Mathematical Biosciences and Engineering

MBE, 18(2): 1722–1739.
DOI: 10.3934/mbe.2021089
Received: 25 October 2020
Accepted: 28 January 2021
Published: 07 February 2021

http://www.aimspress.com/journal/MBE

Research article

A visually secure image encryption method based on integer wavelet transform and rhombus prediction

Xianyi Chen[1,2], Mengling Zou[1], Bin Yang[3], Zhenli Wang[4], Nannan Wu[1] and Lili Qi[5,*]

[1] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China
[2] Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, Nanjing 210044, China
[3] School of Design, Jiangnan University, Wuxi 214028, China
[4] Computer Information and Network Security Department, Jiangsu Police Institute, Nanjing 210031, China
[5] School of Computer Engineering, Weifang University, Weifang 261061, China

* **Correspondence:** Email: liliqi77@163.com; Tel: +8613914795525.

Abstract: Traditional image encryption technology usually encrypts a normal image into a noise matrix, which can protect the image in a certain extent, but noise appearance is easy to arouse the suspicion of attackers. To avoid this problem, a method of encrypting image into carrier image with visual meaning is proposed. Inspired by the existing visually secure encryption technique, we proposed an improved method based on the integer wavelet transform (IWT) and prediction scheme. The secret image is hidden in the high frequency coefficients of IWT to achieve good invisibility, and prediction error are used to replace the pixels of the carrier image to improve the final image quality. Experimental results and analysis show that the quality of the encrypted image is 3.5 dB better than that of the previous ones.

Keywords: image encryption; visually meaningful; discrete wavelet transform; rhombus prediction

1. Introduction

Encryption and steganography are the two information branches of the information security, they

are used in a wide of the privacy protect and conceal communication of the digital media [1], such as text, image, audio video and so on. The image encryption focuses on preventing unauthorized accessing by encoding the secret information into an encrypted image similar to noise or texture [1,3]. Whereas steganography is committed to hiding the conceal communication by embedding the secret information into a carrier image and which will not change the visual appearance of the original image [4–6]. Although there are differences in principles and methods, they can protect information effectively.

The image encryption technology can be divided into two classes: the spatial domain method [7,8] and the frequency domain method [9]. The encryption method in spatial domain treats the image as two-dimensional data and works on the secret pixels directly to generate an encrypted image with random noise. Typical algorithms include Advanced Encryption Standard (AES) [10], chaotic systems [11,12], wave transmission [13], DNA coding [14], and some recently published symmetric encryption and asymmetric encryption methods [15–18]. For the frequency domain encryption, Fourier transform (FFT) or discrete cosine transform (DCT) are used to transform the image from the spatial domain to the frequency domain firstly, and then the frequency data will be encrypted [19]. Image encryption is an efficient security tool during the privacy protection usually converts a two-dimensional image into one-dimensional data [20]. Since these methods destroy the correlation within the image, attackers can be extremely hard to extract useful information from the encrypted images [21], so it can protect the privacy of the secret image during transmission and storage in some extent [22].

However, as we all know, the encrypted images are cryptographic images similar to noise or texture, which will make an obvious visual sign indicating that the encrypted image contains important information, as shown in Figure 1 (a),(b). Therefore, these encrypted images may cause suspicion and even analysis by the attackers when they are transmitted in public channels [23–25].

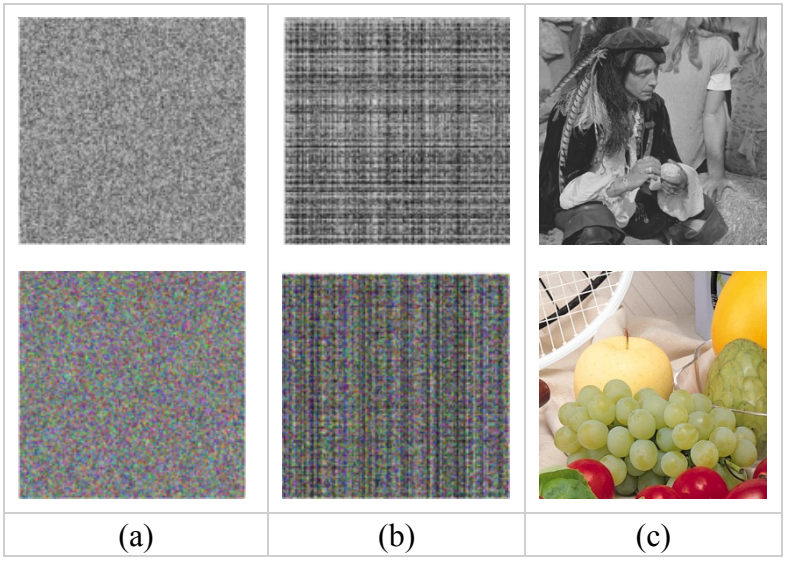


Figure 1. Different types of encrypted images. (a) Encrypted images with noise features; (b) encrypted images with texture features and (c) visual safety encrypted images.

To overcome the disadvantage that the noise and texture features are easy to attract the attention of the encrypted images and improve the visually security, some researchers have tried to encrypt images into normal ones to prevent the content from being suspected by combining the encryption and steganography. The appearance of the encrypted image is almost the same as that of the ordinary

images, which can effectively avoid malicious tamper and attack, thus improving the security of encrypted images [26–28], as shown in the Figure 1(c). For example, in 2015, Bao and Zhou [29] proposed a visually meaningful image encryption (VMEI) called BZ scheme, in which they first pre-encrypt the secret image by an encryption algorithm [30], then embed the pre-processed image into the sub-bands of another carrier image. Although the encrypted image has a visually security appearance with the normal image in this method, the image quality is not very well. Subsequently, to improve the quality and security of the BZ scheme, Kanso and Ghebleh [31] proposed an encryption scheme that can restore the secret image losslessly. In the embedding phase, they first use a two-dimensional lifting wavelet transform (LWT) to divide the carrier image into three high-frequency coefficients and one low-frequency. Later, Yang and Zhang [32] combined with the knowledge of quantum computing to improve the BZ scheme, which reduced the texture features of the secret images to a certain extent and had a better performance. In 2017, Chai et al. [33] trained a data dictionary by using the compressed sensing technology to combine the secret image with carrier image. However, it has a practical problem that the secret image could not be restored losslessly, which limits its development potential for the application of content sensitive.

Focusing on the image quality and integrity, in this paper, we use rhombus prediction and wavelet transform to embed the pre-encrypted secret image into another natural-looking carrier image, the final encrypted image is not only visually secure, but also of high quality. The contributions of the proposed method are:

1). The visual quality of the final carrier image, containing secret image, is improved because the secret pixels are replaced by the prediction errors during the embedding stage, which greatly reduces the modification to the carrier image.

2). The proposed algorithm is reversible. In the proposed method, the receiver can extract secret information from the final encrypted image and reconstruct the secret image.

The paragraph structure of this article is listed as follows: The second part shows the related work. The third section is the introduction of the proposed method. The fourth part gives the experimental results, and the final section summarizes the full text.

2. The introduction of BZ scheme

The BZ scheme [29] mainly includes two steps: 1) pre-encryption phase, 2) Content Transformation Based on Discrete Wavelet Transform (CTDWT) [34]. During the pre-encryption phase, the secret image is encrypted to noise or texture. In the CTDWT stage, the CTDWT is used to divide the carrier image C into four parts: LL, LH, HL and HH, which are denoted as C_A, C_H, C_V and C_D respectively. Then divide the pre-encryption image into two arrays called P_V and P_D respectively [35], and embed the two arrays into the HL and HH sub-bands by value substitution. Finally, an encrypted image containing a secret image is obtained by using inverse CTDWT transform, the details are listed as follows.

