Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

A joint image compression and encryption scheme based on a novel coupled map lattice system and DNA operations*#

Yuanyuan LI[1], Xiaoqing YOU[2], Jianquan LU[†‡3], Jungang LOU[4,5]

[1]*Department of Applied Mathematics, College of Science, Nanjing Forestry University, Nanjing 210037, China*
[2]*School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China*
[3]*Department of Systems Science, School of Mathematics, Southeast University, Nanjing 210096, China*
[4]*Yangtze Delta Region (Huzhou) Institute of Intelligent Transportation, Huzhou University, Huzhou 313000, China*
[5]*School of Computer Science and Technology, Zhejiang Normal University, Jinhua 321004, China*
[†]E-mail: jqluma@seu.edu.cn

Received Dec. 16, 2022; Revision accepted Mar. 2, 2023; Crosschecked Apr. 25, 2023

Abstract: In this paper, an efficient image encryption scheme based on a novel mixed linear–nonlinear coupled map lattice (NMLNCML) system and DNA operations is presented. The proposed NMLNCML system strengthens the chaotic characteristics of the system, and is applicable for image encryption. The main advantages of the proposed method are embodied in its extensive key space; high sensitivity to secret keys; great resistance to chosen-plaintext attack, statistical attack, and differential attack; and good robustness to noise and data loss. Our image cryptosystem adopts the architecture of scrambling, compression, and diffusion. First, a plain image is transformed to a sparsity coefficient matrix by discrete wavelet transform, and plaintext-related Arnold scrambling is performed on the coefficient matrix. Then, semi-tensor product (STP) compressive sensing is employed to compress and encrypt the coefficient matrix. Finally, the compressed coefficient matrix is diffused by DNA random encoding, DNA addition, and bit XOR operation. The NMLNCML system is applied to generate chaotic elements in the STP measurement matrix of compressive sensing and the pseudo-random sequence in DNA operations. An SHA-384 function is used to produce plaintext secret keys and thus makes the proposed encryption algorithm highly sensitive to the original image. Simulation results and performance analyses verify the security and effectiveness of our scheme.

Key words: Compressive sensing; Coupled map lattice (CML); DNA operations; Semi-tensor product
https://doi.org/10.1631/FITEE.2200645 **CLC number:** TN919.81

1 Introduction

Compressive sensing (CS) can compress and encrypt images simultaneously, so it is very suitable for digital image encryption (Rani et al., 2018; Testa et al., 2020; Chai et al., 2022b). CS uses a measurement matrix to compress high-dimensional sparse or compressible signals. The number of samples can be far less than the number of samples restricted by Nyquist's sampling theorem, while the original signal can still be reconstructed from fewer samples (Donoho, 2006). The compression sampling process can be considered as an encryption process, and the measurement matrix as a secret key has been proved to have sufficient computational security (Sreedhanya and Soman, 2012; Fira, 2015) to resist violent attacks (Wu CW et al., 2020). Some recent studies that investigated image encryption based on

‡ Corresponding author
* Project supported by the National Natural Science Foundation of China (Nos. 11901297 and 61973078)
# Electronic supplementary materials: The online version of this article (https://doi.org/10.1631/FITEE.2200645) contains supplementary materials, which are available to authorized users
ORCID: Yuanyuan LI, https://orcid.org/0000-0001-8179-7426; Jianquan LU, https://orcid.org/0000-0003-4423-6034
© Zhejiang University Press 2023

CS can be found in Zhou et al. (2021) and Chai et al. (2022a). However, the realization of CS on image encryption still faces the following three challenges: (1) An extremely large measurement matrix is still needed when encrypting large images, and it will waste a lot of bandwidth resources if all the elements of the measurement matrix are transmitted as secret keys; (2) CS is essentially a linear measurement process, so it cannot resist known-plaintext attacks (NPAs) or chosen-plaintext attacks (CPAs); (3) The CS reconstruction process is complicated and generally takes a long time.

For the first challenge, a classic solution is to combine chaotic cryptography with CS (Kafedziski and Stojanovski, 2011; Li LX et al., 2020). The security measurement matrix is generated by a chaotic system. As long as the encrypter and decrypter negotiate the structure of the chaotic system, and the initial values of the chaotic system can be transmitted as secret keys, the time-consuming problem of transmitting each element of the measurement matrix can be solved (Shao et al., 2019). Therefore, the randomness of the chaotic system has a vital impact on the performance of an encryption system.

