Received: 29 April 2022 | Revised: 22 September 2022 | Accepted: 11 December 2022

IET Image Processing

DOI: 10.1049/ipr2.12731

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Robust image compression-encryption via scrambled block bernoulli sampling with diffusion noise

Zan Chen[1] | Chaocheng Ma[1] | Tao Wang[1] | Yuanjing Feng[1] | Xingsong Hou[2] | Xueming Qian[2]

[1]College of Information Engineering, Zhejiang University of Technology, Hangzhou, China

[2]School of Information and Communication Engineering, Xi'an Jiaotong University, Xi'an, China

Correspondence
Yuanjing Feng, College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China.
Email: fyjing@zjut.edu.cn

Funding information
National Natural Science Foundation of China, Grant/Award Numbers: 61872286, 61976190, 62002327, 62073294; Natural Science Foundation of Zhejiang Province, Grant/Award Numbers: LQ21F020017, LZ21F030003; Agricultural and Social Development Foundation of Hangzhou, Grant/Award Number: 202004A07

Abstract

This paper proposed an image compression-encryption scheme based on compressive sensing theory, which achieves high security, strong robustness, and high rate-distortion performance. First, the denoising preprocessing strategy is applied at the encoder side, which can enhance the rate-distortion performance without sacrificing security and robustness. Second, the preprocessed image is randomly down-sampled using scrambled block Bernoulli sampling with diffusion noise (SBBS-DN), which is generated by combining a hyper-chaotic system and SHA256 hash of the plain image. Third, a deep-learned plug-and-play is embedded prior for plain image reconstruction at the decoder side. Simulation results show that the proposed scheme has desirable security performance (being resistant to different attacks), high R-D performance (PSNR gains over 1.3 dB than JPEG at 0.50 bpp compression ratio), and high error resilience (reconstructed 29.92 dB at 0.50 bpp compression ratio even with 50% bit loss).

1 | INTRODUCTION

As information technology progresses, a large number of digital images are generated, transmitted, and stored. Transmitting digital images is vulnerable to privacy issues such as information leakage and data tampering. Thus, such explosive increasing demand in image communication desires effective privacy-preserving techniques to ensure data security during transmission [1].

Many image encryption algorithms have been developed with various techniques, such as bit-level permutation [2–4], one-time keys [5–7], DNA rule [8–10], logistic map [11–13], and so on. For instance, Dou et al. [4] explored bit-level permutation within the discrete wavelet transform domain to improve the security of encrypted images. Rehman et al. [5] performed image encryption by utilizing one-time keys and the pseudo-rotor substitution machine. Farah et al. [8] proposed an optical image encryption scheme that combines fractional Fourier transform and DNA sequence operation. Zhou et al. [11] proposed an image encryption scheme by combining the logistic map and sine map. However, these image encryption schemes do not take into account the rate-distortion performance. Besides, these encryption schemes are not sufficiently resistant to bit error or bit loss in transmission. Error or loss of a few bits in traditional image coding schemes would result in incorrect image reconstruction.

Compressive sensing (CS) is an emerging light-weight and robust image coding scheme, where image compression and encryption can be realized simultaneously [14, 15]. In the CS measurement process, a meaningful plain image is transformed into a noise-like cipher image with a high level of confidentiality guarantee [16]. The secrecy of the CS-based image coding scheme has been formally analyzed in [17, 18], proving the adequate computational security of CS to resist common attacks.

Except for the outstanding privacy-preserving property, CS-based encryption schemes have another two advantages over traditional image compression schemes [19]. First, CS has an easily implemented encoder that requires a little computing resource. Only a simple randomly down-sampled operation is needed for data compression. Second, it is robust to bit error or loss in transmission. The CS measurements are the democracy

descriptions of the original signal, which makes the encrypted bitstream robust both in the binary erasure channel and binary symmetric channel.

CS-based image encryption schemes have been intensively investigated in recent years. For instance, Zhou et al. [20] proposed a CS-based image encryption scheme by combining cosparse representations, random pixel exchanging, and discrete fractional angular transformation. Chai et al. [21] introduced a CS-based image encryption scheme using the memristive chaotic system, elementary cellular automata. Zhang et al. [22] embedded orthogonal-basis CS measurement matrics into random phase encoding, which can compress multiple images parallelly into stochastic noise-like signals. Chen et al. [23] introduced scrambled block random sampling for CS-based image coding together with a patch-based CS reconstruction algorithm. However, all these CS-based image encryption schemes still suffer from poor rate-distortion performance (close to or lower than JPEG), which limits their widespread use in image transmission.

To address the rate-distortion performance gap meanwhile ensuring high security and strong robustness, this work proposes an image compression-encryption scheme by combining scrambled block Bernoulli sampling with diffusion noise, dilated residual channel attention network (DRCAN) prior, and preprocessing strategy. We conducted extensive experiments to demonstrate our performance in compression, encryption, and robustness performance. Experimental results show that the proposed CS-based coding scheme has convincing security performance (passing all 17 NIST tests and being resistant to differential attack), high R-D performance (PSNR gains over 1.3 dB than JPEG at 0.50 bpp compression ratio), and high error resilience (reconstructed 29.92 dB even with bit loss probability 50% at 0.50 bpp compression ratio). The main contributions of this paper are summarized as follows:

First, we design a simple but efficient scrambled block Bernoulli sampling with diffusion noise to encrypt the original image.

Second, we embed a state-of-the-art deep-learned plug-and-play prior for plain image reconstruction.

Third, we introduce a denoiser to preprocess the original image at the encoder side.

The remainder of this paper is organized as follows. Section 2 introduces the background of CS measurement and CS reconstruction algorithms. Section 3 illustrates an overview of the proposed scheme. The details of the proposed CS encryption process are presented in Section 4. Section 5 introduces the deep-learned plug-and-play prior used for image recovery. The CS preprocessing strategy is presented in Section 6, followed by experimental results in Section 7. Section 8 offers conclusions.

2 | BACKGROUND

2.1 | CS measurement for image encryption

Compressive sensing states that a sparse or compressible signal $x \in R^n$ can be accurately reconstructed from its m random linear measurement results $y \in R^m$, that is,

$$y = \Phi x, \tag{1}$$

where $\Phi \in R^{m \times n} (m << n)$ is the CS measurement matrix [24]. The measurement matrix Φ is related to the encryption effect, encoding complexity, and reconstruction performance.

One well-designed measurement matrix should satisfy the restricted isometric property for CS as well as the security requirements of uncertainty, unpredictability, and nonrepeatability [25]. Although a completely random matrix can offer optimal image reconstruction performance, it suffers from high computational complexity, huge storage, and low efficiency in practical implementations.

Block-based measurement matrix generated from the Chaos system offers an effective alternative way for CS-based image encryption [26]. A simple recurrence chaos equation can produce complex sequences from initial values and a slightly disturbed initial value can generate a completely different measurement matrix. Therefore, it only needs to save and transmit initial values instead of the entire measurement matrix, which can save storage and bandwidth.

2.2 | CS reconstruction for image decryption

Since CS reconstruction is an ill-posed inverse problem, it requires some prior knowledge to constrain the solution space [27, 28]. CS enables the reconstruction of an image by solving the following unconstrained optimization problem

$$x = \arg\min_{x} \|\tilde{y} - \Phi x\| + \lambda R(x), \tag{2}$$

where $\|\tilde{y} - \Phi x\|$ is the fidelity term, $R(x)$ is the regularization term, and λ is an appropriate regularisation parameter.

Based on the type of regularization $R(\cdot)$, the CS reconstruction algorithm can be mainly classified into hand-crafted algorithms and deep-learned algorithms. The popular hand-crafted regularization terms usually involve some manually chosen parameters, which are hard to determine. Deep-learned prior can be implicitly defined by replacing some components in hand-crafted prior algorithms with plug-and-play deep neural networks [29]. For instance, ISTANet replaces the soft-thresholding step in the traditional iterative soft-thresholding algorithm with a learning-based threshold operator [30]. LDAMP uses a convolutional neural network to realize the image denoising step in D-AMP algorithms [31]. Here, we embed a tailored DRCAN prior to the image decryption at the decoder side, which can improve the R-D performance fundamentally.

3 | OVERVIEW OF THE PROPOSED SCHEME

The diagram of the proposed CS-based compression-encryption scheme is shown in Figure 1. At the encoder