Suppose S represents the secret image, K_t denotes the encryption key. Then, S can be encrypted into an indistinguishable pre-encrypted image P by the Eq (1):

$$P = F(S, K_t) \tag{1}$$

where F is the pre-encryption function, such as the Advanced Encryption Standard (AES). After pre-processing, the secret image becomes a noise or texture image.

Decompose the carrier image C to four coefficient matrices C_A, C_H, C_V and C_D by CTDWT, then divide the pre-encrypted image P into two parts P_V and P_D, which can be calculated by Eqs (3) and (4):

$$P_V(i,j) = \lfloor P(i,j)/10 \rfloor \tag{2}$$

$$P_D(I,j) = \lfloor P(I,j) \bmod 10 \rfloor \tag{3}$$

finally, embed the P_V and P_D and parameter into C_V and C_D, respectively.

$$E = D(P, C, K_P) \tag{4}$$

where D is the CTDWT function, the K_P represents the parameter set of DWT, which defines the DWT wavelet transform filter, and E is the final encrypted image.

Take a pixel of the pre-encrypted image with a value of 125 for example, $P_V = \lfloor 125/10 \rfloor = 12$, $P_D = \lfloor 125 \mod 10 \rfloor = 5$, then, C_V holds 12 and C_D holds 5.

In the receiver side, they firstly decompose the encrypted image into four sub-bands namely E_A, E'_H, E'_V, E'_D. To reconstruct the pre-encrypted image, the following formula is defined:

$$P'(i,j) = 10P'_V(i,j) + P'_D(i,j) \tag{5}$$

where, P' is the restored pre-encrypted image, and P'_V, P'_D corresponding to the C_V and C_D sub-bands of image E.

Overall, this encryption system is visually safe, but it is an unwise choice for replacing the coefficient values in the carrier image's C_V and C_D matrices directly, and the visual quality of the encrypted image will be degraded largely.

3. The proposed method

As described in the Section 2, BZ scheme [29] completely replaces the HL and HH parts of the carrier image with the P_V and P_D parts of the pre-encrypted secret image. This operation will directly affect the quality of the final encrypted image, which is also an obvious disadvantage of the scheme. To improve the image quality, we proposed a new meaningful encryption scheme based on the BZ scheme [29], the flowchart of encryption process is shown in Figure 2.

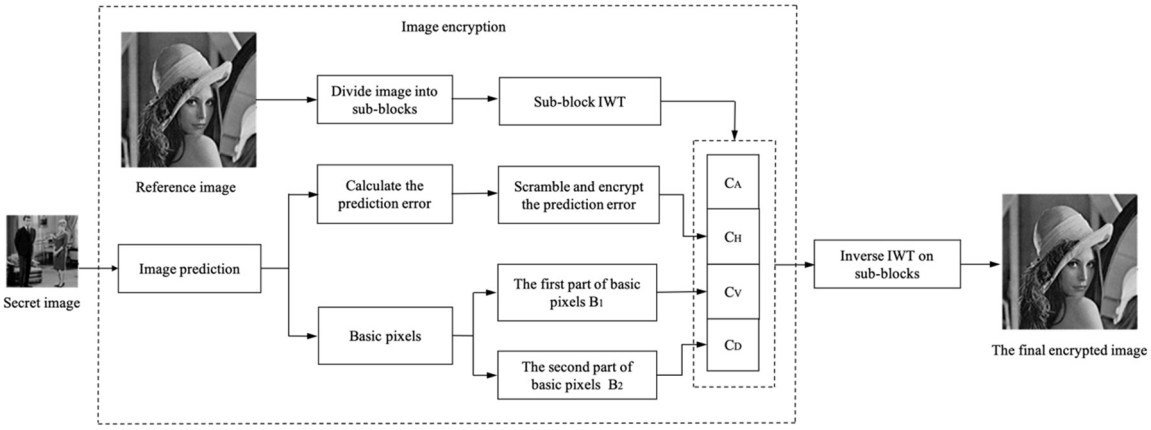


Figure 2. Encryption flowchart of the proposed method.

3.1. Encryption and embedding process

Suppose the size of the secret image S is $m \times n$ and the size of the carrier image C is $2m \times 2n$. Firstly, choose the rhombus predictor proposed by Sachnev et al. [36] to calculate the prediction value of S, which is an effective prediction scheme, and the prediction mode is shown in Figure 3. The pixel value $U(i,j)$ (denoted as Cross set) can be predicted by the four neighboring pixels $v(i,j)$ (denoted as Dot set), and vice versa. The prediction value can be calculated using the Eq (6).

$$U(i,j) = \lfloor (v(i,j-1) + v(i+1,j) + v(i,j+1) + v(i-1,j))/4 \rfloor \tag{6}$$

Then get the prediction error sequence P_s by $S(i,j) - U(i,j)$ and scan it by zigzag manner. After that, using AES algorithm to encrypt e with secret key K_t, the encryption process is calculated by the Eq (7):

$$P_e = F(P_s, K_t) \tag{7}$$

where F is the encryption function and P_e is the encrypted prediction error.

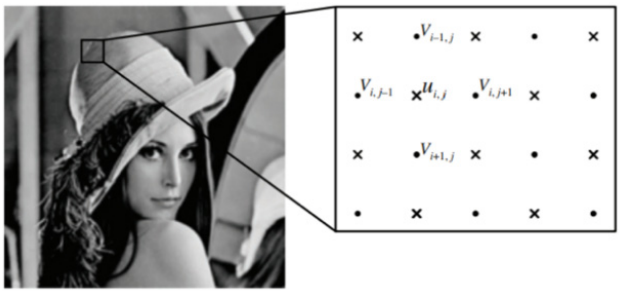


Figure 3. The prediction pattern of rhombus prediction scheme.

Secondly, divide the carrier image into $s \times s$ non-overlapping sub-blocks, then use IWT to decompose each image block into a low frequency sub-band and three high frequency sub-bands, which are denoted as C_A, C_H, C_V and C_D respectively, where C_A is a low-frequency matrix, which concentrates most of the energy and features of the image, and C_H, C_V and C_D represent the middle frequency matrix and high-frequency matrix, which contain the details of the image.

Then, the parameter set K_P, the encrypted prediction error sequence P_e, the basic pixel B used to restore original pixel are embedded into the coefficient matrixes of the carrier image by value replacement with Eq (8).

$$E = D(B, P_e, C, K_P) \tag{8}$$

where, E is the final encrypted image similar to the carrier image.

To prevent the pixels from being outside the range of [0,255], we first adjust the pixels of the carrier image C to be between 10 and 245, and called the adjusted carrier image C'. Input the secret image S, the encryption key K_t, output the final encrypted image, and the details of the embedding algorithm are listed as follows:

Step 1. Shrink the carrier image C with the formula $C' = \lceil \rho - (\omega - \rho)/255C \rceil$ to prevent the overflow and underflow of the pixel value. Where C' is the modified carrier image, and $\rho =$

$10, \omega = 245$.

Step 2. Divide the processed carrier image C' into 8×8 blocks and then divide each block into four parts by IWT, which are represented by C_A, C_H, C_V and C_D.

Step 3. Calculate the prediction value $U(i,j)$ of the secret image using the rhombus prediction scheme, and then calculate the prediction error $P_s(i,j) = S(i,j) - U(i,j)$, and the basic pixels are listed as B.

Step 4. Scramble the prediction error $P_s(i,j)$ first and encrypt it into the sequence P_e using AES algorithm with the secret key K_t.

Step 5. Segment the basic pixels into two parts B_1 and B_2, then divided B_2 into B_V and B_D by the Eqs (2) and (3).