Impulsive coupled networks also have some applications in digital image processing technology (Li XD et al., 2019, 2020). Research has shown that the information communication with a spatiotemporal chaotic system based on a coupled map lattice (CML) is more secure than that with a single map (Kaneko, 1993; Wang Y et al., 2011; Wang XY and Wang, 2012; Zhong and Xu, 2015), because of its larger parameter space, better randomness, more chaotic sequences, and wider range of choices about the initial conditions (Zhang YQ and Wang, 2014; Zhong and Xu, 2015; Xu et al., 2016; Guo et al., 2018). Therefore, a CML system is applicable for secret key design in data protection, but the periodic windows in the bifurcation diagram of the CML system are still large and the spatial ergodicity of the randomness of time series is reduced. In addition, the small range of logistic map parameters restricts encryption schemes. Zhang YQ and Wang (2014) proposed a mixed linear–nonlinear coupled map lattice (MLNCML) system and obtained a larger range of parameters for chaotic behaviors, higher percentage of lattices in chaotic behaviors for most parameters, and fewer periodic windows in bifurcation diagrams for image encryption.

However, the range of logistic map parameters in MLNCML is not large enough, and the randomness of MLNCML is unstable. Therefore, we propose a novel mixed linear–nonlinear coupled map lattice (NMLNCML) system for our image encryption scheme, which further increases the range of logistic map parameters, improves the stability of chaotic features in Kolmogorov–Sinai entropy, and reduces the number of periodic windows in bifurcation diagrams.

In terms of the second challenge of CS, researchers have introduced plaintext keys and added scrambling and diffusion. Among them, DNA computation has been applied to the scrambling and diffusion process due to its great characteristics such as high parallelism, improved memory space, and very low power consumption (Song and Qiao, 2015; Chai et al., 2017; Chen JX et al., 2018; Hu HH et al., 2018; Feng et al., 2019). Song and Qiao (2015) proposed an image encryption scheme by combining DNA coding technology with a CML system that uses a nonlinear logistic map. Chen JX et al. (2018) proposed a self-adaptive encryption algorithm using DNA random encoding and DNA XOR operations with a hyperchaotic Lorenz system. Hu HH et al. (2018) designed a parallel image encryption algorithm based on DNA sequence addition operation and complement operation, in which the chaotic sequence was generated by the integer chaotic system. Chen L et al. (2022) provided a medical privacy protection scheme based on chaos and DNA coding using two coupled chaotic systems to produce cryptographic primitives. These results illustrated that DNA computation could obtain good performance in image encryption.

Regarding the third challenge of CS for image encryption, Xie et al. (2016) initially proposed a model of semi-tensor product compressive sensing (STP-CS). The STP tool has been extensively applied to study Boolean networks, feedback shift registers, and some other problems (Lu et al., 2018, 2021). The model breaks the dimension matching limit and thus reduces the space occupied by the measurement matrix. The STP-CS theory was then applied in image encryption for wireless body area networks by Li LX et al. (2019). As the size of the measurement matrix is reduced, the energy consumption of the sensor nodes in the network is reduced. Li LX et al. (2019) focused on the energy-saving characteristic

of the STP-CS model, but here we use its parallel reconstruction feature to improve the decryption speed.

In this paper, we present a new scheme for image encryption that takes advantages of the NMLNCML system and DNA operations in CS. The proposed NMLNCML system strengthens the chaotic characteristics (e.g., increased range of logistic map parameters, more stable randomness in Kolmogorov–Sinai entropy, and reduced number of periodic windows in bifurcation diagrams) of the system, which is very suitable for image encryption. We apply the NMLNCML system to generate the measurement matrix in CS and the pseudo-random sequence in DNA operations, which ensures the security of the encryption scheme. The STP-CS model with plaintext-related Arnold scrambling is used to effectively reduce the image redundancy information and measurement matrix storage, simultaneously implementing first-level encryption. The entire security is further enhanced by DNA random coding, DNA addition, and bit XOR operation. Simulation results show the effectiveness and superiority of the proposed image encryption scheme.