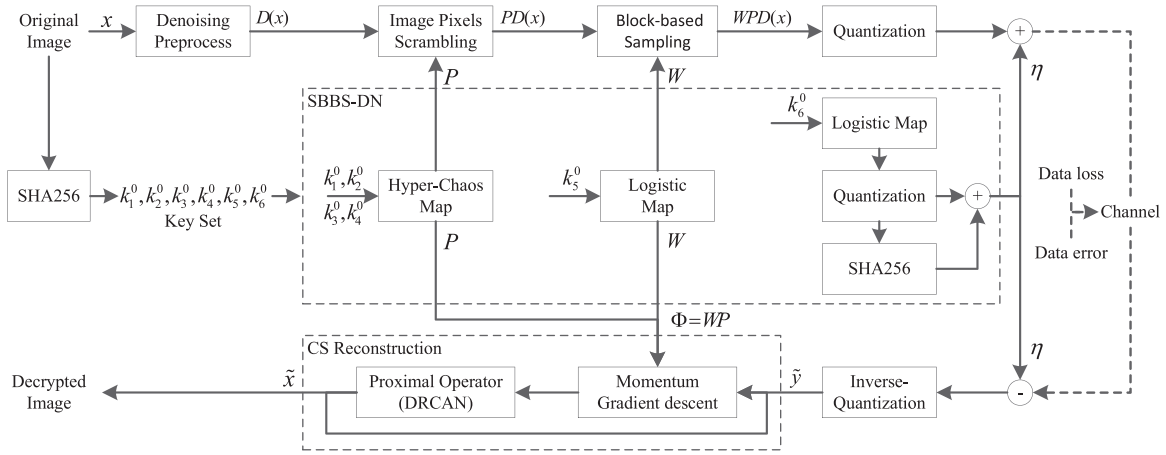

FIGURE 1 Architecture of the proposed CS compression-encryption scheme

side, we first adopt a deep-learned denoiser to preprocess the input plain image. Then, we utilize the scrambled block Bernoulli sampling with diffusion noise (SBBS-DN) to measure the preprocessed plain image. The overall image encoding process can be expressed as

$$\text{Cipher} = \text{mod}(\text{Q}_b(\Phi D(x)) + \eta, 2^b), \tag{3}$$

where Φ, η, $\mathcal{Q}_b(\cdot)$, and $D(\cdot)$ refer to the SBBS matrix, diffusion noise, b-bit quantizer, and preprocessing operation. Specifically, the SBBS matrix is composed of block measurement matrix W and pixel scrambling matrix P, which are generated based on the logistic map and hyper-chaos map, respectively, and the diffusion noise η is generated by a recurrent procedure combining SHA256 and the logistic map. Thus, we can synchronize and generate the measurement process on both the encoder side and the decoder side by transmitting only six secret keys $\{k_1^0, k_2^0, k_3^0, k_4^0, k_5^0, k_6^0\}$.

The decoder can synthesize the same CS measurement matrix as the encoder uses if receiving the correct secret keys. Then, the decoder exploits the designed DRCAN as a plug-and-play prior to the reconstruction of plain images. The overall decoding process can be expressed as

$$\tilde{x} = \text{CS}^{-1}(\text{Q}_b^{-1}(\text{mod}(\text{Cipher} - \text{j}, 2^b))), \tag{4}$$

where $\text{CS}^{-1}(\cdot)$ and $\text{Q}^{-1}(\cdot)$ refer to the applied CS reconstruction algorithm and b-bit inverse-quantizer. In the following sections, we will give more details on the above main parts of the proposed compression-encryption schemes, that is, the chaotic system to create the SBBS-DN, the deep-learned prior for CS reconstruction, and the denoising preprocessing strategy.

4 | SBBS-DN FOR IMAGE COMPRESSION-ENCRYPTION

The proposed compression-encryption encoder is based on the construction of the measurement matrix Φ and diffusion noise η. To simplify the encoding complexity, we split the CS measurement matrix Φ into a product of two matrices

$$\Phi = WP, \tag{5}$$

where $P \in R^{n\times n}$ is a sparse matrix with only one $'1'$ per column and row, and $W \in R^{m\times n}$ is a block diagonal

$$W = \begin{bmatrix} W_B & & 0 \\ & \ddots & \\ 0 & & W_B \end{bmatrix}. \tag{6}$$

Specifically, we take a $\lfloor \frac{mB}{n} \rfloor \times B$ size partial Bernoulli matrix as W_B, in which all elements are either $+1$ or -1 with 50% probability. In this way, the designed SBBS-DN only requires pixel permutation operation and add/sub-operation, which is simple to run.

4.1 | From the input image to the chaotic sequence

The proposed chaotic system applies three independent chaotic maps to generate chaotic sequences for the corresponding measurement matrices and diffusion noise, that is,

$$\begin{cases} \dot{k}_1 = a(k_2 - k_1) + k_4 \\ \dot{k}_2 = ck_1 - k_1k_3 - k_2 \\ \dot{k}_3 = k_1k_2 - bk_3 \\ \dot{k}_4 = dk_4 - k_2k_3 \\ \dot{k}_5 = (e-1)k_5 - ek_5^2 \\ \dot{k}_6 = (f-1)k_6 - fk_6^2 \end{cases}, \tag{7}$$

where the first four equations are the hyper-chaotic Lorenz system, and the last two equations are two independent logistic systems. In the system, we use the Runge–Kutta method with a suitable step length to solve the first four ordinary differential

equations (ODE) and utilize the Euler method with a fixed step length to solve the last two ODE. In this way, our encryption system can generate six pseudo-random sequences $\{k_1^i\}, \dots, \{k_6^i\}$ with the initial conditions $\{k_1^0, \dots, k_6^0\}$.

Furthermore, we use the SHA256 result of the input image as the initial value for the applied chaotic system. Considering that Equation (7) requires six initial values and the SHA256 function outputs 256 bits each time, we pick the first 192 bits to form six 32-bit depth values and then de-quantize these 32-bit depth values uniformly into the prescribed interval of the chaotic system (i.e. $k_1^0 \in (1, 81)$, $k_2^0 \in (-250, 250)$, $k_3^0 \in (0, 0.5)$, $k_4^0 \in (0, 0.5)$, $k_5^0 \in (-40, 40)$, $k_6^0 \in (-40, 40)$).

4.2 | From the chaotic sequence to SBBS-DN

For the pixel scrambling matrix P, we first construct a new sequence $\{k_*^i\}$ by utilizing the first four generated chaotic random sequences

$$k_*^i = \begin{cases} k_1^i - \lfloor k_1^i \rfloor & \text{if } \mod\left(\lfloor k_4^i \times 10^6 \rfloor, 3\right) = 0 \\ k_2^i - \lfloor k_2^i \rfloor & \text{if } \mod\left(\lfloor k_4^i \times 10^6 \rfloor, 3\right) = 1, \\ k_3^i - \lfloor k_3^i \rfloor & \text{if } \mod\left(\lfloor k_4^i \times 10^6 \rfloor, 3\right) = 2 \end{cases} \tag{8}$$

where $\mod(\cdot)$ is the modulo operation and $\lfloor \cdot \rfloor$ is the operation rounding value toward zero. Afterward, we sort $\{k_*^i\}$ in descending order and retrieve the index sequence, denoted as $I_* = \{I_1, \dots, I_n\}$. The scrambled matrix $P \in R^{m \times n}$ can then be obtained by setting the element at position (i, j) as follows

$$P(i, j) = \begin{cases} 1 & \text{if } j = I_i \\ 0 & \text{if } j \neq I_i \end{cases}. \tag{9}$$

For the Bernoulli matrix W_B, we utilize the chaotic sequence $\{k_5^i\}$ to determine whether the element at position (i, j) is 0 or 1, that is,

$$W_B(i, j) = \begin{cases} +1 & \text{if } k_5^{i \times B + j} > 0.5 \\ -1 & \text{if } k_5^{i \times B + j} \leq 0.5 \end{cases}. \tag{10}$$

For diffusion noise η, we first uniformly quantize the chaotic sequence $\{k_6^i\}$ to 8-bit depth integer values ranging from 0 to 255. Then, we add the quantized chaotic sequences with the corresponding SHA256 results, that is,

$$\eta = Q(\{k_6^i\}) + \text{SHA256}(\text{Q}(\{k_6^i\})), \tag{11}$$

where we produce the SHA256 results of $\text{Q}(\{k_6^i\})$ by splitting $\text{Q}(\{k_6^i\})$ into the sub-sequence of length 32 and importing each of the sub-sequence into the SHA256 function.

Through the above system, both the encoder and the decoder can generate the SBBS-DN from the six initial values. Because outputs of the chaotic system are extremely sensitive to the initial values, a slight disturbance of the initial values (or the input image) would cause a huge difference in the generated measurement matrix, which makes the cipher image difficult to crack through the differential attack.

5 | DRCAN PRIOR FOR IMAGE RECONSTRUCTION

In the practical application, cipher images are packaged and transmitted to the decoder side. If having the correct secret keys, the decoder can synthesize the accurate measurement matrix Φ and diffusion noise η. Then, the decoder can yield the CS measurement $\tilde{y}$ from the received cipher image

$$\tilde{y} = \text{Q}_b^{-1}(\mod(\text{Cipher} - \eta, 2^b)). \tag{12}$$

In this work, we utilize the proximal momentum gradient descent algorithm to reconstruct the plain image from $\tilde{y}$ by alternating between the gradient descent step and the proximal operating step

$$v^k = \Phi^{\text{T}}(\Phi x^k - \tilde{y}) + \gamma^{k-1} v^{k-1}, \tag{13}$$

$$x^{k+1} = D(x^k - \alpha v^k), \tag{14}$$

$$\gamma^k = \frac{\varepsilon^{\text{T}}(D(x^k - \alpha v^k + \varepsilon) - x^{k+1})}{m}, \tag{15}$$

where α is the step size, ε is a standard normal random vector, and D is the proximal operator for regularization term R. This splitting approach is an efficient CS reconstruction framework to exploit the plug-and-play prior [31, 32]. We set the initial guess x^0 as zero and step size α as 1. By iterating from Equations (13) to (15), we can obtain the final CS reconstructed image.

In this work, we utilize a dilated residual channel attention network (DRCAN) as the proximal operator $D(\cdot)$ (see Figure 2) for CS image reconstruction [33]. DRCAN mainly composes two residual channel attention blocks (dilated RCAB), which compose eight stacked dilated channel attention layers (dilated CAL). The relative dilation factors in each dilated CALs are set to (1,2,3,4,4,3,2,1), which can expand the capacity of the receptive field.