Step 6. Embed the prediction error into C_H, the basic pixel B_1 into C_V, and B_2 into C_D by the value substitution. The modified sub-bands are denoted as C_A, C'_H, C'_V and C'_D.

Step 7. Apply inverse IWT to the modified sub-band of each block to get the final encrypted image E.

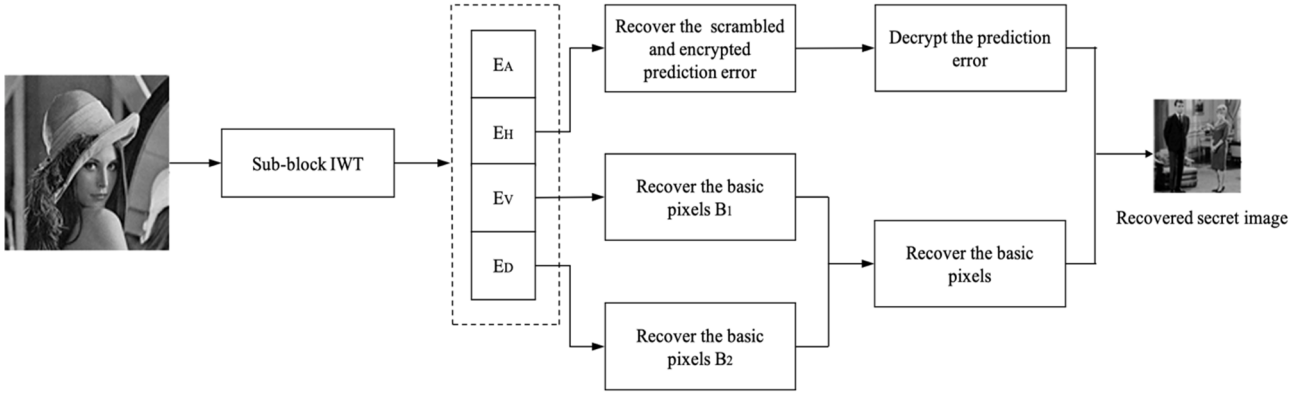


Figure 4. Decryption flowchart of the proposed method.

3.2. Decryption and reconstruction process

The restoration of the secret image can be carried out according to the steps in the encryption phase, which is usually the reverse operation. According to the decryption framework in Figure 4, the decryption phase mainly includes two steps: information extraction and image reconstruction.

In the information extraction stage, we first use IWT to divide each block of the final encrypted image E into four parts called E_A, E_H, E_V and E_D. Secondly, the encrypted prediction error sequence is extracted from E_H, and two parts of the basic pixel are extracted from E_V and E_D, i.e., $P'_e = E_H$, $B'_1 = E_V$. B'_2 are restored from E_D by the Eq (9).

$$B_2'(i,j) = 10B'_V(i,j) + B'_D(i,j) \tag{9}$$

where $B_2'(i,j)$ is the extracted basic pixel, $B'_V(i,j)$ and $B'_D(i,j)$ represent the pixels obtained by applying inverse IWT to the final encrypted image.

Finally, P'_e is decrypted with the key, the original prediction error can be restored in the reverse order of zigzag, and the secret image is reconstructed according to the basic pixel and prediction error.

4. Experiments and evaluations

All experiments are implemented in MatlabR2016a, and the configuration of the computer is i5-2450 M and 8 GB of memory. To compare fairly with the previous schemes, we use the same wavelet kernel function "db1" with the BZ scheme to decompose the carrier image. All images are downloaded from Bose base image library [37], and the secret image is one fourth size of the carrier image.

4.1. The appearance of the encrypted image

The appearance of the final encrypted image will change with the selected carrier image. The proposed scheme can not only embed secret images into gray carrier images of different sizes, but also can be used for color image encryption. The three channels of the color image are separated, and each channel is encrypted according to the gray image processing method described above. Finally, combine the secret carriers of the three channels together to generate the final color image encryption. Figure 5 is an example of the proposed scheme, the first line shows the secret image, the carrier image, the final encrypted image, and the reconstructed secret image, respectively, and the second line is the histograms of the corresponding images. From the experimental results we can see that there is almost no difference in histograms between the carrier and the final encrypted images. That is, the two pictures are resemble in the human visual system and will not cause people's doubt.

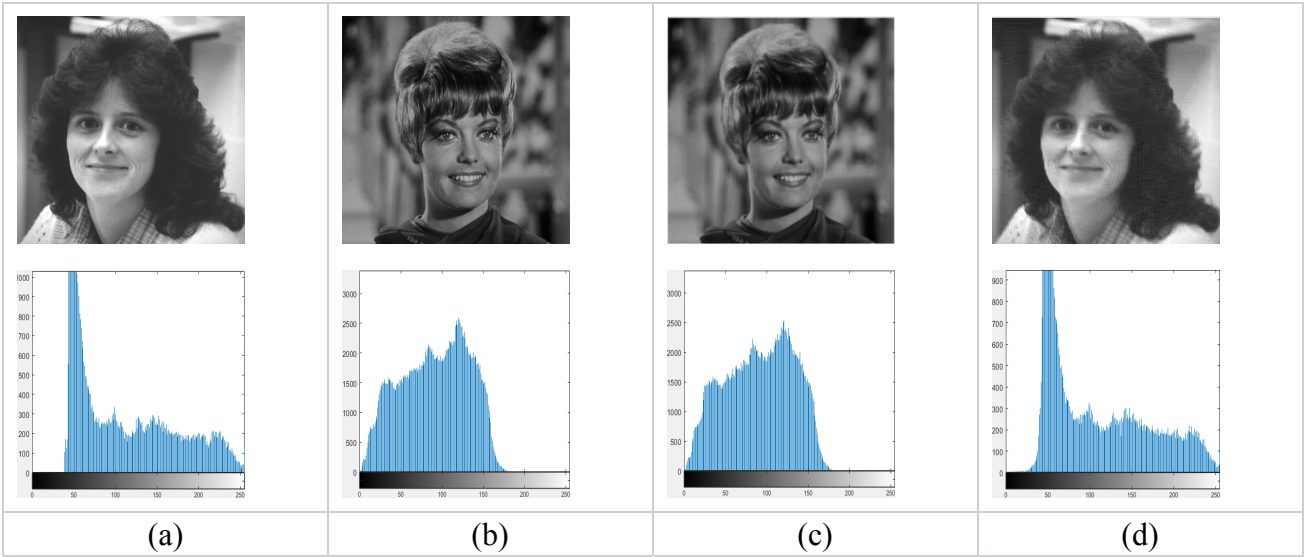
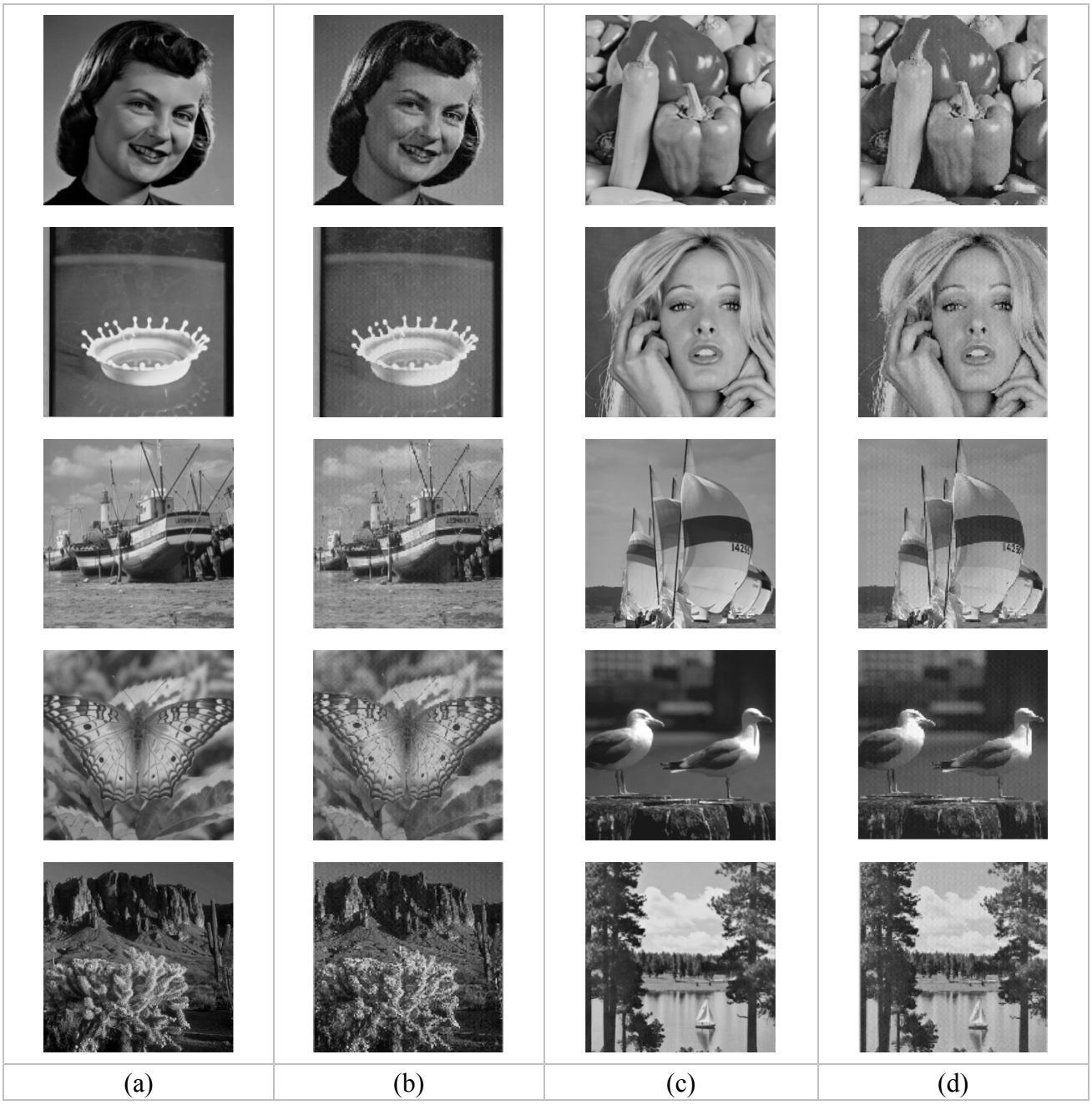


