IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

A New Image Encryption Algorithm Based on Modified Optically Injected Semiconductor Laser Chaotic System

XUEJUN LI[1], BO LI[1], BO SUN[2], ZHISEN WANG[1], CAIYIN WANG[3] AND JUN MOU[1].

[1]School of Information Science and Engineering, Dalian Polytechnic University, Dalian, 116034, China
[2]School of Management, Dalian Polytechnic University, Dalian 116034, China
[3]School of Light Industry and Chemical Engineering, Dalian Polytechnic University, Dalian, 116034, China

Corresponding author: Bo Li (libolb@dlpu.edu.cn); Bo Sun (sunbo@dlpu.edu.cn).

This work was supported by the National Science Foundation for Young Scientists of China (Grant No.61802041); Doctoral Scientific Research Foundation of Liaoning Province of China (Grant No. 2020-BS-210).

ABSTRACT Compared with general chaotic systems, laser chaotic systems have more complex dynamic behaviors and extremely high sensitivity to parameters and initial values. So far, there are few studies on the application of laser chaotic systems to image encryption. Therefore, this paper proposes a new image encryption scheme based on an optical injection semiconductor laser chaotic system. The encryption scheme mainly includes two processes of scrambling and diffusion. The scrambling process converts the pseudo-random sequences generated by the laser chaotic system into chaotic matrixes and scrambling each pixel through a random point scrambling algorithm. In the diffusion process, the chaotic sequences generated by the laser chaotic system are quantized into random numbers and applied to the improved gravitational model algorithm to achieve the effect of pixel diffusion. The experimental results and security analysis indicate that the proposed algorithm has good image encryption performance and can effectively resist various common attacks on image encryption systems.

INDEX TERMS Image encryption; Laser chaotic system; Random point scrambling; Improved gravitation model

I. INTRODUCTION

WITH the rapid development of the communications industry, more and more information is transmitted through the Internet [1]. Digital images are one of the most important components of multimedia exchange [2]. The number of digital images distributed through social media or instant messaging tools has reached the highest level in history. However, there are huge security risks in the transmission of images in an open network environment [3]–[6], such as illegal theft of information, data tampering, and data deletion, and so on [7]. Therefore, the security of digital image transmission and storage has become a research hotspot [8]–[10]. Encryption is the simplest but most effective way to protect digital images. Currently, most of the image encryption algorithms are based on both scrambling and diffusion. By scrambling, the position information of the pixels in the plaintext image can be disrupted, making it visually impossible to obtain the information of the plaintext image. However, the pixel value of the plaintext image cannot be changed only by the scrambling operation, so it cannot resist known-plaintext attacks. The diffusion process is used to replace the pixel values so that the correlation between adjacent pixels of the ciphertext image is greatly reduced and the security of the encryption is improved. However, the diffusion operation alone may lead to noise interference or corruption in the transmission of the ciphertext image and the information of the plaintext image cannot be decrypted properly. Combining the scrambling and diffusion operations on the plaintext image will effectively solve the problems arising from using them alone for encryption. The traditional encryption system is designed for text information. However, compared with text information, the image has features with visualization, high redundancy, and high relevance [11]. Therefore, traditional text encryption methods are not suitable for image encryption [12]. Chaos [13]–[15], as a theoretical system sensitive to initial conditions, meets the needs of cryptography very well.

In recent years, chaotic systems have been widely used in secure communication because of their complex nonlinear features [16]–[20]. Driven by Fridrich's pioneering

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3113734, IEEE Access

work, chaos theory became a satisfactory solution for image encryption [21]. Subsequently, researchers designed many cryptosystems based on chaos theory, such as compressed sensing [22]–[27], DNA encoding [28]–[33], S-box [34]–[36], neural network [37]–[40], and so on.

In previous studies, some simple chaotic maps, such as one-dimensional maps and two-dimensional maps, have weak key spaces [41]–[46]. Their chaotic sequence orbits are simple [47], [48] and can be predicted by techniques such as regression mapping, phase space reconstruction, and nonlinear prediction. At the same time, the randomness of chaotic mapping will be significantly reduced in the digital domain, and it will be vulnerable to selected plaintext or known-plaintext attacks [49]. With the rapid development of computer computing power and the continuous improvement of encryption technology requirements, the security of simple, low-level chaotic systems is declining.

The semiconductor laser chaotic system has been paid close attention because of its more complex dynamic behavior changes and extremely high sensitivity to parameters [50], [51]. The application of semiconductor laser chaotic system to image secure communication can greatly improve the reliability of the encryption system. For example, an cryptosystem based on laser chaotic synchronization and Arnold cat mapping was proposed by Shu-Ying Wang et al. [52]. In [53], a chaotic laser was utilized to obtain a random key stream and scramble the original image in a pixel arrangement of the scanned image. To intensify the security of cryptosystem, a new image encryption scheme based on the light injection laser chaotic system [54], [55] is proposed in this paper. This encryption scheme combines the random point scrambling algorithm and the improved gravitation model diffusion algorithm, and a good encryption effect can be obtained by performing a round of encryption on the plaintext image.

The rest of this paper is arranged as follows. The optical injected laser chaotic system is introduced in section 2. In section 3, the proposed cryptosystem is introduced in detail. In section 4, the security of the proposed cryptosystem is analyzed from various angles. The summarizes and prospects of this paper's work are given in section 5.

II. OPTICAL INJECTED SEMICONDUCTOR LASER CHAOTIC SYSTEM

A semiconductor laser with monochromatic light injection can be modeled by a three-dimensional velocity equation composed of a complex electric field $P = P_u + iP_v$ and a normalized population inversion n. The proportional equation of the system can be described as

$$\begin{cases} \dot{P} = K + (\frac{1}{2}(1+i\alpha)n - i\omega)P \\ \dot{n} = -2\Gamma n - (1+2Bn)(|P|^2 - 1) \end{cases} \tag{1}$$

Equation (1) can be rewritten into three ordinary differential equations. By separating the imaginary part and real part of the complex electric field, which can be directly used for integration:

$$\begin{cases} \frac{dP_u}{dt} = K + \frac{1}{2}P_u n + (\omega - \frac{1}{2}\alpha n)P_v \\ \frac{dP_v}{dt} = \frac{1}{2}P_v n - (\omega - \frac{1}{2}\alpha n)P_u \\ \frac{dn}{dt} = -2\Gamma n - (1+2Bn)({P_u}^2 + {P_v}^2 - 1) \end{cases} \tag{2}$$

where $P^2 = P_u^2 + P_v^2$, the dimensionless injected field strength is K, and the parameters B and Γ are obtained by the following formula:

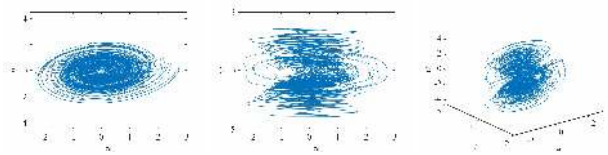
$$B = \frac{\omega_R}{2\Gamma_0}, \quad \Gamma = \frac{\Gamma_N}{2\omega_R} + B \tag{3}$$

where Γ_0 is the inverse lifetime of photons, and Γ_N is the inverse lifetime of electrons.