6 | IMAGE PREPROCESSING STRATEGY

One strategy to improve CS reconstruction performance is to measure the preprocessed image (i.e. $\Phi D(x)$) instead of the original one (i.e. Φx). Such CS preprocessing strategy has been proved to be substantially equivalent to revising the CS regularization term with a linear approximation [34]. Consequently, the preprocessing operator should correspond to the regularization used for the CS reconstruction. For instance, [35] adopts the sparse-filtering preprocessing to enhance wavelet sparse regularization, and [36] adopts col-

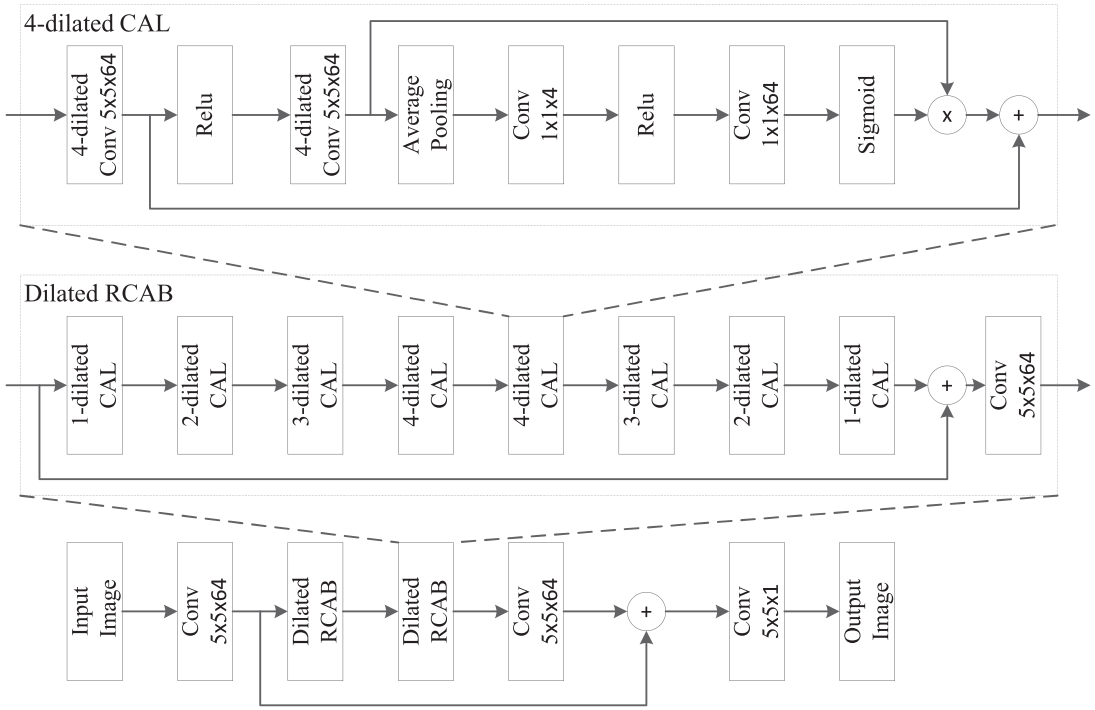

FIGURE 2 The architecture of the designed dilated residual channel attention network for proximal operator $D(\cdot)$

FIGURE 3 Test images. From left to right, the test images are Barbara, Boats, Cameraman, Foreman, House, Lena, Monarch, and Parrots

laboration reduced rank preprocessing to enhance low-rank regularization. Specifically, $D(\cdot)$ is the residual channel attention network used as the proximal operator at the decoder side. Such denoising preprocessing strategy can improve the rate-distortion performance, meanwhile maintaining the encryption and robustness properties of the CS-based coding scheme.

7 | EXPERIMENTAL RESULTS

To verify the performance of the proposed image compression-encryption scheme, we conducted extensive simulations. The measurement block size B in Equation (5) is set as 32. The parameters in Equation (7) are set as $a = 10$, $b = 8/3$, $c = 28$, $d = -1$, $e = 4$, and $f = 4$. As shown in Figure 3, eight 256×256 size images are used for the testing. We used DIV2K [37] as the training dataset to train the proximal operator $D(\cdot)$. Note that all test images are not included in the training dataset, and all PSNR results are computed between the reconstructed and the original (not the pre-processed) images.

7.1 | Encrypted and decrypted image

The encrypted images have different sizes depending on the compression ratio (CR), that is,

$$\mathrm{CR} = \frac{m \times b}{n}, \tag{16}$$

where m is the number of CS measurement; n is the pixel number of the original image; b is the quantization bit depth for each CS measurement; and units are bits per pixel (bpp). The height and width of the cipher image are equal to the number of CS measurement blocks, that is, $\frac{n}{B}$, and the number of CS measurements in each block, that is, $\lfloor \frac{mB}{n} \rfloor$, respectively. Here, we fix the quantization bit depth as 7 and control the compression ratio by adjusting m.

Figure 4 shows encoded images and decoded images of Lena and Parrots corresponding to CR = 0.25, 0.50, 0.75, and 1.00 bpp, respectively. We further compute peak signal noise ratio (PSNR)to evaluate the quality of the decrypted images. It can be seen that all ciphertexts are similar to white

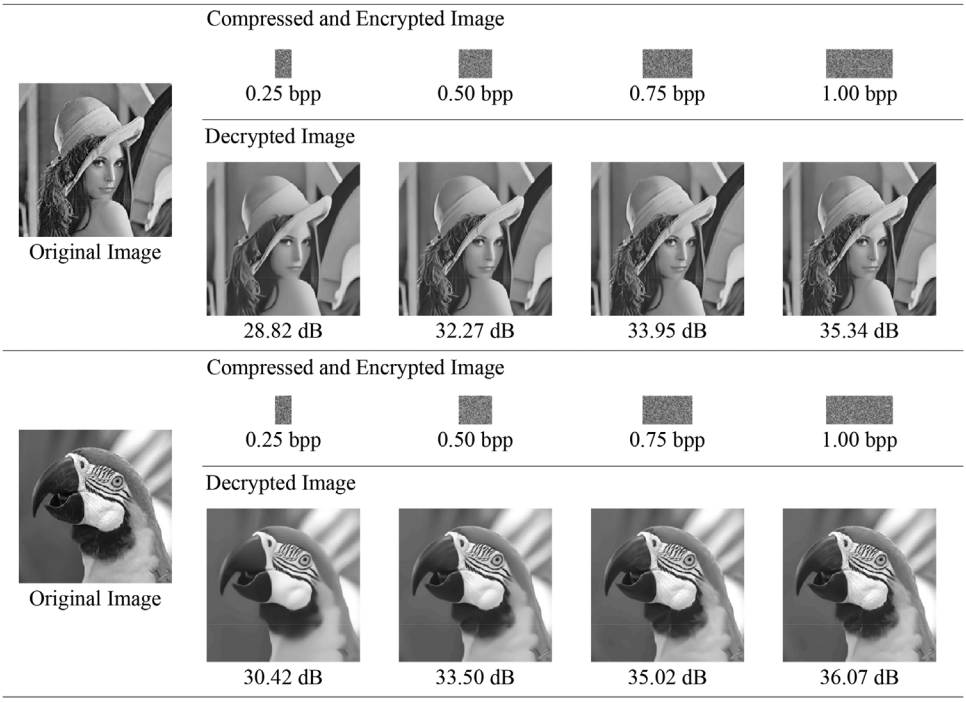

FIGURE 4 Visualization of encrypted and decrypted test images with the proposed CS compression-encryption scheme

noise, without leaking any visual perception of the original images, and the decrypted images can achieve acceptable reconstruction visual quality even at a low compression ratio of 0.25 bpp.

7.2 | Compression performance

We compare the proposed method with three popular traditional image compression standards, that is, JPEG [38], CCSDS-IDC [39], and JPEG2K [40], which do not have the image encryption capacity. Their order of R-D performance and encoding complexity from low to high is JPEG, CCSDS-IDC, and JPEG2K. Besides, we test the R-D performance of some CS-based image encryption schemes, which utilize BM3D [41], NLR [42], LDAMP [31], ISTANet [30], OPINENet [43], and AMPNet [44] for reconstruction, and lagrangian interpolation (LIP) [45] and DNA rule [46] for encryption. The PSNR results of the test images with different image coding schemes are listed in Table 1.

Comparing the first six columns and the last columns of Table 1, we can see that the designed DRCAN prior can significantly improve the R-D performance of the CS-based coding scheme. The results achieve 2.28 and 1.57 dB gains over LIP-NLR and LIP-LDAMP at the compression ratio of 0.50 bpp. Comparing the last four columns of Table 1, we can see that the proposed scheme can outperform JPEG and approach the performance of JPEG2K at low compression ratios. The average reconstructed PSNR of the proposed scheme is, respectively, 3.01 and 0.52 dB higher than JPEG and CCSDS-IDC, and is only 0.26 dB lower than JPEG2K. Considering that the encoding process of the proposed scheme does not utilize entropy coding or other technologies to eliminate the redundancy among the measurements, the R-D performance of our scheme can be further improved.

Besides the PSNR metric, we also give the visual quality of the competing schemes. Figure 5 presents the parts of reconstructed images, in which the zoomed portions show that the proposed scheme can restore more sharp details with fewer artifacts. All these testing results indicate that our method achieves positive reconstruction performance both in quantitative and perceptual terms.

7.3 | Encryption performance

7.3.1 | Key space and key sensitivity analysis

To resist brute-force attacks, the key space should be larger than 2^{100} [47]. In the proposed scheme, six initial values in Equation (7), that is, $k_1^0, \ldots, k_6^0$, are regarded as the secret keys in the encryption process. Six 32-bit depth secret keys are generated from the SHA256 result of the input plain image. Therefore, the overall key space size S is $(2^{32})^6$, which means that the proposed scheme is resistant to brute-force attacks.