Figure 5. The first line is the secret image, the carrier image, the encrypted image and the reconstructed image; the second line is the corresponding histograms of the images.

As shown in Figure 6, we randomly selected five groups of the secret images (girl face, milk drop, boat, butterfly and hill) and the carrier images (pepper, sailing, boat, birds, and lake) to show the final encrypted images obtained by our algorithm and the BZ scheme [29]. The results of the two algorithms are slightly different, and our method has a better visual effect.

As Zeng et al. mentioned in [38], the gray histogram counts the frequency of all pixels in the image according to the gray value, if the histograms of the two images are close, they can be considered to be visually similar. To show the difference between the final encrypted image and the carrier image

more clearly, we calculate the difference between their histograms, as shown in Figure 7, which indicates that the overall effect of the proposed algorithm is better than the BZ scheme [29]. This is because the value of prediction error is smaller than the pre-encrypted image, so the impact of the replacement on the carrier image is small, which can improve the visual quality of the encrypted image.



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

Figure 6. The final encrypted images of BZ and the proposed schemes. The odd columns (a) and (c) are the results of the proposed scheme, and the even columns (b) and (d) are the results of BZ scheme.

4.2. Image quality evaluation

To evaluate the visual quality of the encrypted image, we mainly use two common image quality

evaluation standards, Peak signal to noise ratio (PSNR) and structural similarity (SSIM) [39]. PSNR is an objective standard to evaluate the image. The larger the PSNR value is, the less distortion is. SSIM is an index to measure the similarity of two images in brightness, contrast and structure, and the closer the value of SSIM is to 1, the more similar the two images are. The calculation formulas are listed as follows

$$\mathrm{PSNR}(\mathrm{C},\mathrm{E}) = 10\log_{10}\frac{255^2\times \mathrm{M}\times \mathrm{N}}{\sum_{\mathrm{i}=1}^{\mathrm{M}}\sum_{\mathrm{j}=1}^{\mathrm{N}}(\mathrm{H}(\mathrm{i},\mathrm{j})-\mathrm{C}(\mathrm{i},\mathrm{j}))^2} \tag{10}$$

where the image's size is $\mathrm{M}\times\mathrm{N}$, $\mathrm{C}(\mathrm{i},\mathrm{j})$ and $\mathrm{E}(\mathrm{i},\mathrm{j})$ are the pixel value of the carrier image and the final encrypted image, respectively. Then, the similarity between the secret image S and the reconstructed secret image R is calculated by SSIM [39], and it is based on luminance, contrast and structure, and here is the specific equation:

$$\mathrm{SSIM}(\mathrm{S},\mathrm{R}) = \frac{(2\mu_{\mathrm{S}}\mu_{\mathrm{R}}+c_1)(2\sigma_{\mathrm{SR}}+\mathrm{c}_2)}{(\mu_{\mathrm{S}}^2+\mu_{\mathrm{R}}^2+c_1)(\sigma_{\mathrm{S}}^2+\sigma_{\mathrm{R}}^2+\mathrm{c}_2)} \tag{11}$$

where, μ_S and μ_R are the mean of images S and R, σ_{S} and σ_{R} are the variance of images S and R, σ_{SR} is the covariance of S and R, c_1 and c_2 are constants to avoid denominators becoming zero, $\mathrm{c}_1=(\mathrm{k}_1\times\mathrm{l})^2$, $\mathrm{c}_2=(\mathrm{k}_2\times\mathrm{l})^2$, usually, $\mathrm{k}_1=0.01, \mathrm{k}_2=0.03$ and $\mathrm{l}=255$.

In addition to the above two typical quality evaluation criteria, we introduce a new method called the Two Dimensional-Detrended fluctuation analysis (2D-DFA) to further analyze the image [43]. Suppose the size of an image I is $\mathrm{M}\times\mathrm{N}$, dvide I into $\mathrm{M}_\mathrm{s}\times\mathrm{N}_\mathrm{s}$ non-overlapping blocks of the same size $\mathrm{s}\times\mathrm{s}$, where, $\mathrm{M}_\mathrm{s}=\mathrm{M}/\mathrm{s}$, and $\mathrm{N}_\mathrm{s}=\mathrm{N}/\mathrm{s}$. The detrended fluctuation of the image I can be calculated as:

$$\mathrm{F}^2(\mathrm{s}) = \frac{1}{\mathrm{M}_\mathrm{s}}\frac{1}{\mathrm{N}_\mathrm{s}}\sum_{\mathrm{v}=1}^{\mathrm{M}_\mathrm{s}}\sum_{\mathrm{w}=1}^{\mathrm{N}_\mathrm{s}}\mathrm{F}^2(\mathrm{v},\mathrm{w},\mathrm{s}) \tag{12}$$

where, $\mathrm{F}^2(\mathrm{v},\mathrm{w},\mathrm{s})$ is the detrended fluctuation of each sub-block.