Modify equation (2) by $B = \Gamma = \omega = 0$. Firstly, removing the constant-coefficient "1/2" , and letting $P_u \to u$, $P_v \to v$, $n \to w$. Then add the damping constant $-\varepsilon$ to the dv/dt equation. Finally, a simpler laser chaotic system is obtained:

$$\begin{cases} \frac{du}{dt} = K + w(u - \alpha v) \\ \frac{dv}{dt} = w(\alpha u - \varepsilon v) \\ \frac{dw}{dt} = 1 - u^2 - v^2 \end{cases} \tag{4}$$

where u, v, and w denote system variables. α, ε and K represent the parameters of the system. Assuming that the step length h=0.01, the parameters α=4, ε=0.38, K=0.4, and the initial values u_0=0.1, v_0=0.1, w_0=0.1, then the attractor phase diagrams in this state are shown in Fig.1. Meanwhile, we can get the corresponding Lyapunov exponent LEs= (0.2331, 0, -0.3393), and the Lyapunov exponent dimension D_L=2.6870. Since the dimension of the system is fractional and the largest Lyapunov exponent is positive, the system is in chaotic state in this case.



(a) (b) (c)

FIGURE 1. Phase diagrams with α = 4, ε = 0.38, K = 0.4 (a) $u - v$ plane (b) $u - w$ plane (c) $u - v - w$ space

A. INFLUENCE OF SYSTEM PARAMETERS ON DYNAMIC CHARACTERISTICSC

In this subsection, we analyze the dynamic characteristics of the laser chaotic system by bifurcation diagram, Lyapunov exponential spectrum, and complexity diagram.

Set parameters $\alpha = 7$, $\varepsilon = 0.23$, $K = 0.5$. Step length $h = 0.01$, initial values $x_0 = 0.1$, $y_0 = 0.1$, $z_0 = 0.1$. For parameters α, ε, and K, if only one of them is changed, then when $\alpha \in (-15, 15)$, $\varepsilon \in (-8, 2)$, and $K \in (-2, 2)$, the corresponding bifurcation diagrams, Lyapunov exponential spectrums, and complexity diagrams are shown in Fig.2. From the observation in Fig.2, it can be found that the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3113734, IEEE Access

traversal intervals of all parameters are relatively large and have high complexity, so the laser chaotic system is suitable for information security communication.

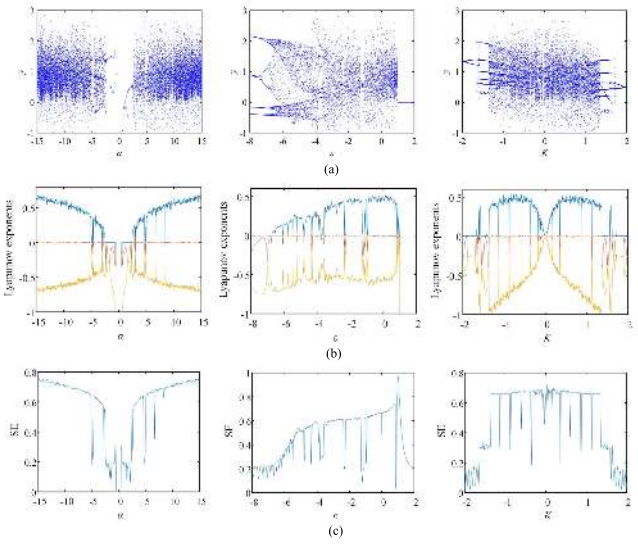


FIGURE 2. Dynamic characteristics of parameters α, ε, and K, (a) Bifurcation diagram (b) Lyapunov exponential spectrum (c) Complexity diagram

III. ENCRYPTION AND DECRYPTION SCHEMES

A. IMAGE ENCRYPTION PROCESS

The encryption system mainly includes two processes of scrambling and diffusion. The processing flowchart of encryption algorithm is given in Fig.3, and it can be described as:

Input: Plaintext image $I_{M\times N}$.

Step 1: Set the keys. All pixels of the input image $I_{M\times N}$ are summed and then quantized, and the quantized result is added to $\alpha, \varepsilon, K, u_0, v_0$, and w_0. The quantification process and key setting can be described as:

$$\begin{cases} q = 10^{-13} \times sum(sum(I)) \\ Keys = [\alpha + q; \varepsilon + q; K + q; u_0 + q; v_0 + q; w_0 + q] \end{cases} \tag{5}$$

Step 2: Iteratively generate 6 (m+ $M\times N$) chaotic pseudo-random sequences from the laser chaotic system, and abnegate the first m values to heighten the sensitivity of the system parameters. Among them, the chaotic pseudo-random sequences u, v, and w are used in the scrambling process, and the pseudo-random sequences p_1, p_2, and p_3 are utilized in the diffusion operation.

Step 3: Quantify the pseudo-random sequences u, v, and w to obtain the vectors C_u, C_v, and C_w. Then convert the vectors C_u, C_v, and C_w into $M \times N$ matrices U, V, and W.

$$\begin{cases} C_u = mod(floor(abs(u \times 10^{16})), M \times N) \\ C_v = mod(floor(abs(v \times 10^{16})), M \times N) \\ C_w = mod(floor(abs(w \times 10^{16})), M \times N) \end{cases} \tag{6}$$

$$\begin{cases} U = reshape(C_u(m : M \times N), M, N) \\ V = reshape(C_v(m : M \times N), M, N) \\ W = reshape(C_w(m : M \times N), M, N) \end{cases} \tag{7}$$

Step 4: Apply the U, V, and W obtained in step 3 to the point random scrambling algorithm, and generate scrambling image I_1. The scrambling process is expressed as:

$$\begin{cases} g = \mathrm{mod}(\begin{bmatrix} 1 & U(i,j) \times W(i,j) \\ V(i,j) & U(i,j) \times V(i,j) + 1 \end{bmatrix} \\ \qquad \begin{bmatrix} i \\ j \end{bmatrix}, \begin{bmatrix} M \\ N \end{bmatrix}) + \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ T = I_1(i,j); I_1(i,j) = I_1(g(1), g(2)); \\ \qquad I_1(g(1), g(2)) = T \end{cases} \tag{8}$$

Step 5: Quantify the pseudo-random sequence p_1, p_2, and p_3 generated in step 2 to obtain 3 random numbers P_1, P_2, and P_3.

$$\begin{cases} P_1 = (sum(abs(p_1) - floor(p_2)))/M \\ P_2 = (sum(abs(p_2) - floor(p_3)))/M \\ P_3 = (sum(abs(p_3) - floor(p_1)))/M \end{cases} \tag{9}$$

Step 6: Apply random numbers P_1, P_2, and P_3 to the improved gravitational model to diffuse the scrambled image I_1. Finally, the ciphertext image $C_{M\times N}$ is obtained.

$$\begin{cases} PP = \mathrm{mod}(round(h * \frac{P_1 i^4 + P_2 j^2 + P_1 P_2 {P_3}^2}{(P_1 - i)^2 + (P_2 - j)^2 + {P_3}^2}, 256) \\ C_{M\times N} = bitxor(\mathrm{uint8}(PP), I_1) \end{cases} \tag{10}$$

Output:Ciphertext image $C_{M\times N}$.

