimedia Tools and Applications*, vol. 78, no. 7, pp. 8311–8334, 2019.

[26] M. Fakhredanesh, M. Rahmati, and R. Safabakhsh, "Steganography in discrete wavelet transform based on human visual system and cover model," *Multimedia Tools and Applications*, vol. 78, no. 13, pp. 18475–18502, 2019.

[27] D. Xiao, Y. Chang, T. Xiang, and S. Bai, "A watermarking algorithm in encrypted image based on compressive sensing with high quality image reconstruction and watermark performance," *Multimedia Tools and Applications*, vol. 76, no. 7, pp. 9265–9296, 2017.

[28] R. Zhang, D. Xiao, and Y. Chang, "A novel image authentication with tamper localization and self-recovery in encrypted domain based on compressive sensing," *Security and Communication Networks*, vol. 2018, Article ID 1591206, 15 pages, 2018.

[29] R. Thanki and S. Borra, "Fragile watermarking for copyright authentication and tamper detection of medical images using compressive sensing (CS) based encryption and contourlet domain processing," *Multimedia Tools and Applications*, vol. 78, no. 10, pp. 13905–13924, 2019.

[30] J.-S. Pan, W. Li, C.-S. Yang, and L.-J. Yan, "Image steganography based on subsampling and compressive sensing," *Multimedia Tools and Applications*, vol. 74, no. 21, pp. 9191–9205, 2015.

[31] R. Thanki, S. Borra, V. Dwivedi, and K. Borisagar, "A steganographic approach for secure communication of medical images based on the DCT-SVD and the compressed sensing (CS) theory," *The Imaging Science Journal*, vol. 65, no. 8, pp. 457–467, 2017.

[32] M. Li, H. Fan, H. Ren, D. Lu, D. Xiao, and Y. Li, "Meaningful image encryption based on reversible data hiding in compressive sensing domain," *Security and Communication Networks*, vol. 2018, Article ID 1591206, 12 pages, 2018.

[33] A. A. A. EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Optics and Laser Technology*, vol. 116, pp. 92–102, 2019.

[34] E. J. Candès, "The restricted isometry property and its implications for compressed sensing," *Comptes Rendus Mathematique*, vol. 346, no. 9-10, pp. 589–592, 2008.

[35] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, 2014.