To evaluate the fractal scale characteristics of the image, $\mathrm{F}^2(\mathrm{s})$ should be displayed as power law scale:

$$\mathrm{F}^2(\mathrm{s})\sim\mathrm{s}^{\alpha} \tag{13}$$

where α is a scaling exponent, and when the α of the final encrypted image is closer to that of the carrier image, the visual quality of final encrypted image will be better [43].

Figure 8 shows the PSNR and SSIM of 50 pairs of randomly selected carrier images and the corresponding final encrypted images [41]. As can be seen from Figure 8, the data obtained by our scheme is generally better than that of the BZ algorithm. The average values of these 50 groups of results are recorded in Table 1. The results show that compared with BZ scheme [29], the PSNR and SSIM of this scheme are improved by 3.421 db and 0.0269, respectively.

Table 1. The average result of 50 random test images.

Algorithm	SSIM	PSNR (dB)
BZ scheme	0.9365	28.596
Proposed scheme	0.9634	32.017

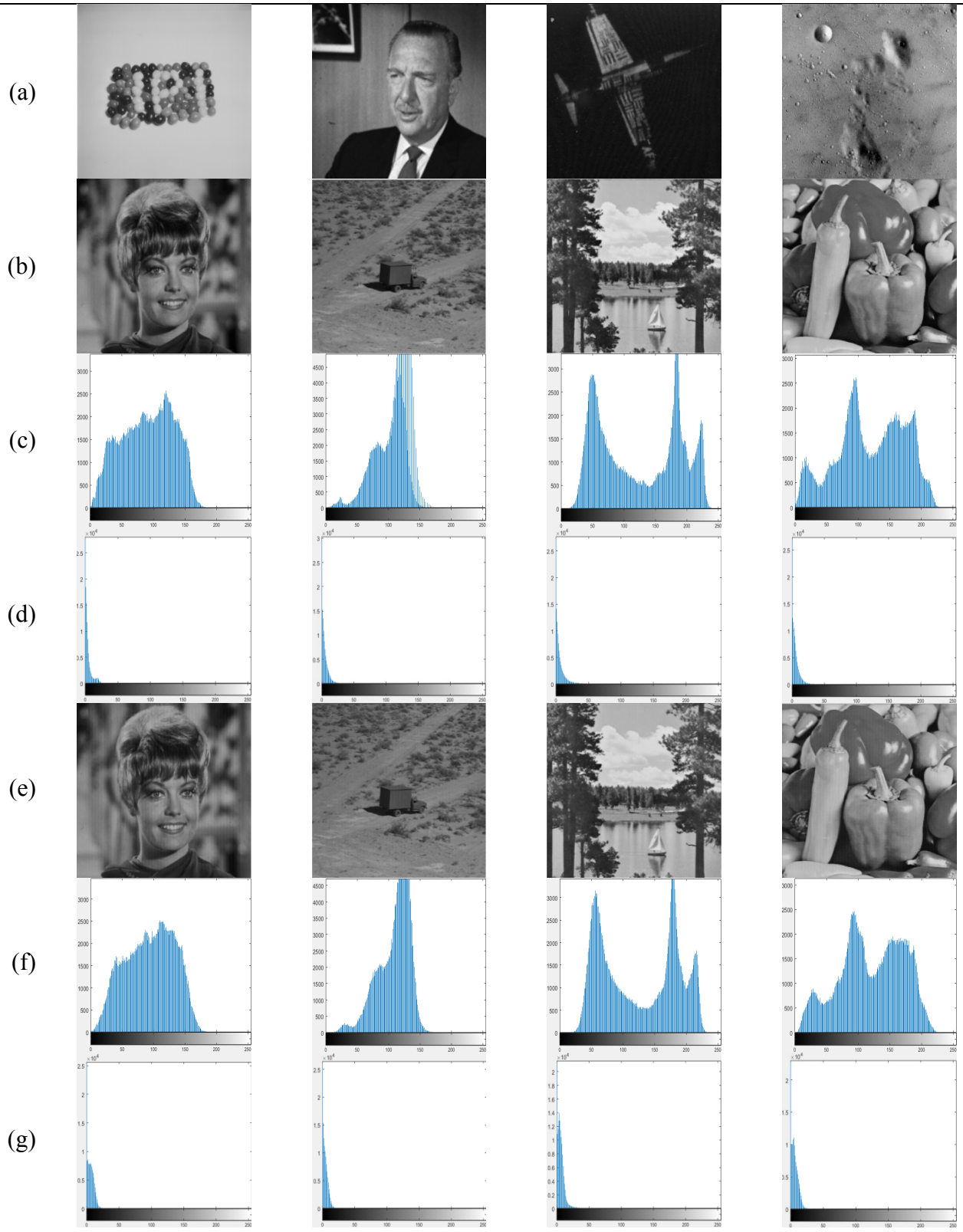
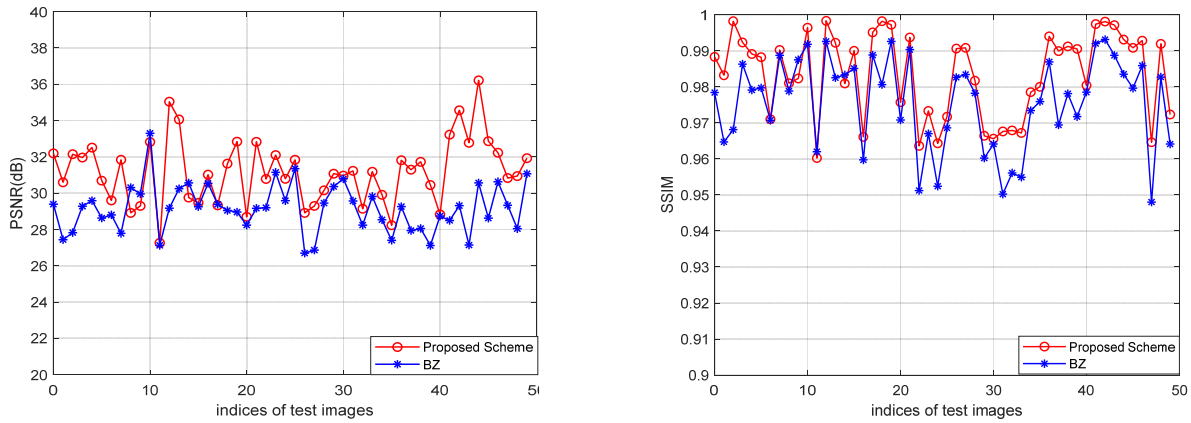


Figure 7. From the first to the seventh lines are: (a) four secret images; (b,c) the final encrypted images and its histograms; (d) the difference histograms of the carrier and final encrypted images; (e,f) the encryption results of BZ scheme and its histograms; (g) the difference histograms of the carrier and final encrypted images.



(a) (b)

Figure 8. PSNR and SSIM comparison of the carrier and final encrypted images.

Table 2. Visual evaluation results of reconstructed images.

Secret image	Carrier image	PSNR (dB)	SSIM
Woman	Lena	32.8463	0.9956
Gray	Air plane	35.1514	0.9846
Tank	Milk drop	28.9360	0.9875
Girl face	Gold hill	34.7419	0.9820
Clown	Trucks	28.4238	0.9528
Zelda	Candy	32.4504	0.9875
Fruits	Tree	27.4208	0.9865
Bee	Air plane	35.0504	0.9843
Bird	Estatua	28.4238	0.9528
Yacht	House	32.4290	0.9874
Average		31.5874	0.9801

The quality of extracted secret image also evaluates the algorithm. We use the images in Table 2 to discuss the reconstruction ability of the proposed method. The PSNR and SSIM of the reconstructed secret image in Table 2 is 31.5874db and 0.9801, respectively, therefore, the reconstructed images are visually acceptable.