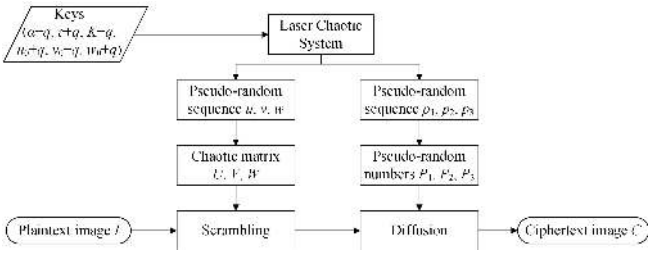


FIGURE 3. Processing flowchart of the encryption algorithm

B. IMAGE DECRYPTION PROCESS

Since each key is associated with the plaintext and related to the precision of quantification, it increases the difficulty of the attacker's deciphering and makes the cryptographic system more secure. The processing flowchart of decryption algorithm is given in Fig.4, and it can be expressed as:

Input: Ciphertext image $C_{M\times N}$.

Step 1: Generate 6 chaotic sequences S={u, v, w, p_1, p_2, p_3} based on the keys ($\alpha + q$, $\varepsilon + q$, $K + q$, $u_0 + q$, $v_0 + q$, $w_0 + q$).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3113734, IEEE Access

Step 2: The quantized random numbers P_1, P_2, P_3 are obtained from step 5 of the encryption process, and the reverse diffusion process is:

$$\begin{cases} PP = \mathrm{mod}(round(h * \frac{P_1 i^4 + P_2 j^2 + P_1 P_2 {P_3}^2}{(P_1 - i)^2 + (P_2 - j)^2 + {P_3}^2}), 256) \\ D_1 = bitxor(\mathrm{uint8}(PP), C_{M \times N}) \end{cases} \tag{11}$$

Step 3: Three chaotic matrixs U, V, and W are generated from step 3 of the encryption process. According to the inverse scrambling rule of chaotic random point scrambling, the image D_1 obtained by inverse diffusion is inversely scrambled. The inverse scrambling process is:

$$\begin{cases} g = \mathrm{mod}(\begin{bmatrix} 1 & U(i,j) \times W(i,j) \\ V(i,j) & U(i,j) \times V(i,j) + 1 \end{bmatrix} \\ \quad \begin{bmatrix} i \\ j \end{bmatrix}, \begin{bmatrix} M \\ N \end{bmatrix}) + \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ T = D_1(i,j); D_1(i,j) = D_1(g(1), g(2)); \\ \quad D_1(g(1), g(2)) = T \end{cases} \tag{12}$$

Step 4: Finally, the restored image $D_{M \times N}$ is generated.
Output:Decryption image $D_{M \times N}$.

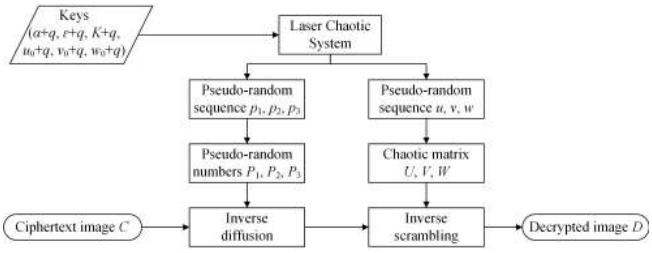


FIGURE 4. Processing flowchart of the decryption algorithm

IV. PERFORMANCE ANALYSIS OF THE PROPOSED ENCRYPTION SCHEME

A. SIMULATION RESULTS

The safety and feasibility of the proposed cryptosystem is analyzed in detail in this section. Set $\alpha = 7$,$\varepsilon = 0.23$, $K = 0.5$, $u_0 = 0.1$, $v_0 = 0.1$, $w_0 = 0.1$. Fig.5 (a), (d), (g) are "Camera", "Couple", and "Peppers" with a size of 256×256, and the corresponding encrypted images are shown in Fig.5 (b), (e), (h). When all the keys are correct, the restored images are shown in Fig.5 (c), (f), (i). As shown in the numerical simulation results, it can be seen that this encryption scheme can encrypt regular information into noise-like information, and attackers are impossible to get effective information from the ciphertext image.

B. KEY SPACE ANALISIS

The keys in this paper mainly include $\alpha + q$, $\varepsilon + q$, $K + q$, $u_0 + q$, $v_0 + q$, and $w_0 + q$, and the accuracies of all of them are shown in Tab.1. Hence, the total key space of the cryptosystem is $10^{(15+16+16+16+17+17)} \approx 2^{322}$, which is much larger than the theoretical requirement of 2^{100}. Besides,

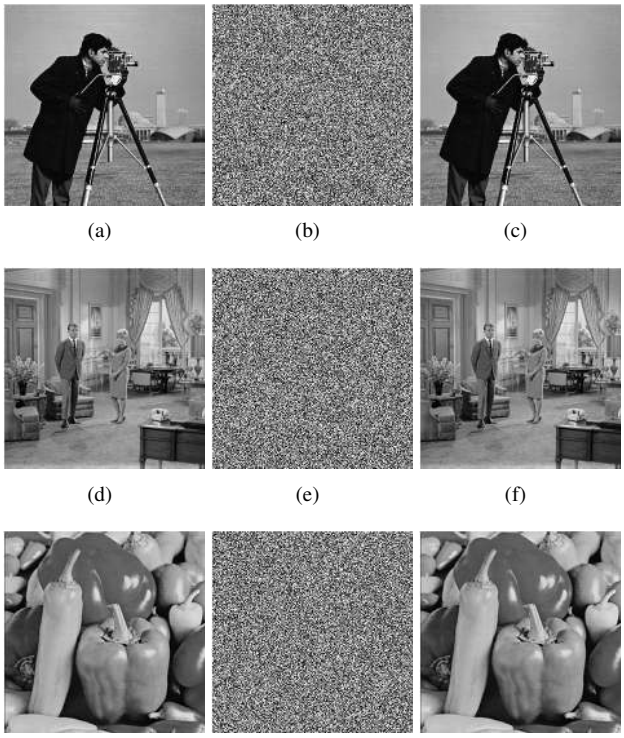


FIGURE 5. Simulation results of encryption and decryption

compared with the key space of other encryption algorithms in Tab.2. The analysis result indicates that our key space is lager. That is to say, the proposed encryption scheme can resist brute force attacks.

TABLE 1. The accuracy of keys

Accuracy	10^{-15}	10^{-16}	10^{-17}
Keys	$\alpha + q$	$\varepsilon + q, K + q, u_0 + q$	$v_0 + q, w_0 + q$

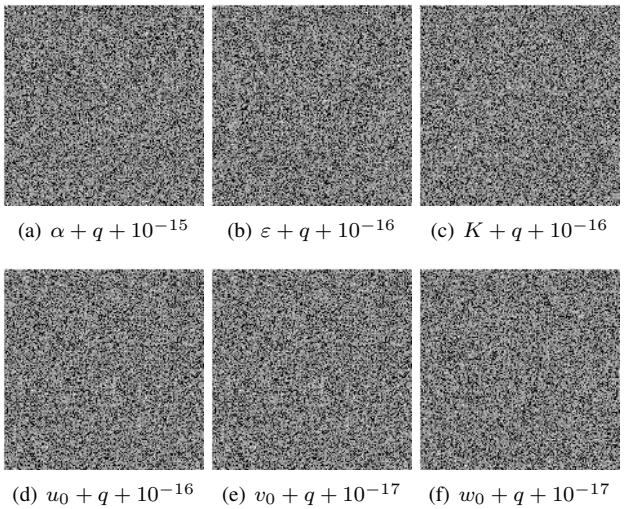
TABLE 2. Key space for different encryption schemes