2 Proposed NMLNCML system

In our proposed scheme, an NMLNCML system with L lattices coupled by neighborhood links is defined as

$$x_{n+1}(i) = \mathrm{mod}(f[x_n(i)] + (1-\eta)\cdot\{f[x_n(i+1)] + f[x_n(i-1)]\} + \eta\cdot\{f[x_n(j)] + f[x_n(k)]\}, 1), \tag{1}$$

where i, j, k are different lattices ($2 \le i \le L-1$, $1 \le j,\ k \le L$), η is the coupling parameter ($0 \le \eta \le 1$), n is the time sequence ($n = 1, 2, \ldots$), and $f(x)$ is the logistic map satisfying $f(x) = \mu x(1-x)$ with $\mu \in [3.56, 4]$. Lattices j and k are both nonlinear neighbors of lattice i, and the relationship among i, j, and k is determined by an Arnold transform:

$$\begin{bmatrix} j \\ k \end{bmatrix} = \mathrm{mod}\left(\begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}\begin{bmatrix} i \\ i \end{bmatrix}, L\right), \tag{2}$$

where p and q are the parameters of Arnold mapping.

2.1 Kolmogorov–Sinai entropy

The NMLNCML system consists of L lattices. For each lattice, it is a chaotic system, so the Lyapunov exponent (LE) (Wang XY and Liu, 2020) values of each lattice can be computed. Without loss of generality, we apply Kolmogorov–Sinai entropy density (KED) h and Kolmogorov–Sinai entropy breadth (KEB) h_{u} (Zhang YQ and Wang, 2014) to describe the chaotic characteristics of the spatiotemporal chaotic system. h can eliminate the influence of the number of lattices. The larger the value, the stronger the chaotic characteristics of the system. When h is 0, it means that the spatiotemporal chaotic system is behaving normally. h_{u} is employed to further describe the chaotic majority of L lattices. The larger the value, the more lattices have chaotic behaviors, and thus the system exhibits stronger chaotic properties.

As in the MLNCML system (Zhang YQ and Wang, 2014), we set $L = 100$, $p = 12$, and $q = 7$ in our system. Figs. 1 and 2 show the Kolmogorov–Sinai entropy comparisons between the proposed NMLNCML system and MLNCML system with different μ and η values. Figs. 1b–1f and Figs. 2b–2f show the chaotic situations of the MLNCML system from $\epsilon = 0$ to $\epsilon = 0.8$.

First, from Figs. 1b–1f and Figs. 2b–2f, it can be clearly seen that under different ϵ, the changes of Kolmogorov–Sinai entropy are not stable. The density and breadth of Kolmogorov–Sinai entropy in Figs. 1c and 2c are lower than those in other subfigures, and the fluctuations are more intense. In the proposed NMLNCML system, the changes of Kolmogorov–Sinai entropy are stable (Figs. 1a and 2a), because they are not affected by ϵ, which means that the chaotic property of the proposed system is more stable. Second, in the MLNCML system, the variation range of parameter μ that keeps the system in a chaotic state is $[3.56, 4]$, while in the NMLNCML system, the variation range of μ is $[2.28, 4]$, which is wider than that in the MLNCML system. Third, from the comparison between Fig. 1a (Fig. 2a) and Figs. 1b–1f (Figs. 2b–2f), it can be seen that the Kolmogorov–Sinai entropy of the proposed system is larger than that of the MLNCML system, and thus the chaotic property is stronger. In addition, without complex parameter selection, it is more user-friendly to set only the initial value of the chaotic lattice and the linear–nonlinear coupling parameter η to obtain the chaotic sequence.