Also, an efficient encryption scheme should be highly sensitive to secret keys and plaintext. We test the key and plaintext sensitivity of the proposed scheme. Taking C(·) as the encryption encoder, we evaluate the key and plaintext sensitivity quantitatively using root mean square error (RMSE) as follows:

$$S_{k_i} = \|C(x, k + \Delta k_i) - C(x, k)\|_2 / \sqrt{m}, \quad (17)$$

TABLE 1 PSNR(dB) results for different image coding schemes

		Methods									
Images	Bpp	LIP -BM3D	LIP -NLR	LIP -LDAMP	DNA -ISTANet	DNA - OPINENet	DNA -AMPNet	JPEG2K	CCSDS-IDC	JPEG	Proposed
Barbara	0.25	24.57	22.06	23.07	21.17	22.96	23.78	27.26	25.43	23.86	26.01
	0.50	28.62	27.22	25.20	23.43	24.35	24.51	31.56	30.10	27.69	28.75
	0.75	31.00	31.08	27.89	23.49	24.70	24.73	34.33	32.85	31.08	31.26
	1.00	32.47	32.33	29.99	24.93	27.27	28.47	36.74	34.76	33.49	33.00
Boats	0.25	22.66	23.09	26.30	23.25	26.52	27.60	28.32	27.87	25.23	27.99
	0.50	29.52	28.77	29.45	27.04	29.53	29.65	32.88	31.56	30.21	31.66
	0.75	31.54	31.60	32.11	27.24	30.81	30.60	35.99	34.87	32.93	33.26
	1.00	32.95	33.16	33.12	29.01	33.08	31.38	38.05	36.60	35.06	34.77
Cameraman	0.25	24.94	21.65	27.11	20.48	23.46	24.17	27.32	26.78	25.03	28.20
	0.50	28.38	27.58	29.30	23.37	26.34	26.36	31.00	30.48	28.59	30.52
	0.75	29.45	28.69	30.26	23.46	26.83	26.80	33.92	33.09	30.83	31.42
	1.00	30.27	29.32	31.55	25.12	29.29	29.57	36.47	35.04	32.63	32.41
Foreman	0.25	31.30	30.16	32.14	26.37	27.19	32.37	34.33	33.76	30.47	33.08
	0.50	34.68	34.17	34.70	31.83	32.01	32.60	38.21	37.16	35.23	35.36
	0.75	36.17	36.29	36.46	32.69	36.13	35.06	40.77	39.71	37.30	36.73
	1.00	36.97	37.28	37.41	32.78	36.20	35.28	42.65	40.98	39.00	37.59
House	0.25	28.29	28.30	31.86	24.80	28.06	30.43	33.09	32.25	29.90	32.88
	0.50	34.25	33.48	34.23	29.70	31.58	32.43	36.12	35.60	34.59	34.68
	0.75	35.46	35.40	35.41	30.11	33.78	33.90	39.02	37.04	36.49	35.66
	1.00	36.40	36.26	36.00	31.43	34.99	35.52	40.97	39.51	38.20	36.60
Lena	0.25	24.20	24.29	27.36	23.21	26.19	27.14	29.10	28.69	25.41	28.82
	0.50	29.52	29.35	30.33	27.19	29.09	29.14	33.32	32.52	30.32	32.27
	0.75	31.57	32.24	32.98	27.42	29.96	29.80	36.57	35.54	32.75	33.95
	1.00	33.16	33.80	34.15	28.66	32.47	32.35	39.13	37.84	34.80	35.34
Monarch	0.25	19.87	20.00	25.05	20.17	24.80	25.92	25.70	24.98	22.89	27.12
	0.50	26.91	27.14	28.90	25.37	28.93	29.02	29.84	29.21	27.33	30.51
	0.75	29.03	29.40	30.92	25.58	29.86	29.65	33.06	31.89	29.90	32.41
	1.00	30.38	30.86	32.71	27.10	32.65	33.72	35.62	34.72	31.68	34.06
Parrots	0.25	27.67	25.19	29.35	22.12	24.35	25.97	31.46	30.55	27.62	30.42
	0.50	31.66	31.31	32.62	26.01	28.34	28.47	35.85	35.40	32.48	33.50
	0.75	33.36	33.60	34.20	26.18	29.27	29.15	38.67	37.49	35.00	35.02
	1.00	34.56	34.84	35.42	28.03	31.81	32.09	40.81	39.68	36.87	36.07
Average	0.25	25.44	24.34	27.78	22.70	25.44	27.17	29.57	28.79	26.30	29.31
	0.50	30.44	29.88	30.59	26.74	28.77	29.02	33.60	32.75	30.80	32.16
	0.75	32.20	32.29	32.53	27.02	30.17	29.96	36.54	35.31	33.29	33.71
	1.00	33.40	33.48	33.79	28.38	32.22	32.30	38.81	37.39	35.22	34.98

$$S_x = \|C(x + \Delta x, k) - C(x, k)\|_2 / \sqrt{m}, \tag{18}$$

where $x + \Delta x$ represents only adding 1 to a random pixel of plain image x, and $k + \Delta k_i$ represents only disturbing the ith element of secret keys with $\epsilon = 2^{-32}$. From Table 2, we can see that the value of the cipher image changes dramatically with a small disturbance. Figure 6 qualitatively illustrates the decrypted boats, from which we can see that the decrypted images with wrong secret keys cannot provide any perceptive information. A slight modification of secret keys leads to a wrong image that provides no perceptive information.

7.3.2 | Correlation of adjacent pixels

For a meaningful plain image, the value of correlation coefficients is close to one, whereas for a cipher image, the value

FIGURE 5 Reconstructed Cameraman at 0.25 bpp. (a) LIP-BM3D; (b) LIP-NLR; (c) LIP-LDAMP; (d) DNA-ISTANet; (e) DNA-OPINENet; (f) DNA-AMPNet; (g) JPEG2K; (h) CCSDS-IDC; (i) JPEG; (j) Proposed

TABLE 2 Key and plaintext sensitivity of the proposed encryption scheme for different test images

Images	S_x	S_{k_1}	S_{k_2}	S_{k_3}	S_{k_4}	S_{k_5}	S_{k_6}
Barbara	33.51	12.56	12.56	12.52	12.53	32.67	33.19
Boats	34.17	12.11	12.09	12.10	12.08	33.62	33.18
Cameraman	35.42	15.10	15.05	15.10	15.08	32.88	32.84
Foreman	35.39	11.40	11.46	11.47	11.38	33.35	33.93
House	28.68	10.46	10.50	10.40	10.44	31.96	34.02
Lena	33.68	11.61	11.66	11.64	11.65	33.44	32.06
Monarch	34.21	13.93	13.93	13.84	13.86	33.49	33.29
Parrots	34.62	13.79	13.81	13.75	13.76	33.60	33.87
Average	33.77	12.70	12.71	12.68	12.68	33.13	33.30

can be reduced close to zero by an efficient cryptosystem. Supposing that x and y are the adjacent pixels of an image, the correlation coefficient between x and y is calculated by the following formula:

$$r_{xy} = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \bar{x})^2 \cdot \sum_{i=1}^{N}(y_i - \bar{y})^2}}, \tag{19}$$

where $\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$ and $\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$. We randomly select 4000 pairs of adjacent pixels in horizontal, vertical, and diagonal directions.

Table 3 gives the correlation coefficients of adjacent pixels for the proposed scheme and two competing schemes, that is, 2DCS-ETC [48] and MRKCS [49]. 2DCS-ETC and MRKCS are two CS-based image coding schemes, of which R-D performance is lower than JPEG. From Table 3, we can see that the correlation coefficients of the proposed scheme are close to zero. Figure 7 further shows the pictorial representation of the distribution of the adjacent pixels in the plain and cipher images in three directions for the test image Lena. One can see that distributions of the plain image are similar to linear-like areas, whilst distributions of the encrypted image are random-like areas.

7.3.3 | Histogram analysis

To show the distribution also display the normalized histograms of plain and their respective cipher images. As shown in Figure 8, it is clear that the histogram of cipher images is more uniform than that of plain images. In addition, to quantitatively evaluate the uniformity of the plain and cipher image, we further calculate the variances of the histograms [50]

$$\mathrm{Var}(x) = \frac{1}{2^{2b}}\sum_{i=1}^{2^b}\sum_{j=1}^{2^b}\frac{1}{2}\left(p_i - p_j\right)^2, \tag{20}$$

where p_i denotes the proportion of pixels with pixel value to be i. Lower variances of histograms mean higher uniformity of the of pixel values in an image, we images. Table 4 gives the variances of the histograms of the plain images and cipher images, from which we can see that the histogram variance of the cipher image is greatly reduced compared with that of the plain image. Thus, the attackers cannot find any useful statistical data from the cipher image.