Encryption scheme	Ref. [7]	Ref. [32]	Ref. [45]	Ref. [47]	**Ours**
Key space	2^{312}	2^{498}	2^{186}	2^{256}	$\mathbf{2^{322}}$

C. KEY SENSITIVITY ANALYSIS

Taking "Camera" as an example, small changes of 10^{-15}, 10^{-16}, and 10^{-17} are added to the decryption keys ($\alpha+q$, $\varepsilon+q$, $K+q$, u_0+q, v_0+q, w_0+q) in this paper respectively, and their decryption images are given in Fig.6. As shown in Fig.6 that the plaintext image cannot be recovered when decrypting with the illegal key. It shows that the slight change of the key can generate two completely different sequences. The context of cipher image is changed because of the sequences. Hence, the proposed cryptosystem has high key sensitivity.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3113734, IEEE Access



(a) $\alpha + q + 10^{-15}$ (b) $\varepsilon + q + 10^{-16}$ (c) $K + q + 10^{-16}$

(d) $u_0 + q + 10^{-16}$ (e) $v_0 + q + 10^{-17}$ (f) $w_0 + q + 10^{-17}$

FIGURE 6. Sensitivity test results under different keys

D. INFORMATION ENTROPY ANALYSIS

Information entropy is usually utilized to evaluate the uncertainty of pixel information. Mathematically, information entropy can be described as:

$$H(r) = -\sum_{j=0}^{2^n-1} p(r_j)\log_2 p(r_j) \tag{13}$$

where $p(r_j)$ is the probability of r_j. The expectation of the information entropy of 2^8-level gray image is equal to 8. The entropies of several standard images are given in Tab.3. As shown in the simulation results that the entropies of the ciphertext images are near to the expected value of 8. Therefore, the distributions of ciphertext images pixels are very irregular and have a good encryption effect.

TABLE 3. Information entropy of different images

Image (256×256)	Camera	Couple	Peppers	Girl	Woman
Plaintext image	7.0097	7.4000	7.5773	3.2981	7.1991
Ciphertext image	7.9972	7.9974	7.9973	7.9974	7.9971

E. DIFFERENTIAL ATTACK ANALYSIS

Differential attack analysis ensures that very small changes or modifications in ordinary images should bring significant differences in the encryption process. The number of pixels change rate (NPCR) and unified average changing intensity (UACI) are the two most commonly used test indicators ,and they are expressed as

$$NPCR = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{H(i,j)}{M \times N} \times 100\% \tag{14}$$

$$UACI = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|G(i,j) - G'(i,j)|}{255 \times M \times N} \times 100\% \tag{15}$$

$$H(i,j) = \begin{cases} 0 & G(i,j) = G'(i,j) \\ 1 & G(i,j) \neq G'(i,j) \end{cases} \tag{16}$$

where $G(i,j)$ and $G'(i,j)$ are the (i,j)-th pixel of image G and G' respectively. The test results of different images are shown in Tab.4 and Tab.5 that the NPCR and UACI in this paper are near to the expected value (99.6094% and 33.4635%). Therefore, the proposed cryptographic system can effectively propagate small differences in ordinary images to the entire cryptographic image, and the cryptographic system has high plaintext sensitivity.

F. HISTOGRAM ANALYSIS

The histograms of "Camera", "Couple" and "Peppers" are shown in Fig.7. Compared with the ups and downs of the plaintext images pixel distribution, the ciphertext images have a relatively uniform pixel distribution. In addition, the χ^2-test can quantitatively measure the difference in pixel distribution between the plaintext and ciphertext image. As shown in Tab.6, the χ^2-test values of different ciphertext images are all smaller than the critical values when the significance level is 0.1, 0.05, and 0.01, respectively. Therefore, the cryptosystem can hide the pixel information in the image very well.

G. CORRELATION ANALYSIS OF ADJACENT PIXELS

In general, plaintext images have high correlation in all directions, while the image encrypted by a security encryption system should have a low correlation. The correlation can be calculated as:

$$E(u) = \frac{1}{N}\sum_{i=1}^{N} u_i \tag{17}$$

$$D(u) = \frac{1}{N}\sum_{i=1}^{N} [u_i - E(u)]^2 \tag{18}$$

$$Cov(u,v) = \frac{1}{N}\sum_{i=1}^{N} [u_i - E(u)][v_i - E(v)] \tag{19}$$

$$R_{uv} = \frac{|Cov(u,v)|}{\sqrt{D(u)D(v)}} \tag{20}$$

We randomly choose 10,000 groups of adjacent pixels of different direction from the plaintext image as samples to test the correlation. The test result of "Camera" is shown in Fig.8 that the plaintext image has a high correlation in different directions, while the encrypted image is almost randomly scattered. Moreover, the correlation coefficients(CCs) of several standard images are given in Tab.7. As shown in the test results that the CCs of the plaintext images are very high. After being encrypted by the proposed algorithm, the CCs of the ciphertext images are very close to zero. Therefore, the proposed scheme greatly destroys the correlation of the plaintext image.

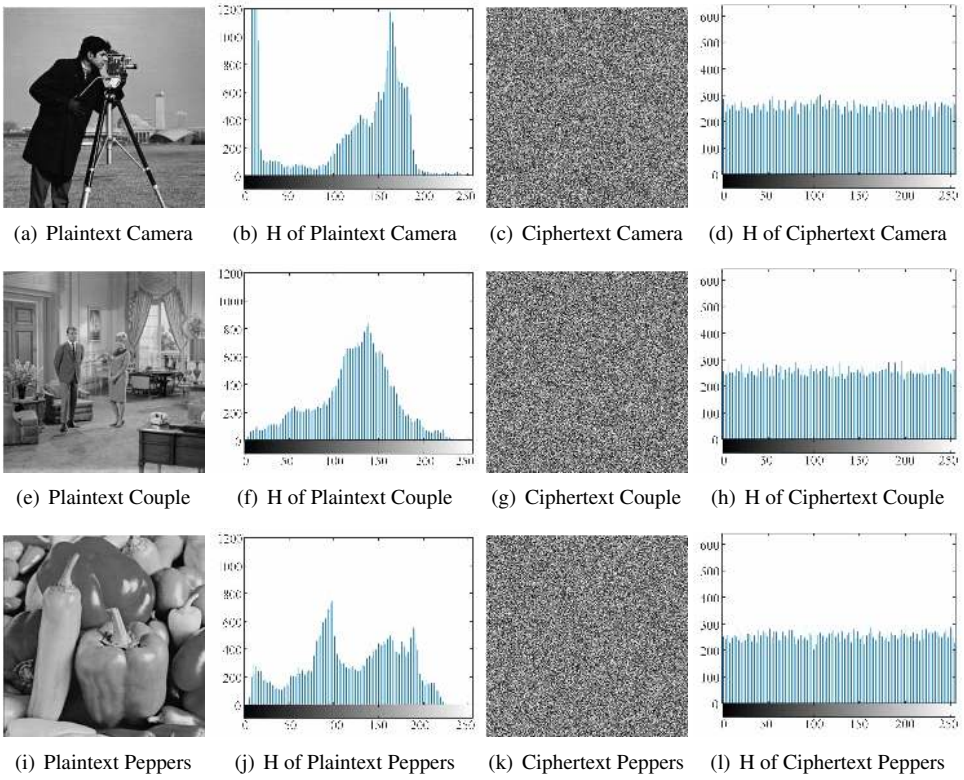
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3113734, IEEE Access