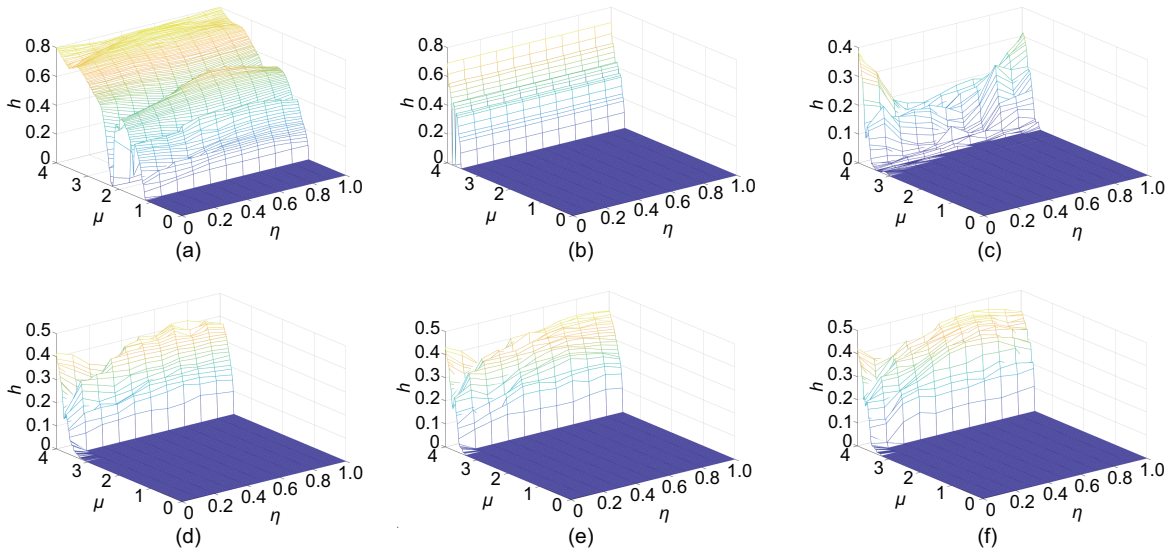

Fig. 1 Kolmogorov–Sinai entropy density comparison between the NMLNCML and MLNCML systems: (a) NMLNCML; (b) MLNCML (ϵ=0); (c) MLNCML (ϵ=0.2); (d) MLNCML (ϵ=0.4); (e) MLNCML (ϵ=0.6); (f) MLNCML (ϵ=0.8)

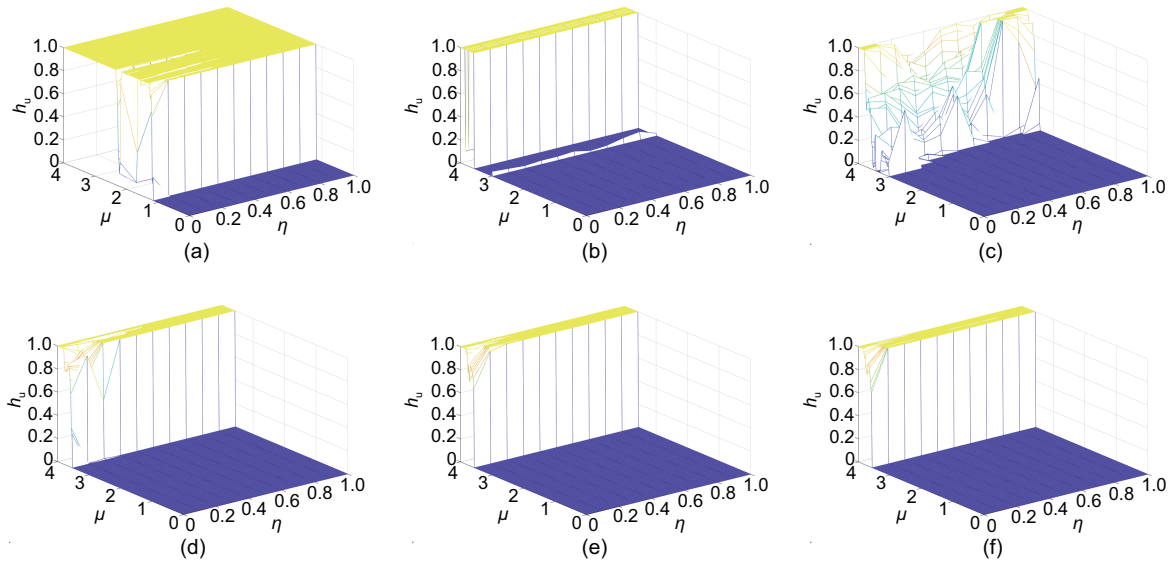

Fig. 2 Kolmogorov–Sinai entropy breadth comparison between the NMLNCML and MLNCML systems: (a) NMLNCML; (b) MLNCML (ϵ=0); (c) MLNCML (ϵ=0.2); (d) MLNCML (ϵ=0.4); (e) MLNCML (ϵ=0.6); (f) MLNCML (ϵ=0.8)