7.3.4 | Entropy analysis

The higher the information entropy of the data, the more unpredictable and random the data are. The information entropy is

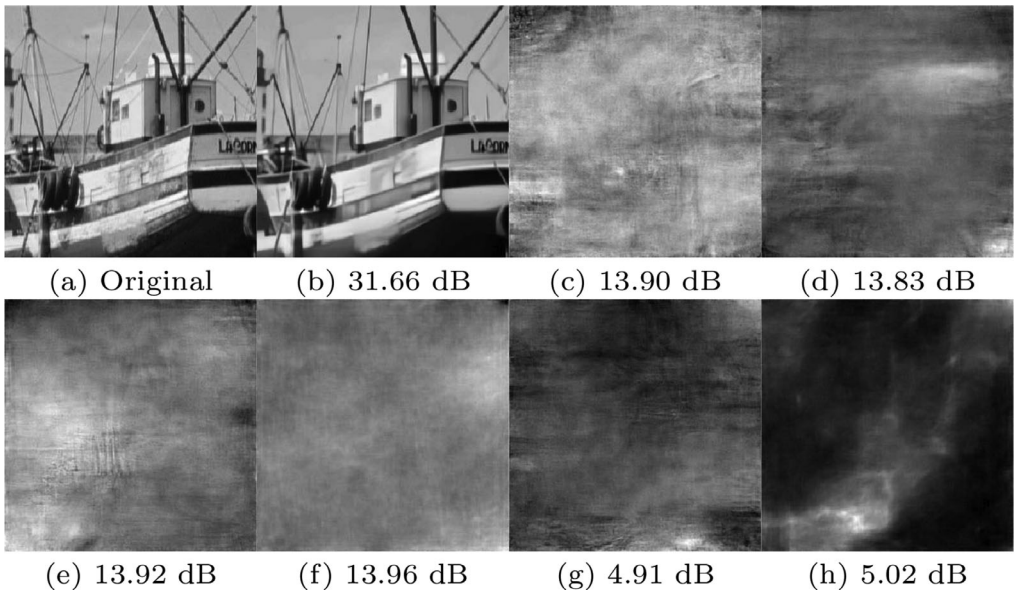

FIGURE 6 Decrypted boats with different keys at 0.50 bpp compression ratio. Only one element of the secret keys deviates $\epsilon = 2^{-32}$ from the true key. (a) original image; (b) correct keys; (c) $k_1^0 + \epsilon$; (d) $k_2^0 + \epsilon$; (e) $k_3^0 + \epsilon$; (f) $k_4^0 + \epsilon$; (g) $k_5^0 + \epsilon$; (h) $k_6^0 + \epsilon$

TABLE 3 Comparison of correlation coefficient of adjacent pixels in cipher images

Image		Vertical	Horizontal	Diagonal
Plain Image		**0.9528**	**0.9688**	**0.9306**
2DCS-ETC	0.25 bpp	-0.0044	0.0296	-0.0096
	0.50 bpp	0.0246	-0.0126	0.0118
	0.75 bpp	0.0120	-0.0041	0.0013
	1.00 bpp	0.0734	-0.0194	-0.0015
MRKCS	0.25 bpp	0.0243	0.0556	-0.0123
	0.50 bpp	0.0268	0.0371	-0.0017
	0.75 bpp	0.0378	0.1069	0.0057
	1.00 bpp	0.0349	0.1000	-0.0087
Proposed	0.25 bpp	-0.0156	-0.0080	0.0021
	0.50 bpp	-0.0091	-0.0145	0.0033
	0.75 bpp	-0.0102	-0.0093	0.0042
	1.00 bpp	-0.0119	0.0026	-0.0088

maximized when the data is uniformly distributed. We calculate the residual from the entropy of images to the maximum entropy as follows:

$$\mathrm{E}(x) = \sum_{i=1}^{2^b} \left(\frac{1}{2^b} \log_2 2^b - p_i \log_2 \frac{1}{p_i} \right) = b - \sum_{i=1}^{2^b} p_i \log_2 \frac{1}{p_i}, \quad (21)$$

where a smaller $\mathrm{E}(x)$ means that the image x is more like a random image with uniformly distributed pixel values. As shown in Table 5, the residuals from the entropy of the cipher images to the maximum entropy are much close to zero, demonstrating the security of the method under entropy attacks.

7.3.5 | Randomness analysis with NIST SP800-22

SP800-22 is a statistical test standard for validating the randomness of sequence published by American National Institution of Standard and Technology (NIST) [51], which contains 17 different sub-tests measuring various distributional characteristics of sequence. We subject 100 different cipher images to NIST SP800-22, where we obtain different cipher images by changing one pixel of the plain image. As suggested by NIST, one cipher is regarded as passing a sub-test of NIST SP800-22 if the p-value is larger than 0.01. Table 6 presents the average cipher p-value and passing proportion of each sub-test. We can see that all passing proportions are higher than 0.96, which indicates that our cipher images generated from the plain image has a high randomness guarantee.

7.3.6 | Differential attack

The differential attack aims to find a meaningful relation between plain and cipher images by examining the impact of modifications to plain images on cipher images. To evaluate the resistance to the differential attack, we calculate the number of pixel changing rate (NPCR) and unified average changed intensity (UACI) as follows

$$\begin{cases} \mathrm{NPCR} = \dfrac{\sum_{i,j} R(i,j)}{m}, \\ R(i,j) = \begin{cases} 1, & c_1(i,j) \neq c_2(i,j) \\ 0, & c_1(i,j) = c_2(i,j), \end{cases} \end{cases} \quad (22)$$

$$\mathrm{UACI} = \frac{1}{m} \left[\sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{2^b - 1} \right], \quad (23)$$

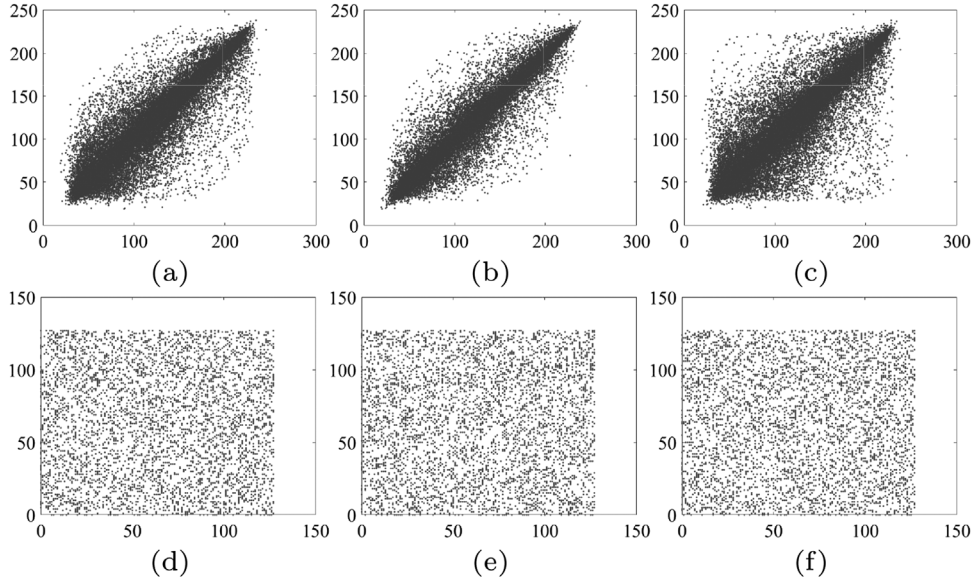

FIGURE 7 Correlation analysis of test image Lena. The X and Y coordinates are the values of two pixels adjacent to each other in the horizontal, vertical, or diagonal directions. Panels (a)–(c) refer to the horizontal, vertical, and diagonal correlation of plain image; (d)–(f) refer to the horizontal, vertical, and diagonal correlation of cipher image

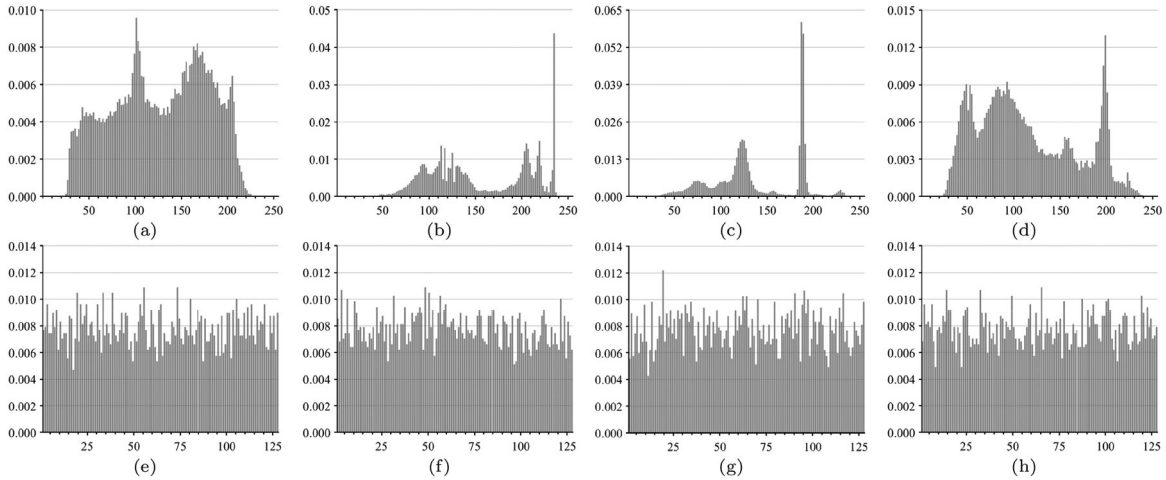

FIGURE 8 Normalized histogram of plain and cipher images. (a–d) The histograms of four plain images (Barbara, Foreman, House, and Monarch); (e–h) the corresponding histograms of cipher images

where c_1 and c_2 are two cipher images before and after one pixel of the plain image changed.

Suppose that c_1 and c_2 obey two independent random uniform distributions, then the expected NPCR and UACI metrics can be, respectively, calculated as

$$\mathrm{NPCR}_{\mathrm{expected}} = \left(1 - \frac{1}{2^b}\right), \tag{24}$$

$$\mathrm{UACI}_{\mathrm{expected}} = \frac{1}{2^{2b}}\left(\frac{\sum_{i=1}^{2^b-1}(i+1)i}{2^b - 1}\right), \tag{25}$$

from which $\mathrm{NPCR}_{\mathrm{expected}} = 99.22\%$ and $\mathrm{UACI}_{\mathrm{expected}} = 33.59\%$ for $b = 7$. Table 7 presents the NPCR and UACI metrics corresponding to the changes in four different positions of the plain images. All NPCR and UACI results are quite close to the expected values, which shows that the proposed scheme is sensitive to the plain image.