Although PSNR is considered as an objective index of encrypted images, there are some defects occasionally. To make up for this shortcoming, 2D-DFA is used to further analyze the encrypted image and compare it with the BZ scheme [29]. Table 3 shows that the proposed algorithm is superior to BZ scheme [29] under different image evaluation standards for the images in Table 2. Although fluctuation function $F^2(s)$ present similar values for the two schemes, the scaling exponent α of the encrypted image obtained by our scheme is more similar than the BZ scheme [29].

4.3. Security analysis

In this section, we will analyze the security of the proposed method in terms of secret key sensitivity, noise attack and anti-clipping attack.

4.3.1. Key sensitivity analysis

Generally speaking, the key security mentioned in the image encryption system mainly refers to that in the process of decryption and image reconstruction, it has a significant impact on the recovery of secret image. In this paper, we use the AES algorithm to encrypt the prediction error, and choose the key = ($[K_t, K_p]$). Where, K_t is the encryption key of AES and K_p is the parameter of integer wavelet. We set K_t = [60,46,98,30,45,90,105,78], K_p = db1. In the process of image reconstruction, we consider the influence of the subtle changes of keys to the experimental results. We first keep the K_p unchanged, and use $key_1 = ([K_{t1}, K_p])$ to decrypt the image, where K_{t1} = [56,46,98,30,45,90,105,78]. Then, keep the K_t unchanged, and use $key_2 = ([K_t, K_{p2}])$ for decryption, where $K_{p2} = db3$. The correct key can recover the secret image, but only the tampered image can be obtained by slightly modifying the key set, as shown in Figure 9.

Table 3. Comparison with the BZ scheme [29] under different image evaluation method.

PSNR		SSIM		α		
BZ [29]	Proposed	BZ [29]	Proposed	Carrier image	BZ [29]	Proposed
30.6381	35.4325	0.9514	0.9855	1.7296	1.7837	1.7294
31.1496	36.7506	0.9599	0.9942	1.6533	1.6809	1.6533
29.4083	33.6058	0.9538	0.9637	2.3407	2.3483	2.3412
30.8539	35.4803	0.9591	0.9869	2.0818	2.0842	2.0813
28.4904	34.9240	0.9512	0.9760	2.1153	2.1469	2.1027
30.5042	35.3548	0.9542	0.9804	1.8038	1.8076	1.8042
27.4208	32.3308	0.9469	0.9527	2.2784	2.2798	2.2780
28.0504	34.6295	0.9507	0.9718	2.2909	2.2972	2.2925
29.4238	35.3982	0.9493	0.9841	1.8172	1.8936	1.8175
27.4290	32.7326	0.9438	0.9552	2.3258	2.3762	2.3203

4.3.2. Noise attack

As is known to all, in the process of image transmission and processing, images are inevitably contaminated by various noises [40,42]. For this purpose, we add different degrees of Gaussian noise, salt and pepper noise and speckle noise into the final encrypted image, and then analyze whether the proposed method can recover the secret image. As can be seen from Figure 10, adding 0.001% noise, the reconstructed secret image has different degrees of visual damage, and Gaussian noise has the greatest impact on the image, but the outline of the secret image is still clear and visible. Table 4 shows the comparison of performance between the proposed scheme and BZ scheme [29] under different kinds of noise attacks. From Table 4, we can observe that even after the noise attack and the cutting attack, the image quality of the proposed method is better than that of the BZ scheme both in encryption process and decryption.

4.3.3. Different degree of clipping attack

In addition, the image may be subject to cropping attacks during image transmission, we apply

64×64 and 128×128 cropping attacks to the secret carrier image, and then reconstruct the secret image. Figure 11 shows us the cropped encrypted images and the corresponding reconstructed images and Table 4 shows that the visual quality of the secret image is acceptable even though a large amount of data is cropped.

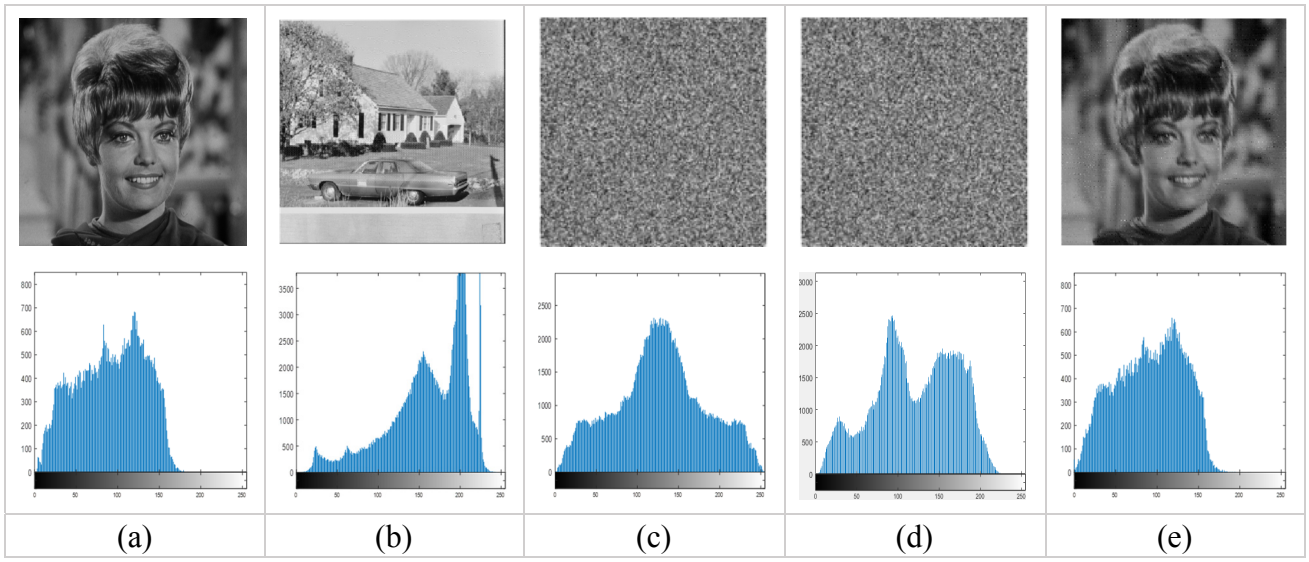


Figure 9. Key sensitivity test. Column (a) is the secret image and its histogram, (b) is the encrypted image and its histogram, (c) and (d) are the garbled image obtained by wrong keys and (e) is the image reconstructed with the correct key.