TABLE 4. NPCR value of different images

Image (256×256)	NPCR (%)	Critical Value (%)		
		$N^*_{0.05}$=99.5693	$N^*_{0.01}$=99.5527	$N^*_{0.001}$=99.5341
Camera	99.6185	Pass	Pass	Pass
Couple	99.6063	Pass	Pass	Pass
Peppers	99.6170	Pass	Pass	Pass
Girl	99.6048	Pass	Pass	Pass
Woman	99.6078	Pass	Pass	Pass

TABLE 5. UACI value of different images

Image (256×256)	UACI(%)	Critical Value (%)		
		$U^{*+}_{0.05}$=33.2824 $U^{*-}_{0.05}$=33.6447	$U^{*+}_{0.01}$=33.2255 $U^{*-}_{0.01}$=33.7016	$U^{*+}_{0.001}$=33.1594 $U^{*-}_{0.001}$=33.7677
Camera	33.4731	Pass	Pass	Pass
Couple	33.4702	Pass	Pass	Pass
Peppers	33.4704	Pass	Pass	Pass
Girl	33.4618	Pass	Pass	Pass
Woman	33.4831	Pass	Pass	Pass



(a) Plaintext Camera (b) H of Plaintext Camera (c) Ciphertext Camera (d) H of Ciphertext Camera

(e) Plaintext Couple (f) H of Plaintext Couple (g) Ciphertext Couple (h) H of Ciphertext Couple

(i) Plaintext Peppers (j) H of Plaintext Peppers (k) Ciphertext Peppers (l) H of Ciphertext Peppers

FIGURE 7. Histograms of different images

H. ROBUSTNESS ANALYSIS

Because digital images are transmitted through the network or stored in physical media, they are susceptible to noise pollution or partial data loss. A good image encryption system should have good robustness performance against noise and partial data loss. This section will analyze the robustness of the proposed algorithm through Gaussian noise(GN), Salt & Pepper noise(SPN), and shear attack.

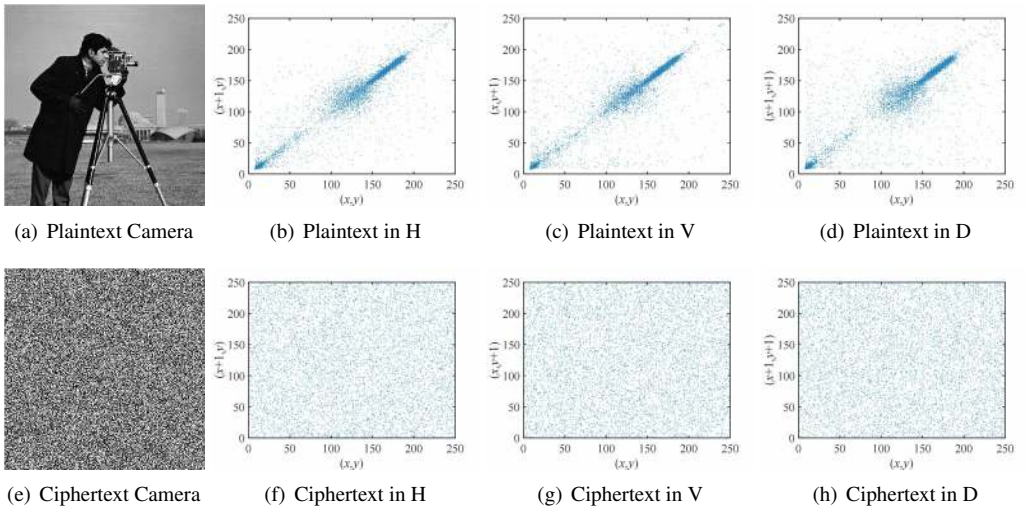
1) Noise attack analysis

A good image encryption system should have good robustness performance against noise attack. In order to simulate

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3113734, IEEE Access

TABLE 6. χ^2 test results of different images

Image (256×256)	χ^2-value(Plaintext image)	χ^2-value(Ciphertext image)	Critical value(2^8-level)		
			$\chi^2_{0.1} = 284.3360$	$\chi^2_{0.05} = 293.2478$	$\chi^2_{0.01} = 310.4574$
Camera	1.1097×10^5	254.6250	Pass	Pass	Pass
Couple	5.4617×10^4	235.5234	Pass	Pass	Pass
Peppers	3.1696×10^4	247.5703	Pass	Pass	Pass
Girl	2.0847×10^6	236.8828	Pass	Pass	Pass
Woman	6.5357×10^4	264.5313	Pass	Pass	Pass



(a) Plaintext Camera (b) Plaintext in H (c) Plaintext in V (d) Plaintext in D

(e) Ciphertext Camera (f) Ciphertext in H (g) Ciphertext in V (h) Ciphertext in D

FIGURE 8. Correlation test of adjacent pixels

TABLE 7. CCs of different images

Image	Plaintext image			Ciphertext image		
(256×256)	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Camera	0.9588	0.9338	0.9083	0.0003	-0.0011	-0.0035
Couple	0.9344	0.9262	0.8775	-0.0044	-0.0070	-0.0002
Peppers	0.9716	0.9650	0.9394	-0.0018	-0.0001	0.0015
Girl	0.9477	0.9615	0.9326	-0.0043	0.0035	-0.0008
Woman	0.9360	0.9051	0.8640	0.0016	-0.0044	-0.0034

the noise interference that may occur during transmission, different intensities of SPN and GN are added into the ciphertext images. Fig.9 shows the decrypted results after adding noise to the ciphertext images. As shown in Fig.9, the encrypted images can still be restored to the plaintext images after receiving different types of noise. Although the decrypted images contain some noise, most of the information of the plaintext image can still be identified.

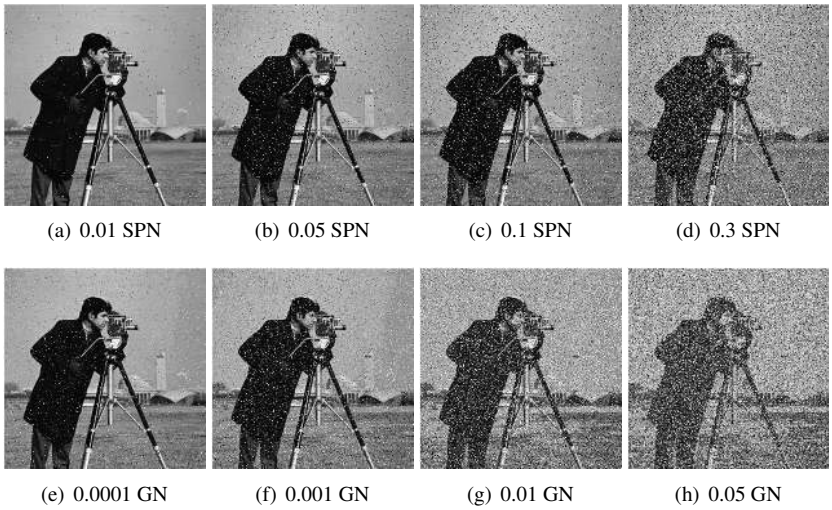
2) Shear attack analysis

By cutting part of the encrypted image information and restoring it to the original image. The results of 1/16, 1/8, 1/4, 1/2 cut size and decryption are recorded in Fig.10. As shown in Fig.10, although the qualities of the decrypted images decrease with the expansion of the cropping range, they can still be visually recognized. Therefore, the proposed encryption algorithm has high robustness.