7.3.7 | Classical types of attacks

Ciphertext-only attacks, chosen-ciphertext attacks, known-plaintext attacks, and chosen-plaintext attacks are four classic types of attacks, of which the chosen-plaintext attack is the most powerful one. If a cryptosystem can resist the chosen-plaintext attack, it can resist other types [52–55].

We set the secret keys via the SHA256 function of the plain image, resulting in different secret keys for different plain

TABLE 4 Variances of histograms for plain and cipher images

Images		Barbara	Boats	Cameraman	Foreman	House	Lena	Monarch	Parrots
Plain		$\mathbf{6.93 \times 10^{-6}}$	$\mathbf{2.38 \times 10^{-5}}$	$\mathbf{2.58 \times 10^{-5}}$	$\mathbf{3.20 \times 10^{-5}}$	$\mathbf{7.00 \times 10^{-5}}$	$\mathbf{9.43 \times 10^{-6}}$	$\mathbf{9.36 \times 10^{-6}}$	$\mathbf{1.66 \times 10^{-5}}$
Cipher	0.25 bpp	3.67×10^{-6}	3.04×10^{-6}	3.33×10^{-6}	2.86×10^{-6}	3.17×10^{-6}	3.33×10^{-6}	2.63×10^{-6}	3.18×10^{-6}
	0.50 bpp	1.67×10^{-6}	1.98×10^{-6}	1.70×10^{-6}	1.50×10^{-6}	2.10×10^{-6}	1.49×10^{-6}	1.56×10^{-6}	1.36×10^{-6}
	0.75 bpp	1.19×10^{-6}	1.04×10^{-6}	1.07×10^{-6}	1.41×10^{-6}	1.10×10^{-6}	8.72×10^{-7}	1.18×10^{-6}	9.44×10^{-7}
	1.00 bpp	8.65×10^{-7}	7.49×10^{-7}	9.81×10^{-7}	8.44×10^{-7}	1.05×10^{-6}	7.79×10^{-7}	9.76×10^{-7}	8.76×10^{-7}

TABLE 5 Residuals from the entropy of images to the maximum entropy

Images		Barbara	Boats	Cameraman	Foreman	House	Lena	Monarch	Parrots
Plain		**0.4748**	**0.8544**	**0.9903**	**0.9917**	**1.5070**	**0.5557**	**0.5284**	**0.5859**
Cipher	0.25 bpp	0.0526	0.0489	0.0587	0.0427	0.0445	0.0403	0.0463	0.0485
	0.50 bpp	0.0316	0.0252	0.0285	0.0269	0.0260	0.0288	0.0263	0.0227
	0.75 bpp	0.0151	0.0149	0.0160	0.0164	0.0119	0.0123	0.0150	0.0122
	1.00 bpp	0.0123	0.0100	0.0106	0.0117	0.0111	0.0123	0.0104	0.0125

TABLE 6 Cipher and Chaos results of NIST SP800-22 test suite

Statistical test	Passing proportion	Cipher p-value	Cipher results	Chaos p-value	Chaos results
Frequency	1.00	0.4816	SUCCESS	0.4651	SUCCESS
Block frequency ($m = 20,000$)	1.00	0.4588	SUCCESS	0.3554	SUCCESS
Runs	0.98	0.4914	SUCCESS	0.4577	SUCCESS
Longest runs of ones	1.00	0.5149	SUCCESS	0.7867	SUCCESS
Rank	1.00	0.4929	SUCCESS	0.1536	SUCCESS
Spectral DFT	0.97	0.4951	SUCCESS	0.1692	SUCCESS
Non-overlapping templates ($m = 9$)	0.99	0.5086	SUCCESS	0.5110	SUCCESS
Overlapping templates ($m = 9$)	0.99	0.4910	SUCCESS	0.6712	SUCCESS
Maurers universal	1.00	0.4659	SUCCESS	0.3698	SUCCESS
Linear complexity ($m = 500$)	0.98	0.5161	SUCCESS	0.9502	SUCCESS
Serial p-value1($m = 16$)	0.99	0.5046	SUCCESS	0.0751	SUCCESS
Serial p-value2($m = 16$)	0.99	0.4899	SUCCESS	0.0830	SUCCESS
Approximate entropy ($m = 10$)	1.00	0.5174	SUCCESS	0.8817	SUCCESS
Cumulative sums (Forward)	1.00	0.4813	SUCCESS	0.7495	SUCCESS
Cumulative sums (Reverse)	1.00	0.4762	SUCCESS	0.3382	SUCCESS
Random excursions ($x = -1$)	0.98	0.5302	SUCCESS	0.6582	SUCCESS
Random excursions variant ($x = -1$)	0.98	0.4737	SUCCESS	0.1297	SUCCESS

images. Then, we take the secret keys as the initial values of the chaotic maps to create measurement matrix Φ and diffusion noise η. A slight change of the plain image would result in a totally different measurement process (i.e. Equation (3)). Thus, the cipher image of our scheme is heavily dependent on the plain image and is resistant to known/chosen-plaintext attacks.

In some cases, attackers may use particular plain images, such as all-black images and all-white images, to break down the encryption scheme. Table 8 illustrates the residual from image entropy to maximum entropy (Equation (21)) and correlation coefficient (Equation (19)) of both all-black and all-white plain images, from which we can see that both metrics are close to zero, at the same level of the natural images. Useful information cannot be obtained from the cipher images of all-black and all-white plain images, indicating that the particular images attack method cannot work.

TABLE 7 NPCR and UACI for different positions

Images	Metrics	Position of the changed pixel (1,1)	(100,200)	(200,100)	(256,256)
Barbara	NPCR(%)	99.20	99.20	99.26	99.22
	UACI(%)	33.65	33.66	33.60	33.63
Boats	NPCR(%)	99.24	99.23	99.11	99.19
	UACI(%)	33.56	33.67	33.09	33.44
Cameraman	NPCR(%)	99.25	99.23	99.21	99.25
	UACI(%)	33.73	33.61	33.65	33.67
Foreman	NPCR(%)	99.19	99.26	99.12	99.22
	UACI(%)	33.57	33.52	33.00	33.64
House	NPCR(%)	99.21	99.21	99.22	99.21
	UACI(%)	33.60	33.56	33.60	33.57
Lena	NPCR(%)	99.16	99.09	99.23	99.22
	UACI(%)	33.13	32.66	33.57	33.55
Monarch	NPCR(%)	99.21	99.21	99.23	99.24
	UACI(%)	33.63	33.55	33.61	33.72
Parrots	NPCR(%)	99.22	99.22	99.20	99.22
	UACI(%)	33.57	33.52	33.19	33.62

TABLE 8 Residual from the entropy of the cipher image to the maximum entropy and correlation coefficient for all-black and all-white images

Images	Entropy residual	Correlation coefficients Horizontal	Vertical	Diagonal
Cipher of all white	0.0097	-0.0033	-0.0033	0.0111
Cipher of all black	0.0099	-0.0094	0.0086	-0.0034

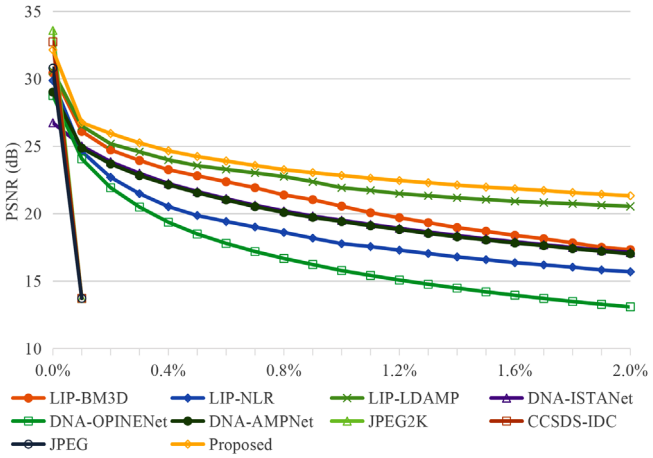

FIGURE 9 Average reconstructed PSNRs of comparison schemes at 0.50 bpp with different bit error probabilities P_{BSC}

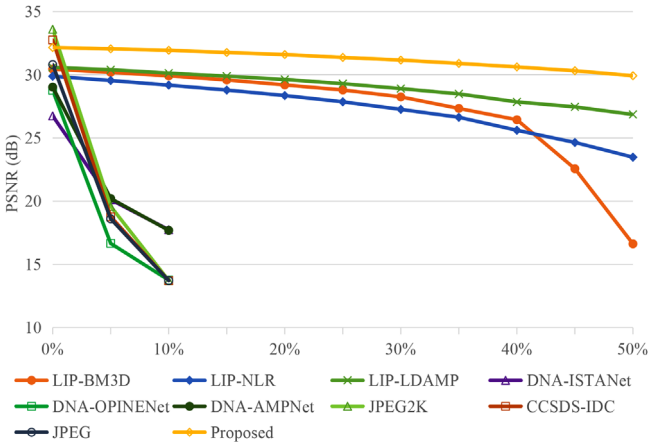

FIGURE 10 Average reconstructed PSNRs of comparison schemes at 0.50 bpp with different bit loss probabilities P_{BEC}

7.4 | Robustness performance

The measurements are quantized into bits, which may be lost or wrong during the process of transmission. In this section, we evaluate the robustness of the proposed scheme under the binary symmetric channel (BSC) and the binary erasure channel (BEC). In BSC, a transmitted bit will be 'flipped' with a bit error probability of P_{BSC}, and in BEC, a transmitted bit will be not received with a bit loss probability of P_{BEC}.