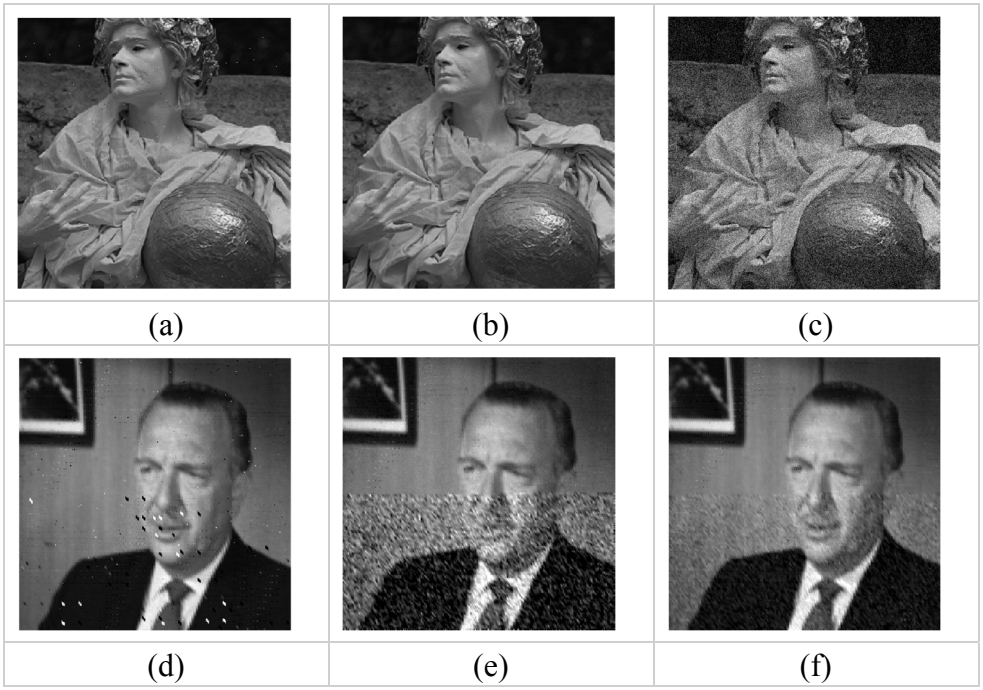


Figure 10. Noise attack experiments. (a–c): Add 0.001% salt and pepper noise, speckle noise and Gaussian noise into the final encrypted image; (d–f): reconstructed image from the noisy image.

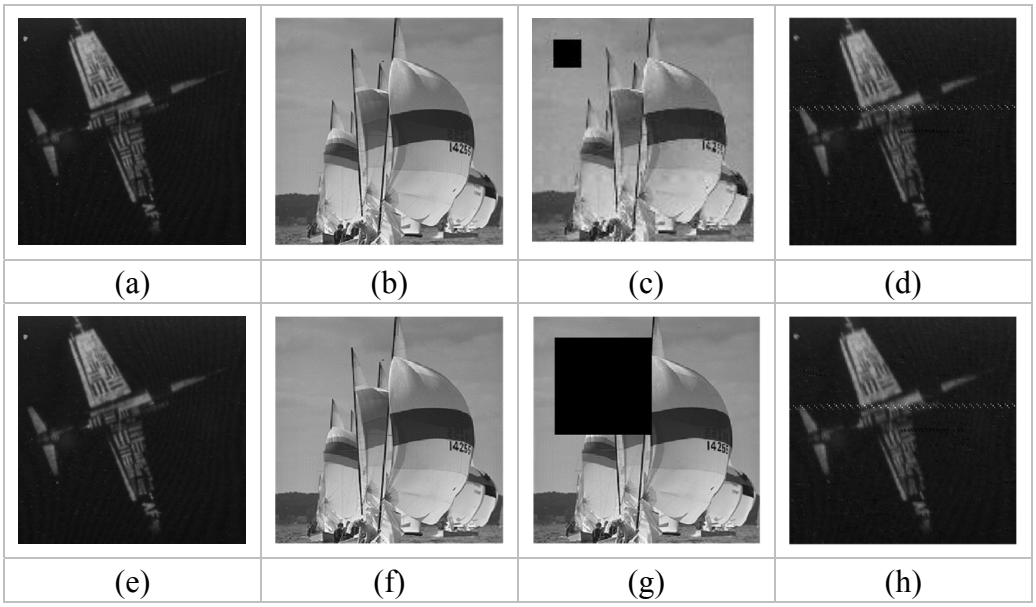


Figure 11. Different degrees of cropping attacks and restored images. (a) and (e): secret image airplane; (b) and (f): the final encrypted image sailing; (c) and (g): the final encrypted image with 64×64 and 128×128 loss; (d) and (h): restored images.

Table 4. The results of different types and degrees of attacks on the final encrypted images, a represents the encrypted image and b represents the recovered secret image.

Attacks	Our method				BZ scheme [29]			
	$PSNR^a$	$SSIM^a$	$PSNR^b$	$SSIM^b$	$PSNR^a$	$SSIM^a$	$PSNR^b$	$SSIM^b$
Salt and pepper noise	28.7762	0.9433	27.6284	0.9263	28.6284	0.9263	27.2488	0.9013
Speckle noise	27.5826	0.9005	22.5257	0.7425	21.5257	0.7425	19.6210	0.6625
Gaussian noise	25.7414	0.8352	23.3082	0.8268	23.3082	0.8268	20.3451	0.7104
64×64 data cutting	28.0570	0.9273	27.6201	0.9635	27.6201	0.9635	26.5394	0.8690
128×128 data cutting	24.2238	0.7647	23.0592	0.9110	28.0592	0.9110	26.8405	0.8873

Table 5. Comparison of computation time of encryption and decryption steps.

Secret image	Carrier image	Process	BZ scheme	Proposed scheme	Difference
Girl face	Gold hill	Encryption	25.9486	26.9253	0.9767
		Decryption	36.9262	36.9701	0.0439
Fruits	Tree	Encryption	25.9137	26.8302	0.9165
		Decryption	36.8964	36.9983	0.0619
Zelda	Candy	Encryption	25.9228	26.8936	0.9708
		Decryption	36.8985	36.9698	0.0713
Average		Encryption	25.9283	27.0611	0.9547
		Decryption	36.9070	36.9577	0.0590

4.3.4. Running time and computation complexity analysis

Running time and computation complexity are two important standards to measure the algorithm. In this part, we will compare the computation time between the BZ scheme [29] and our algorithm both in encryption and decryption process. For the fairness, we use the same pre-encryption algorithm in BZ scheme and this paper, i.e., AES encryption method, and change the key to do the test. Table 5 shows the experimental results. We can see that the difference of encryption time and decryption time between the two methods is 0.9547 and 0.0590 respectively. The time difference is acceptable, and the computation complexity of this paper is similar to that of BZ scheme.

5. Conclusions

This paper proposes a visual secure image encryption algorithm, which not only improves the visual quality of the final encrypted image, but also restores the secret image. In the proposed method, the rhombus predictor is used to calculate the prediction value of the secret image. The prediction error value is far less than the secret variable value, so it improves the visual quality of the final encrypted image to a certain extent. Visually meaningful image encryption can well protect the image and the encrypted image can be transmitted safely in the channel without the suspicion of the attacker, moreover, the secret image extraction is independent of the carrier image, which increases the usability of the proposed scheme. In the future work, we are committed to the application of the method for privacy protection of the internet users.

Conflict of Interests

The authors declare that they have no conflict of interests.

Acknowledgements

This work is supported by the National Key R&D Program of China under grant 2018YFB1003205; by the National Natural Science Foundation of China under grant U1836208, U1536206, U1836110, 61972207, 61602253, 61672294; by the Engineering Research Center of Digital Forensics, Ministry of Education; by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) fund; by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) fund, China.

Reference

1. D. D. Hou, W. M. Zhang, N. Yu, Image camouflage by reversible image transformation, *J. Visual Commun. Image Representation*, **40** (2016), 225–236.
2. G. R. Chen, Y. B. Mao, C. K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, *Chaos Solitons Fractals*, **21** (2004), 749–761.
3. M. Mollaeefar, A. Sharif, M. Narazi, A novel encryption scheme for colored image based on high level chaotic maps, *Multimed Tools Appl.,* **76** (2017), 607–629.