I. SAFETY PERFORMANCE COMPARISON

In this subsection, we compare this algorithm with the algorithm Ref. [7], [32], [45], [47] from the three aspects of adjacent pixel correlation, anti-differential attack, and information entropy. As shown from the comparison with different schemes in Tab.8 that the ciphertext images encrypted by the proposed cryptosystem have a lower correlation, and the NPCR and UACI are closer to the expected values. At the same time, the information entropies of the ciphertext images are near to the theoretical value 8. Therefore, the algorithm in this paper has better security performance.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3113734, IEEE Access



(a) 0.01 SPN (b) 0.05 SPN (c) 0.1 SPN (d) 0.3 SPN

(e) 0.0001 GN (f) 0.001 GN (g) 0.01 GN (h) 0.05 GN

FIGURE 9. Analysis of SPN and GN attack with different intensity

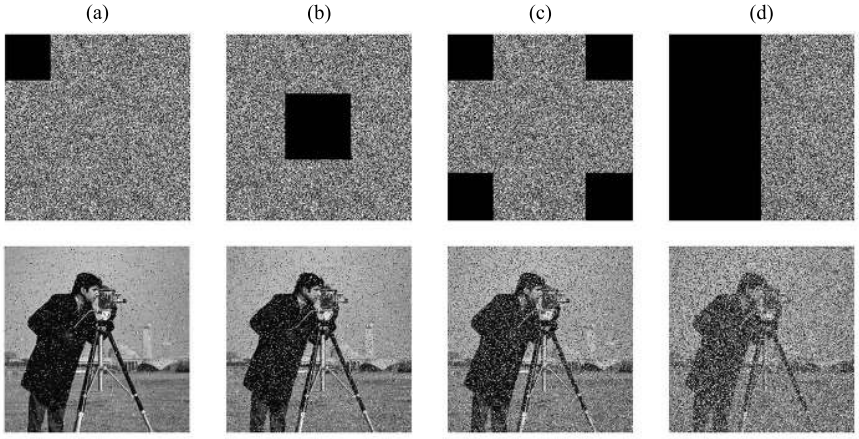


FIGURE 10. Analysis of shear attack with different intensity (a) Shear size $= 1/16$ (b) Shear size $= 1/8$ (c) Shear size $= 1/4$ (d) Shear size $= 1/2$

TABLE 8. Compare the security performance of different encryption algorithms

Image (256*256)	Algorithm	CC(Ciphertext imaage)			NPCR(%)	UACI(%)	Entropy
		Horizontal	Vertical	Diagonal			
Camera	Ref. [7]	0.0063	-0.0014	0.0168	99.5749	33.3691	7.9955
	Ref. [32]	0.0083	0.0080	0.0015	99.6193	33.3891	9.9968
	Ref. [45]	-	-	-	99.6261	33.4946	7.9973
	Ref. [47]	-0.0047	-0.0195	0.0279	99.6105	33.6862	7.9964
	Ours	**0.0003**	**-0.0011**	**-0.0035**	**99.6185**	**33.4731**	**7.9972**
Couple	Ref. [7]	-0.0122	0.0262	-0.0257	99.5606	33.3723	7.9951
	Ref. [32]	0.0043	0.0045	0.0033	99.6153	33.5017	7.9956
	Ref. [45]	0.0022	0.0066	0.0079	99.5834	33.3945	7.9972
	Ref. [47]	-0.0236	-0.0045	0.0016	99.6312	33.7252	7.9980
	Ours	**-0.0044**	**-0.0070**	**-0.0002**	**99.6063**	**33.4702**	**7.9974**
Peppers	Ref. [7]	0.0194	-0.0091	0.0123	99.5808	33.3540	7.9965
	Ref. [32]	-0.0013	0.0067	0.0020	99.5815	33.4946	7.9963
	Ref. [45]	0.0117	0.0171	0.0030	99.6139	33.5195	7.9972
	Ref. [47]	0.0071	-0.0065	-0.0165	99.6236	33.7386	7.9958
	Ours	**-0.0018**	**-0.0001**	**0.0015**	**99.6170**	**33.4704**	**7.9973**

V. CONCLUSION

In this paper, a new image encryption scheme based on a modified optically injected semiconductor laser chaotic system, which is combined with random point scrambling and an improved gravitational model is proposed. In the proposed encryption system, since the system keys are associated with the plaintext image, different plaintext image inputs will get different keys, so that small changes in pixels in the plaintext image will result in two completely different ciphertext images. Therefore, it greatly improves the anti-differential attack capability of the encryption scheme. Secondly, the starting position of the scrambling process is random, and the process of different plaintext scrambling is different. Finally, the random numbers obtained from different plaintexts are inconsistent, and the calculation process of the gravitational model is nonlinear. Therefore, the proposed encryption algorithm exhibits good confusion and diffusion characteristics. The security performance analysis results show that the proposed encryption algorithm has good security and efficiency, can resist a variety of attacks, and has high robustness against noise. Therefore, this scheme is a better alternative to image encryption and can better meet today's needs. In future work, we will study high-security and high-efficiency image compression encryption algorithms to ease the pressure of network transmission.

ACKNOWLEDGEMENTS

This work was supported by the National Science Foundation for Young Scientists of China (Grant No.61802041); Doctoral Scientific Research Foundation of Liaoning Province of China (Grant No. 2020-BS-210).

AUTHOR CONTRIBUTIONS

Xuejun Li designed and carried out experiments, data analyzed and manuscript wrote. Bo Li and Bo Sun made the theoretical guidance for this paper. Zhisen Wang and Caiyin Wang carried out experiment. Jun Mou improved the algorithm. All authors reviewed the manuscript.

CONFLICT OF INTEREST

No conflicts of interests about the publication by all authors.

REFERENCES

[1] X. Peng and Y. Zeng, "Image encryption application in a system for compounding self-excited and hidden attractors," Chaos, Solitons & Fractals, vol. 139, 2020, doi: 10.1016/j.chaos.2020.110044.

[2] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, "Cross-plane colour image encryption using a two-dimensional logistic tent modular map," Information Sciences, vol. 546, pp. 1063-1083, 2021, doi: 10.1016/j.ins.2020.09.032.

[3] X. Yuan, L. Zhang, J. Chen, K. Wang, and D. Zhang, "Multiple-image encryption scheme based on ghost imaging of Hadamard matrix and spatial multiplexing," Applied Physics B, vol. 125, no. 9, 2019, doi: 10.1007/s00340-019-7286-9.

[4] I. Yasser, F. Khalifa, M. A. Mohamed, and A. S. Samrah, "A New Image Encryption Scheme Based on Hybrid Chaotic Maps," Complexity, vol. 2020, pp. 1-23, 2020, doi: 10.1155/2020/9597619.

[5] Z. Hua, B. Xu, F. Jin, and H. Huang, "Image Encryption Using Josephus Problem and Filtering Diffusion," IEEE Access, vol. 7, pp. 8660-8674, 2019, doi: 10.1109/access.2018.2890116.

[6] S. A. Banu and R. Amirtharajan, "A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach," Med Biol Eng Comput, vol. 58, no. 7, pp. 1445-1458, Jul 2020, doi: 10.1007/s11517-020-02178-w.

[7] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," Optics and Lasers in Engineering, vol. 66, pp. 10-18, 2015, doi: 10.1016/j.optlaseng.2014.08.005.