The robustness is the most competitive advantage of the CS-based image coding scheme. Traditional image coding schemes, that is, JPEG, CCSDS-IDC, and JPEG2K, are sensitive to bit error and bit loss. As shown in Figures 9 and 10, a low P_{BSC} and P_{BEC} will cause the traditional image coding schemes unable to reconstruct the entire image. On the contrary, some CS-based image coding schemes can defend bit loss or bit error due to the democracy of CS measurements. As shown in Figures 9 and 10, the PSNR degradation of the proposed scheme is less sensitive to the P_{BSC} and P_{BEC}. Although other CS-based image coding schemes, including BM3D-CS, NLR-CS, and LDAMP, are also robust to bit error and loss, there is a significant PSNR gap from the proposed scheme. For example, the proposed still obtains 29.92 dB reconstructed PSNR, much higher than the LDAMP with 26.86 dB when $P_{BEC} = 50\%$.

Figure 11 further depicts the reconstructed Parrots at 0.50 bpp compression ratio when $P_{BSC} = 0.25\%$ and $P_{BEC} = 5\%$. One can see that the proposed scheme can recover most of the visual information of the original images, while traditional image coding schemes fail to reconstruct the image. One can also observe that other CS-based schemes are only able to reconstruct the image with poor visual quality.

7.5 | Discussion

7.5.1 | Preprocessing influence

To enhance R-D performance, the original image is preprocessed by a denoising network before CS random sampling process. The adopted denoising network is designed to deal with images with additive white Gaussian noise (AWGN) from a certain noise level. Table 9 presents the average reconstructed

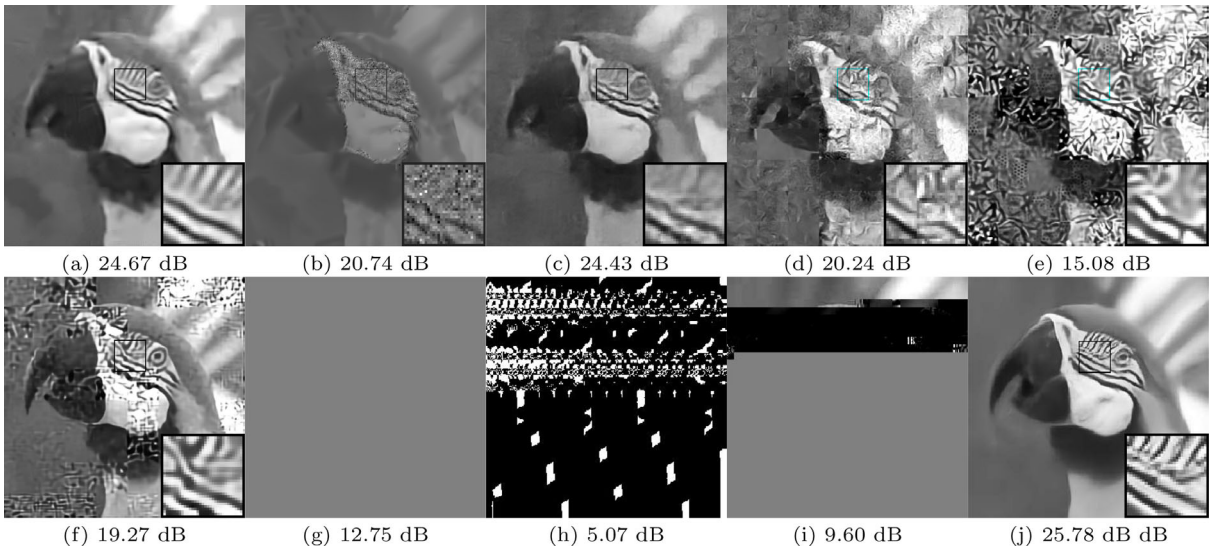

FIGURE 11 Reconstructed Parrot at 0.50 bpp when $P_{BSC} = 0.25\%$ and $P_{BEC} = 5\%$. (a) LIP-BM3D; (b) LIP-NLR; (c) LIP-LDAMP; (d) DNA-ISTANet; (e) DNA-OPINENet; (f) DNA-AMPNet; (g) JPEG2K; (h) CCSDS-IDC; (i) JPEG; (j) Proposed

TABLE 9 R-D performance of the denoising preprocessing strategy using the denoising network trained for the different range of noise levels

	Range of noise levels						
Bpp	**0**	**[0,5]**	**[5,10]**	**[10,15]**	**[15,20]**	**[20,30]**	**[30,40]**
0.25	28.05	28.09	28.46	28.82	29.25	29.31	29.41
0.50	31.02	31.09	31.69	32.01	32.16	30.43	30.76
0.75	32.88	33.00	33.61	33.71	33.20	30.57	30.94
1.00	34.38	34.53	34.98	34.84	33.61	30.73	31.14

TABLE 10 Encoding time comparison (s)

	Compression ate (bpp)			
Methods	**0.25**	**0.50**	**0.75**	**1.00**
JPEG2K	0.0416	0.0458	0.0465	0.0470
CCSDS-IDC	0.0103	0.0123	0.1390	0.1570
JPEG	0.0032	0.0045	0.0047	0.0051
Proposed w DP	0.0279	0.0283	0.0285	0.0287
Proposed w/o DP	0.0062	0.0064	0.0067	0.0072

PSNRs of the proposed scheme when using the preprocessing denoising network trained for a different range of noise levels, in which the first column means adding no denoising preprocessing. For a low compression ratio such as 0.25 bpp, a preprocessing denoising network for a high noise level can obtain promising PSNR results, and for a high compression ratio, a denoising network for a low noise level is a better option. Underlined values are the reconstruction PSNRs when using the denoising network for the pre-setted noise level. As shown in Table 9, denoising preprocessing can enhance the R-D performance efficiently.

7.5.2 | Computing complexity

We compare the encoding time of the proposed scheme with the other three image compression standards, that is, JPEG, CCSDS-IDC, and JPEG2K. We disregard other CS-based image coding schemes in Section 7.2 for their low R-D performance. The comparisons are performed on a PC with Intel i5 CPU and Nvidia RTX 2070 GPU. Traditional image compression standards are carried out in C or C++, and the proposed scheme is realized in Matlab. Table 10 gives the average running time over eight test images with different compression ratios, from which we can see that the encoding time of the proposed scheme without denoising preprocessing (DP) strategy is shorter than that of CCSDS-IDC. Even after introducing the DP strategy, the encoding time of the proposed scheme is still less than that of JPEG2K.

8 | CONCLUSION

Here, we proposed an efficient and robust image compression-encryption scheme. We designed a chaotic system to generate SBBS matrix and diffusion noise for encryption and utilized deep-learned prior for plain image reconstruction. Besides, we adopted a denoising preprocessing strategy to enhance rate-distortion performance. For compression performance, our scheme outperforms JPEG, achieving PSNR gains over 3 dB at 0.25 bpp. For encryption performance, the proposed scheme has a huge key space. For robust performance, images with good quality can be obtained at high bit error or loss probability. In terms of running efficiency, the encoding time of the proposed method is about 70% of JPEG2K. In summary, the proposed scheme can compress and encrypt images simultaneously, meanwhile achieving high security, low encoding time, strong robustness, and high rate-distortion performance.

Regarding our future work, there exist several aspects for improvement. First, one can replace DRCAN with a more powerful deep network technology such as Transformer. Second, one can introduce the progressive coding strategy to further improve R-D performance. Third, one can combine the proposed cipher within steganography technology to enhance image safety.

AUTHOR CONTRIBUTIONS

Zan Chen: Formal analysis, methodology, writing - original draft. Chaocheng Ma: Resources, software, validation. Tao Wang: Writing - review and editing. Yuanjing Feng: Funding acquisition, supervision. Xingsong Hou: Project administration. Xueming Qian: Conceptualization. All authors have read and agreed to the published version of the manuscript.

ACKNOWLEDGEMENTS

This research was sponsored in part by the National Natural Science Foundation of China (Grant Nos. 62002327, 61976190, 62073294, 61872286), Natural Science Foundation of Zhejiang Province (Grant No. LQ21F020017, LZ21F030003), and the Agricultural and Social Development Foundation of Hangzhou (Grant No. 202004A07).

CONFLICT OF INTEREST

The authors declare no conflict of interest.