2.2 Bifurcation diagrams

A bifurcation diagram describes a series of abrupt changes in the state of a dynamic system with the change of control parameters, such as the period-doubling bifurcation, which leads to chaos. Set the system parameters as $L = 100$, $p = 12$, $q = 7$, and $\epsilon = 0.5$. Fig. 3 shows the bifurcation diagrams of the MLNCML and NMLNCML systems with $\mu \in [0, 4]$ and $\eta = 0.3, 0.5, 0.7, 0.9$. From Figs. 3b, 3d, 3f, and 3h, we can see that the MLNCML system contains many periodic windows when $\mu \in [0, 3.56]$. Compared with the MLNCML system, although several values of parameter μ make the system non-chaotic in Figs. 3a, 3c, 3e, and 3g, the range of optional parameter μ in the NMLNCML has been enlarged from $[3.56, 4]$ to $[2.28, 4]$. Moreover, the number of periodic windows has decreased,

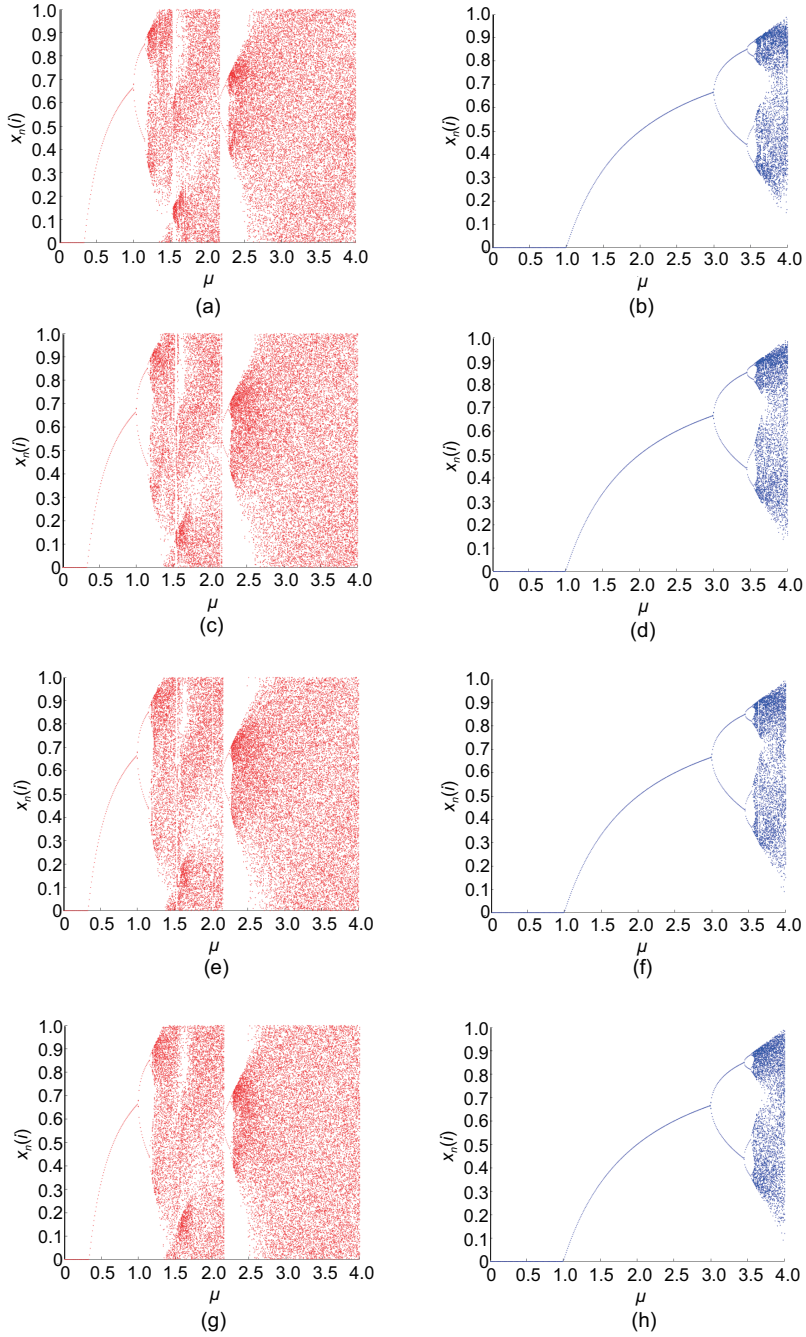

Fig. 3 Bifurcation diagrams of the NMLNCML and MLNCML systems: (a) NMLNCML (η=0.3); (b) MLNCML (η=0.3); (c) NMLNCML (η=0.5); (d) MLNCML (η=0.5); (e) NMLNCML (η=0.7); (f) MLNCML (η=0.7); (g) NMLNCML (η=0.9); (h) MLNCML (η=0.9)

and the chaos and ergodicity of the system have been significantly improved.