[8] J. Chen, L. Chen, and Y. Zhou, "Universal chosen-ciphertext attack for a family of image encryption schemes," IEEE Transactions on Multimedia, pp. 1-1, 2020, doi: 10.1109/tmm.2020.3011315.

[9] X. Li, J. Mou, L. Xiong, Z. Wang, and J. Xu, "Fractional-order double-ring erbium-doped fiber laser chaotic system and its application on image encryption," Optics & Laser Technology, vol. 140, p. 107074, 2021, doi: 10.1016/j.optlastec.2021.107074.

[10] G.-D. Ye, X.-L. Huang, L. Y. Zhang, and Z.-X. Wang, "A self-cited pixel summation based image encryption algorithm," Chinese Physics B, vol. 26, no. 1, p. 010501, 2017, doi: 10.1088/1674-1056/26/1/010501.

[11] S. Wang, C. Wang, and C. Xu, "An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm," Optics and Lasers in Engineering, vol. 128, 2020, doi: 10.1016/j.optlaseng.2019.105995.

[12] S. K.U and A. Mohamed, "A novel image encryption scheme using both pixel level and bit level permutation with chaotic map," Applied Soft Computing, vol. 90, 2020, doi: 10.1016/j.asoc.2020.106162.

[13] T. Liu, H. Yan, S. Banerjee, and J. Mou, "A fractional-order chaotic system with hidden attractor and self-excited attractor and its DSP implementation," Chaos Solitons & Fractals, vol. 145, no. 2, p. 110791, 2021, doi: 10.1016/j.chaos.2021.110791.

[14] X. Ma, J. Mou, J. Liu, C. Ma, F. Yang, and X. Zhao, "A novel simple chaotic circuit based on memristor–memcapacitor," Nonlinear Dynamics, vol. 100, no. 3, pp. 2859-2876, 2020/05/01 2020, doi: 10.1007/s11071-020-05601-x.

[15] X. Chen et al., "Pseudorandom Number Generator Based on Three Kinds of Four-Wing Memristive Hyperchaotic System and Its Application in Image Encryption," Complexity, vol. 2020, p. 8274685, 2020/12/24 2020, doi: 10.1155/2020/8274685.

[16] C. Xu, J. Sun, and C. Wang, "An Image Encryption Algorithm Based on Random Walk and Hyperchaotic Systems," International Journal of Bifurcation and Chaos, vol. 30, no. 04, 2020, doi: 10.1142/s0218127420500601.

[17] T. Liu, S. Banerjee, H. Yan, and J. Mou, "Dynamical analysis of the improper fractional-order 2D-SCLMM and its DSP implementation," The European Physical Journal Plus, vol. 136, no. 5, p. 506, 2021/05/07 2021, doi: 10.1140/epjp/s13360-021-01503-y.

[18] C. Ma, J. Mou, P. Li, and T. Liu, "Dynamic analysis of a new two-dimensional map in three forms: integer-order, fractional-order and improper fractional-order," The European Physical Journal Special Topics, 2021/06/02 2021, doi: 10.1140/epjs/s11734-021-00133-w.

[19] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A New Image Encryption Algorithm for Grey and Color Medical Images," IEEE Access, vol. PP, no. 99, pp. 1-1, 2021, doi: 10.1109/ACCESS.2021.3063237.

[20] A. Sahasrabuddhe and D. S. Laiphrakpam, "Multiple images encryption based on 3D scrambling and hyper-chaotic system," Information Sciences, vol. 550, pp. 252-267, 2021, doi: 10.1016/j.ins.2020.10.031.

[21] Fridrich and Jiri, "Symmetric Ciphers Based on Two-Dimensional Chaotic Maps," International Journal of Bifurcation & Chaos, vol. 8, no. 06, pp. 1259-1284, 1998, doi: 10.1142/S021812749800098X.

[22] J. Wang, Q.-H. Wang, and Y. Hu, "Image Encryption Using Compressive Sensing and Detour Cylindrical Diffraction," IEEE Photonics Journal, vol. 10, no. 3, pp. 1-14, 2018, doi: 10.1109/jphot.2018.2831252.

[23] H. Fan, K. Zhou, E. Zhang, W. Wen, and M. Li, "Subdata image encryption scheme based on compressive sensing and vector quantization," Neural Computing and Applications, vol. 32, no. 16, pp. 12771-12787, 2020, doi: 10.1007/s00521-020-04724-x.

[24] Y. Song, Z. Zhu, W. Zhang, L. Guo, X. Yang, and H. Yu, "Joint image compression–encryption scheme using entropy coding and compressive sensing," Nonlinear Dynamics, vol. 95, no. 3, pp. 2235-2261, 2018, doi: 10.1007/s11071-018-4689-9.

[25] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing," Optics & Laser Technology, vol. 82, pp. 121-133, 2016, doi: 10.1016/j.optlastec.2016.02.018.

[26] J. Xu, J. Mou, J. Liu, and J. Hao, "The image compression–encryption algorithm based on the compression sensing and fractional-order chaotic system," The Visual Computer, 2021, doi: 10.1007/s00371-021-02085-7.

[27] X. Chai, H. Wu, Z. Gan, D. Han, Y. Zhang, and Y. Chen, "An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing," Information Sciences, vol. 556, pp. 305-340, 2021, doi: 10.1016/j.ins.2020.10.007.

[28] X. Zhang, F. Han, and Y. Niu, "Chaotic Image Encryption Algorithm Based on Bit Permutation and Dynamic DNA Encoding," Comput Intell Neurosci, vol. 2017, p. 6919675, 2017, doi: 10.1155/2017/6919675.

[29] D. H. ElKamchouchi, H. G. Mohamed, and K. H. Moussa, "A Bijective Image Encryption System Based on Hybrid Chaotic Map Diffusion and DNA Confusion," Entropy, vol. 22, no. 2, 2020, doi: 10.3390/e22020180.

[30] L. Huang, S. Wang, J. Xiang, and Y. Sun, "Chaotic Color Image Encryption Scheme Using Deoxyribonucleic Acid (DNA) Coding Calculations and Arithmetic over the Galois Field," Mathematical Problems in Engineering, vol. 2020, pp. 1-22, 2020, doi: 10.1155/2020/3965281.

[31] T. Wang and M.-h. Wang, "Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding," Optics & Laser Technology, vol. 132, 2020, doi: 10.1016/j.optlastec.2020.106355.

[32] Y.-G. Yang, B.-W. Guan, J. Li, D. Li, Y.-H. Zhou, and W.-M. Shi, "Image compression-encryption scheme based on fractional order hyper-chaotic systems combined with 2D compressed sensing and DNA encoding," Optics & Laser Technology, vol. 119, 2019, doi: 10.1016/j.optlastec.2019.105661.

[33] Y. Sha, Y. Cao, H. Yan, X. Gao, and J. Mou, "An image encryption scheme based on IAVL permutation scheme and DNA operations," IEEE Access, vol. PP, no. 99, pp. 1-1, 2021, doi: 10.1109/ACCESS.2021.3094563.

[34] H. Liu, A. Kadir, and C. Xu, "Cryptanalysis and constructing S-Box based on chaotic map and backtracking," Applied Mathematics and Computation, vol. 376, 2020, doi: 10.1016/j.amc.2020.125153.

[35] H. Liu, B. Zhao, and L. Huang, "Quantum Image Encryption Scheme Using Arnold Transform and S-box Scrambling," Entropy, vol. 21, no. 4, 2019, doi: 10.3390/e21040343.