4. D. Xiao, J. Liang, Q. Ma, Y. Xiang, Y. Zhang, High capacity data hiding in encrypted image based on compressive sensing for nonequivalent resources, *Comput. Mater. Continua*, **58** (2019), 1–13.
5. J. Fridrich, M. Goljan, R. Du, Detecting LSB steganography in color and gray-scale images, *IEEE Multimedia*, **8** (2001), 22–28.
6. S. Husien, H. Badi, Artificial neural network for steganography, *Neural Comput. Appl.*, **26** (2015), 111–116.
7. J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, *Int. J. Bifurcation Chaos,* **8** (1998), 1259–1284.
8. G. Gu, L. Jie, A fast image encryption method by using chaotic 3D cat maps, *Optik Int. J. Light Electron Optics,* **125** (2014), 4700–4705.
9. Z. H. Guan, F. Huang, W. Guan, Chaos-based image encryption algorithm, *Phys. Lett. A,* **346** (2005), 153–157.
10. J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, et al., Report on the development of the Advanced Encryption Standard (AES), *J. Res. Natl. Inst. Stand. Technol.,* **106** (2001), 511–577.
11. Z. Y. Xia, L. H. Liu, H. J. Shim, X.Y. Chen, B. Jeon, A privacy-preserving image retrieval based on AC-Coefficients and color histograms in cloud environment, *Comput. Mater. Continua*, **58** (2019), 27–43.
12. L. Teng, X. Wang, J. Meng, A chaotic color image encryption using inter grated bit-level permutation, *Multimed Tools Appl.*, **77** (2018), 6883–6896.
13. M. Ahmad, O. Farooq, *Secure satellite images transmission scheme based on chaos and discrete wavelet transform*, International Conference on High Performance Architecture and Grid Computing, Springer, Berlin, Heidelberg, 2011.
14. L. Xiong, Z. Xu, Y. Q. Shi, An integer wavelet transform based scheme for reversible data hiding in encrypted images, *Multidimens. Syst. Signal Process.*, **29** (2018), 1191–1202.
15. G. D. Ye, K. X. Jiao, H. Wu, C. Pan, X. Huang, An asymmetric image encryption algorithm based on a fractional-order chaotic system and the RSA public-key cryptosystem, *Int. J. Bifurcation Chaos*, **30** (2020), 2050233.
16. G. D. Ye, C. Pan, Y. X. Dong, Y. Shi, X. L. Huang, Image encryption and hiding algorithm based on compressive sensing and random numbers insertion, *Signal Process.*, **172** (2020), 107563.
17. X. L. Huang, Y. X. Dong, K.X. Jiao, G. D. Ye, Asymmetric pixel confusion algorithm for images based on RSA and Arnold transform, *Front. Inf. Technol. Electron. Eng.*, **21** (2020), 1783–1794.
18. H. S. Ye, N. R. Zhou, L. H. Gong, Multi-image compression-encryption scheme based on quaternion discrete fractional hartley transform and chaotic systems, *Signal Process.*, **175** (2020), 107652.
19. Z. Hua, Y. Zhou, C. M. Pun, C. L. P. Chen, 2D Sine logistic modulation map for image encryption, *Inf. Sci.,* **297** (2015), 80–94.
20. X. Y. Chen, H. D. Zhong, Z. F. Bao, A GLCM feature based approach for reversible image transformation, *Comput. Mater. Continua*, **59** (2019), 239–255.
21. J. Tian, Reversible data embedding using a difference expansion, *IEEE Trans. Circuits Syst. Video Technol.,* **13** (2003), 890–896.
22. J. Li, X. Li, B. Yang, X. Sun, Segmentation-Based image copy-move forgery detection scheme, *IEEE Trans. Inf. Forensics Secur.*, **10** (2015), 507–518.

23. X. Gao, C. Deng, X. Li, D. Tao, Geometric distortion insensitive image watermarking in affine covariant regions, *IEEE Trans. Syst. Man Cybern. Part C*, **40** (2010), 278–286.
24. M. L. Liu, H. S. Seah, C. Zhu, W. Lin, F. Tian, Reducing location map in prediction-based difference expansion reversible image data embedding, *Signal Process.,* **92** (2012), 819–828.
25. R. Calderbank, I. Daubechies, W. Sweldens, B. Yeo, Wavelet transforms that map integers to Integers, *Appl. Comput. Harmonic Anal.,* **5** (1998), 332–369.
26. L. L. Shen, X. F. Chen, Z. Q. Pan, K. Fan, F. Li, J. Lei, No-reference stereoscopic image quality assessment based on global and local content characteristics, *Neurocomputing*, **424** (2021), 132–142.
27. Z. Q. Pan, X. K. Yi, Y. Zhang, H. Yu, F. L. Wang, S. Kwong, Frame-level bit allocation optimization based on video content characteristics for HEVC, *ACM Trans. Multimedia Comput. Commun. Appl.,* **16** (2020), 1–20.
28. Z. Q. Pan, X. K. Yi, Y. Zhang, B. Jeon, S. Kwong, Efficient in-loop filtering based on enhanced deep convolutional neural networks for HEVC, *IEEE Trans. Image Process.*, **29** (2020), 5352–5366.
29. L. Bao, Y. Zhou, Image encryption: Generating visually meaningful encrypted images, *Inf. Sci.,* **324** (2015), 197–207.
30. M. V. D. Veen, F. Bruekers, A. V. Leest, S. Cavin, *High capacity reversible watermarking for audio*, Security and Watermarking of Multimedia Contents V, International Society for Optics and Photonics, 2003.
31. A. Kanso, M. Ghebleh, An algorithm for encryption of secret images into meaningful images, *Opt. Lasers Eng.,* **90** (2017), 196–208.
32. Y. G. Yang, Y. C. Zhang, X. B. Chen, Y. H. Zhou, W. M. Shi, Eliminating the texture features in visually meaningful cipher images, *Inf. Sci.,* **429** (2018), 102–119.
33. X. Chai, Z. Gan, Y. Chen, Y. Zhang, A visually secure image encryption scheme based on compressive sensing, *Signal Process.*, **134** (2017), 35–51.
34. M. Barni, F. Bartolini, V. Cappellini, A. Lippi, A. Piva, *DWT-based technique for spatio-frequency masking of digital signatures*, Security and Watermarking of Multimedia Contents. International Society for Optics and Photonics, 1999.
35. N. Saravanan, K. I. Ramachandran, Incipient gear box fault diagnosis using discrete wavelet transform (DWT) for feature extraction and classification using artificial neural network (ANN), *Expert Syst. Appl.,* **37** (2010), 4168–4181.
36. V. Sachnev, H. J. Kim, J. Nam, S. Suresh, Y. Q. Shi, Reversible watermarking algorithm using sorting and prediction. *IEEE Trans. Circuits Syst. Video Technol.*, **19** (2009), 989–999.
37. Boss Base Image Database, 2018. Available from: http:// agents. fel. cvut. cz/ stegodata/ RAWs.
38. M. Zeng, Y. Li, Q. Meng, T. Yang, J. Liu, Improving histogram-based image contrast enhancement using gray-level information histogram with application to X-ray images, *Optik,* **123** (2012), 511–520.
39. H. Yao, X. Liu, Z. Tang, C. Qin, Y. Tian, Adaptive image camouflage using human visual system model, *Multimedia Tools Appl.*, **78** (2019), 8311–8334.
40. Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, Image quality assessment: from error visibility to structural similarity, *IEEE Trans. Image Process.*, **13** (2004), 600–612.
41. L. Kamstra, H. J. A. M. Heijmans, Reversible data embedding into images using wavelet techniques and sorting, *IEEE Trans. Image Process.,* **14** (2005), 2082–2090.

42. Y. Luo, M. Du, J. Liu, A symmetrical image encryption scheme in wavelet and time domain, *Commun. Nonlinear Sci. Numer. Simul.,* **20** (2015), 447–460.
43. J. O. Armijo-Correa, J. S. Murguía, and M. Mejía-Carlos, V. E. Arce-Guevara, J. A. Aboytes-González, An improved visually meaningful encrypted image scheme, *Opt. Laser Technol.*, **127** (2020), 106165.

AIMS Press