DATA AVAILABILITY STATEMENT

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

ORCID

Chaocheng Ma https://orcid.org/0000-0002-4229-4321

REFERENCES

1. Chen, J., Chen, L., Zhou, Y.: Universal chosen-ciphertext attack for a family of image encryption schemes. IEEE Trans. Multimedia 23, 2372–2385 (2021)
2. Li, Y., Wang, C., Chen, H.: A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Opt. Lasers Eng. 90, 238–246 (2017)
3. K.U., S., Mohamed, A.: Novel hyper chaotic color image encryption based on pixel and bit level scrambling with diffusion. Signal Process. Image Commun. 99, 116495 (2021)
4. Dou, Y., Li, M.: An image encryption algorithm based on a novel 1d chaotic map and compressive sensing. Multimedia Tools and Applications 80(16), 24437–24454 (2021)
5. Rehman, A.U., Firdous, A., Iqbal, S., Abbas, Z., Shahid, M.M.A., Wang, H., Ullah, F.: A color image encryption algorithm based on one time key, chaos theory, and concept of rotor machine. IEEE Access 8, 172275–172295 (2020)
6. Liu, H., Xu, Y., Ma, C.: Chaos-based image hybrid encryption algorithm using key stretching and hash feedback. Optik 216, 164925 (2020)
7. Zhang, F., Zhang, X., Cao, M., Ma, F., Li, Z.: Characteristic analysis of 2d lag-complex logistic map and its application in image encryption. IEEE MultiMedia 28(4), 96–106 (2021)
8. Farah, M.B., Guesmi, R., Kachouri, A., Samet, M.: A novel chaos based optical image encryption using fractional fourier transform and dna sequence operation. Opt. Laser Technol. 121, 105777 (2020)
9. Yadollahi, M., Enayatifar, R., Nematzadeh, H., Lee, M., Choi, J.-Y.: A novel image security technique based on nucleic acid concepts. J. Inf. Secur. Appl. 53, 102505 (2020)
10. Elmanfaloty, R.A., Alnajim, A.M., Abou-Bakr, E.: A finite precision implementation of an image encryption scheme based on dna encoding and binarized chaotic cores. IEEE Access 9, 136905–136916 (2021)
11. Zhou, Y., Bao, L., Chen, C.P.: A new 1d chaotic system for image encryption. Signal Process. 97, 172–182 (2014)
12. Chai, X., Wu, H., Gan, Z., Han, D., Zhang, Y., Chen, Y.: An efficient approach for encrypting double color images into a visually meaningful cipher image using 2d compressive sensing. Inf. Sci. 556, 305–340 (2021)
13. Hua, Z., Zhou, Y., Huang, H.: Cosine-transform-based chaotic system for image encryption. Inf. Sci. 480, 403–419 (2019)
14. Chen, Z., Hou, X., Shao, L., Gong, C., Qian, X., Huang, Y., Wang, S.: Compressive sensing multi-layer residual coefficients for image coding. IEEE Trans. Circuits Syst. Video Technol. 30(4), 1109–1120 (2020)
15. Zhang, B., Liu, Y., Zhuang, J., Wang, K., Cao, Y.: Matrix permutation meets block compressed sensing. J. Visual Commun. Image Represent. 60, 69–78 (2019)
16. Liu, H., Xiao, D., Zhang, R., Zhang, Y., Bai, S.: Robust and hierarchical watermarking of encrypted images based on compressive sensing. Signal Process. Image Commun. 45, 41–51 (2016)
17. Rachlin, Y., Baron, D.: The secrecy of compressed sensing measurements. In: 2008 46th Annual Allerton Conference on Communication, Control, and Computing, pp. 813–817. IEEE, Piscataway, NJ (2008)
18. Bianchi, T., Bioglio, V., Magli, E.: Analysis of one-time random projections for privacy preserving compressed sensing. IEEE Trans. Inf. Forensics Secur. 11(2), 313–327 (2015)
19. Zhang, Y., Zhang, L.Y., Zhou, J., Liu, L., Chen, F., He, X.: A review of compressive sensing in information security field. IEEE Access 4, 2507–2519 (2016)
20. Zhou, N., Jiang, H., Gong, L., Xie, X.: Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging. Opt. Lasers Eng. 110, 72–79 (2018)
21. Chai, X., Zheng, X., Gan, Z., Han, D., Chen, Y.: An image encryption algorithm based on chaotic system and compressive sensing. Signal Process. 148, 124–144 (2018)
22. Zhang, L., Zhou, Y., Huo, D., Li, J., Zhou, X.: Multiple-image encryption based on double random phase encoding and compressive sensing by using a measurement array preprocessed with orthogonal-basis matrices. Opt. Laser Technol. 105, 162–170 (2018)
23. Chen, Z., Hou, X., Qian, X., Gong, C.: Efficient and robust image coding and transmission based on scrambled block compressive sensing. IEEE Trans. Multimedia 20(7), 1610–1621 (2018)
24. Baraniuk, R.G.: Compressive sensing. IEEE Signal Process Mag. 24(4), 118–121 (2007)
25. Yu, L., Barbot, J.P., Zheng, G., Sun, H.: Compressive sensing with chaotic sequence. IEEE Signal Process Lett. 17(8), 731–734 (2010)
26. Li, L., Fang, Y., Liu, L., Peng, H., Kurths, J., Yang, Y.: Overview of compressed sensing: Sensing model, reconstruction algorithm, and its applications. Appl. Sci. 10(17), 5909 (2020)
27. Chen, Z., Hou, X., Gong, C., Qian, X.: Compressive sensing reconstruction for compressible signal based on projection replacement. Multimedia Tools Appl. 75(5), 2565–2578 (2016)
28. Sun, Y., Yang, Y., Liu, Q., Chen, J., Yuan, X.-T., Guo, G.: Learning non-locally regularized compressed sensing network with half-quadratic splitting. IEEE Trans. Multimedia 22(12), 3236–3248 (2020)
29. Venkatakrishnan, S.V., Bouman, C.A., Wohlberg, B.: Plug-and-play priors for model based reconstruction. In: 2013 IEEE Global Conference on Signal and Information Processing, pp. 945–948. IEEE, Piscataway, NJ (2013)
30. Zhang, J., Ghanem, B.: Ista-net: Interpretable optimization-inspired deep network for image compressive sensing. In: 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 1828–1837. IEEE, Piscataway, NJ (2018)

31. Metzler, C., Mousavi, A., Baraniuk, R.: Learned d-amp: Principled neural network based compressive image recovery. In: Advances in Neural Information Processing Systems, pp. 1772–1783. (2017)
32. Chen, Z., Guo, W., Feng, Y., Li, Y., Zhao, C., Ren, Y., Shao, L.: Deep-learned regularization and proximal operator for image compressive sensing. IEEE Trans. Image Process. 30, 7112–7126 (2021)
33. Chen, Z., Feng, Y., Ren, Y.: Deep 2nd-order residual block for image denoising. Multimedia Tools and Applications 1–19 (2022)
34. Chen, Z., Hou, X., Shao, L., Wang, S.: Revising regularisation with linear approximation term for compressive sensing improvement. Electron. Lett. 55(7), 384–386 (2019)
35. Hou, X., Zhang, L., Chen, Z., Gong, C.: Sparse-filtering in directional lifting wavelet transform domain based bayesian compressive sensing. Int. J. Wavelets Multiresolut. Inf. Process. 12(06), 1450043 (2014)
36. Tan, Y., Hou, X., Chen, Z., Yu, S.: Image compressive sensing reconstruction based on collaboration reduced rank preprocessing. Electron. Lett. 53(11), 717–718 (2017)
37. Timofte, R., Agustsson, E., Gool, L.V., Yang, M.H., Qi, G.: Ntire 2017 challenge on single image super-resolution: Methods and results. In: IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 1110–1121. IEEE, Piscataway, NJ (2017)
38. Rabbani, M., Joshi, R.: An overview of the jpeg 2000 still image compression standard. Signal Process. Image Commun. 17(1), 3–48 (2002)
39. Yeh, P.-S., Armbruster, P., Kiely, A., Masschelein, B., Moury, G., Schaefer, C., Thiebaut, C.: The new ccsds image compression recommendation. In: 2005 IEEE Aerospace Conference, pp. 4138–4145. IEEE, Piscataway, NJ (2005)
40. Taubman, D.S., Marcellin, M.W.: Jpeg2000: Standard for interactive imaging. Proc. IEEE 90(8), 1336–1357 (2002)
41. Metzler, C.A., Maleki, A., Baraniuk, R.G.: From denoising to compressed sensing. IEEE Trans. Inf. Theory 62(9), 5117–5144 (2016)
42. Dong, W., Shi, G., Li, X., Ma, Y., Huang, F.: Compressive sensing via nonlocal low-rank regularization. IEEE Trans. Image Process. 23(8), 3618–3632 (2014)
43. Zhang, J., Zhao, C., Gao, W.: Optimization-inspired compact deep compressive sensing. IEEE J. Sel. Top. Signal Process. 14(4), 765–774 (2020)
44. Zhang, Z., Liu, Y., Liu, J., Wen, F., Zhu, C.: Amp-net: Denoising-based deep unfolding for compressive image sensing. IEEE Trans. Image Process. 30, 1487–1500 (2021)
45. Wu, B., Xie, D., Chen, F., Wang, X., Zeng, Y.: A multi-party secure encryption-sharing hybrid scheme for image data base on compressed sensing. Digital Signal Process. 123, 103391 (2022)
46. Bao, W., Zhu, C.: A secure and robust image encryption algorithm based on compressive sensing and dna coding. Multimedia Tools and Applications 81(11), 15977–15996 (2022)
47. Alvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurcation Chaos 16(08), 2129–2151 (2006)
48. Zhang, B., Xiao, D., Xiang, Y.: Robust coding of encrypted images via 2d compressed sensing. IEEE Trans. Multimedia 23, 2656–2671 (2021)
49. Canh, T.N., Dinh, K.Q., Jeon, B.: Multi-scale/multi-resolution kronecker compressive imaging. In: 2015 IEEE International Conference on Image Processing (ICIP), pp. 2700–2704. IEEE, Piscataway, NJ (2015)
50. Zhang, Y.-Q., Wang, X.-Y.: A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. Inf. Sci. 273, 329–351 (2014)
51. Bassham, L., Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Leigh, S., Levenson, M., Vangel, M., Heckert, N., Banks, D.: A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, Special Publication (NIST SP). National Institute of Standards and Technology, Gaithersburg, MD (2010)
52. Wang, X., Teng, L., Qin, X.: A novel colour image encryption algorithm based on chaos. Signal Process. 92(4), 1101–1108 (2012)
53. Wang, X., Gao, S.: Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a boolean network. Inf. Sci. 539, 195–214 (2020)
54. Xu, L., Gou, X., Li, Z., Li, J.: A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. Opt. Lasers Eng. 91, 41–52 (2017)
55. Wang, X., Teng, L.: An image blocks encryption algorithm based on spatiotemporal chaos. Nonlinear Dyn. 67(1), 365–371 (2012)

How to cite this article: Chen, Z., Ma, C., Wang, T., Feng, Y., Hou, X., Qian, X.: Robust image compression-encryption via scrambled block bernoulli sampling with diffusion noise. IET Image Process. 17, 1478–1492 (2023). https://doi.org/10.1049/ipr2.12731