[36] Y. Zhang, "The unified image encryption algorithm based on chaos and cubic S-Box," Information Sciences, vol. 450, pp. 361-377, 2018, doi: 10.1016/j.ins.2018.03.055.

[37] Y. Hu, S. Yu, and Z. Zhang, "On the Security Analysis of a Hopfield Chaotic Neural Network-Based Image Encryption Algorithm," Complexity, vol. 2020, pp. 1-10, 2020, doi: 10.1155/2020/2051653.

[38] F. Yang, J. Mou, K. Sun, and R. Chu, "Lossless image compression-encryption algorithm based on BP neural network and chaotic system," Multimedia Tools and Applications, vol. 79, no. 27-28, pp. 19963-19992, 2020, doi: 10.1007/s11042-020-08821-w.

[39] L. Chen, H. Yin, T. Huang, L. Yuan, S. Zheng, and L. Yin, "Chaos in fractional-order discrete neural networks with application to image encryption," Neural Netw, vol. 125, pp. 174-184, May 2020, doi: 10.1016/j.neunet.2020.02.008.

[40] D. Ouyang, J. Shao, H. Jiang, S. K. Nguang, and H. T. Shen, "Impulsive synchronization of coupled delayed neural networks with actuator saturation and its application to image encryption," Neural Netw, vol. 128, pp. 158-171, Aug 2020, doi: 10.1016/j.neunet.2020.05.016.

[41] H. Huang, S. Yang, and R. Ye, "Efficient symmetric image encryption by using a novel 2D chaotic system," IET Image Processing, vol. 14, no. 6, pp. 1157-1163, 2020, doi: 10.1049/iet-ipr.2019.0551.

[42] B. Li, X. Liao, and Y. Jiang, "A novel image encryption scheme based on logistic map and dynatomic modular curve," Multimedia Tools and Applications, vol. 77, no. 7, pp. 8911-8938, 2017, doi: 10.1007/s11042-017-4786-7.

[43] J. Liu, D. Yang, H. Zhou, and S. Chen, "A digital image encryption algorithm based on bit-planes and an improved logistic map," Multimedia Tools and Applications, vol. 77, no. 8, pp. 10217-10233, 2017, doi: 10.1007/s11042-017-5406-2.

[44] J. Chen, F. Han, W. Qian, Y.-D. Yao, and Z.-l. Zhu, "Cryptanalysis and improvement in an image encryption scheme using combination of the 1D chaotic map," Nonlinear Dynamics, vol. 93, no. 4, pp. 2399-2413, 2018, doi: 10.1007/s11071-018-4332-9.

[45] Y. Liu, Z. Qin, X. Liao, and J. Wu, "Cryptanalysis and enhancement of an image encryption scheme based on a 1-D coupled Sine map," Nonlinear Dynamics, vol. 100, no. 3, pp. 2917-2931, 2020, doi: 10.1007/s11071-020-05654-y.

[46] H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," Signal Processing, vol. 113, pp. 104-112, 2015, doi: 10.1016/j.sigpro.2015.01.016.

[47] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," Information Sciences, vol. 297, pp. 80-94, 2015, doi: 10.1016/j.ins.2014.11.018.

[48] Q. Liu and L. Liu, "Color Image Encryption Algorithm Based on DNA Coding and Double Chaos System," IEEE Access, vol. 8, pp. 83596-83610, 2020, doi: 10.1109/access.2020.2991420.

[49] C. Li, S. Li, G. Alvarez, G. Chen, and K.-T. Lo, "Cryptanalysis of a chaotic block cipher with external key and its improved version," Chaos, Solitons & Fractals, vol. 37, no. 1, pp. 299-307, 2008, doi: 10.1016/j.chaos.2006.08.025.

[50] S. T. Kingni, J. H. Mbe, and P. Woafo, "Semiconductor lasers driven by self-sustained chaotic electronic oscillators and applications to optical chaos cryptography," Chaos, vol. 22, no. 3, p. 033108, Sep 2012, doi: 10.1063/1.4733702.

[51] F. Yang, J. Mou, C. Ma, and Y. Cao, "Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application," Optics and Lasers in Engineering, vol. 129, 2020, doi: 10.1016/j.optlaseng.2020.106031.

[52] S.-Y. Wang, J.-F. Zhao, X.-F. Li, and L.-T. Zhang, "Image Blocking Encryption Algorithm Based on Laser Chaos Synchronization," Journal of Electrical and Computer Engineering, vol. 2016, pp. 1-14, 2016, doi: 10.1155/2016/4138654.

[53] T. Sivakumar and P. Li, "A secure image encryption method using scan pattern and random key stream derived from laser chaos," Optics & Laser Technology, vol. 111, pp. 196-204, 2019, doi: 10.1016/j.optlastec.2018.09.048.

[54] Sebastian et al., "A unifying view of bifurcations in a semiconductor laser subject to optical injection," Optics Communications, vol. 172, no. 1-6, pp. 279-295, 1999, doi: 10.1016/S0030-4018(99)00603-3.

[55] Y.-D. Chu, X.-F. Li, J.-G. Zhang, and Y.-X. Chang, "Nonlinear dynamics analysis of a modified optically injected semiconductor lasers model," Chaos, Solitons & Fractals, vol. 41, no. 1, pp. 14-27, 2009, doi: 10.1016/j.chaos.2007.11.004.

XUEJUN LI received the B.S. degree of HeFei University of Technology, HeFei, China, in 2019. He is currently pursuing the M.S. degree in Optical Engineering at Dalian Polytechnic University, Dalian, China. His mainly interest includes chaos theory and chaotic digital image cryptosystem.

BO LI received the B.S. degree in communication engineering in 2008 and the PH.D. degree in signal and information processing from Harbin Engineering University, China, in 2013. He is currently a lecturer in the school of information science and engineering of Dalian Polytechnic University in China and has published many journals and conference articles. He is mainly engaged in the research on the theory and application of evolutionary computing, optimal operation of smart microgrid and energy dispatching.

BO SUN received the M.S. degree in law from Dalian Maritime University and Ph.D. degree in economics from Dongbei University of Finance and Economics, Dalian, China. She is currently an associate professor at the School of Management, Dalian Polytechnic University, China. Her mainly research interest includes the industrial economics, regional economics, information security and regulatory environment.

ZHISEN WANG received B.S. degree, the M.S. degree in Jilin University, Jilin, China, and he received the Ph.D. degree in Electrical and communication engineering from Tohoku University, Sendai, Japan, in 2007. He is currently a Professor at the School of Information Science and Engineering, Dalian Polytechnic University. His research interests include Wireless communication and network, digital signal processing, IoT theory and technology.

CAIYIN WANG received the B.S. degree, the M.S. degree in printing and packaging engineering from Wuhan university, Wuhan, China, and the Ph.D. degree in electronic and information engineering from Dalian University of technology, Dalian, China. She is currently an associate professor at the department of printing and packaging engineering, Dalian Polytechnic University, Dalian, China. Her mainly research interest includes the digital image processing and information security.

JUN MOU received the B.S. degree, the M.S. degree and Ph.D. degree in physics and electronics from Central South University, Changsha, China. He is currently an associate professor at the School of Information Science and Engineering, Dalian Polytechnic University, China. His mainly research interest includes the nonlinear system control, secure communication, power system automation and smart grid research.