Because the forking of orbits in the NMLNCML system differs from that in the MLNCML system, we can further divide the value of μ in the NMLNCML system into two intervals, namely $[0, 1.5]$ and $(1.5, 4]$. It can be seen from Fig. 3a that the NMLNCML system shows a similar bifurcation pattern when $\mu \in [0, 1.5]$ with the MLNCML system when $\mu \in [0, 4]$ from one period to two periods, to four periods, to eight periods, and so on. The explanation is that the direct weighting of the lattice and its linear–

nonlinear neighbors accelerates the chaotic process of parameter μ, and the nonlinear modular operation harmonizes the distribution range of chaotic sequences, which enhances the ergodic property of the chaotic sequence. Due to the non-uniformity of the logistic function $f(x)$ and the further increase of parameter μ, some periodic windows still appear in the system when $\mu \in (1.5, 4]$. This phenomenon is more obvious when increasing μ to 2.16; that is, a new bifurcation of two periods to four periods appears in the NMLNCML system. However, due to the introduction of the coupling mode of the nonlinear modulus function, the distribution of the whole system is more uniform and the selection range of parameter μ, which causes the system to be chaotic, is expanded. The retention of nonlinear coupling parameter η inherits the chaotic behaviors of the MLNCML system. Parameter η increases the randomness of the possible period of orbits, which leads to misleading and inconspicuous times of period-doubling bifurcation. The elimination of the coupling coefficient and the introduction of module operation changes the coupling method of the spatiotemporal chaotic system from linear coupling to nonlinear coupling, which further strengthens the chaotic characteristics of the system and greatly reduces the number of periodic windows of the spatiotemporal chaotic system.

3 Proposed image encryption algorithm

3.1 Plaintext-dependent key generation

To enhance the correlation between the plain image and the encryption scheme, an SHA-384 hash function is employed to generate the plaintext-dependent keys. Taking a plain image P as the input, the 48-decimal output of the hash function H is computed. If one pixel value of the plain image changes, the hash value becomes much different. Dividing H into three parts to generate the real initial values for Arnold scrambling, Eq. (3) gives the computation process of the three parameters t, a, b in Arnold scrambling:

$$\begin{cases} H = h_1, h_2, \ldots, h_{48}, \\ t = \mathrm{mod}(t_0 + h_1 \oplus h_2 \oplus \cdots \oplus h_{16}, N), \\ a = a_0 + h_{17} \oplus h_{18} \oplus \cdots \oplus h_{32}, \\ b = b_0 + h_{33} \oplus h_{34} \oplus \cdots \oplus h_{48}, \end{cases} \tag{3}$$

where parameters t_0, a_0, and b_0 are random positive integers given by a sender. Parameter t_0 together with hash bits is used to produce the times of Arnold scrambling t. Parameters a_0 and b_0 as well as hash bits determine the real initial scrambling value of Arnold scrambling. N represents the number of columns in the plain image P.

3.2 Image compression and encryption algorithm

The whole flowchart of our encryption and decryption scheme is shown in Fig. 4. The encryption algorithm conforms to the architecture of scrambling, compression, and diffusion. The detailed encryption process is introduced as follows:

Step 1: calculate the plaintext key parameters t, a, and b associated with the original plain image P_1 with size of $m \times n$ according to Eq. (3).

Step 2: perform discrete wavelet transform (DWT) on the plain image to obtain the sparsity coefficient matrix P_2 with the same size as plain image P_1 via

$$P_2 = \mathrm{DWT}(P_1). \tag{4}$$

Step 3: manipulate Arnold scrambling on P_2 to obtain P_3 of the same matrix size with parameters t, a, and b in step 1. Among them, parameter t represents the number of times to perform Arnold scrambling, and parameters a and b are the scrambling parameters.

Step 4: iterate the NMLNCML system and generate chaotic sequences. As introduced in Section 2, first, set the initial values for $x(1)$, $x(2), \ldots,$ $x(L)$. Next, to ensure the chaos of the chaotic system, run the NMLNCML system $(N_{\mathrm{pre}} + mn)$ times iteratively with the initial values, abandon the preceding N_{pre} times, and finally, L pseudo-random sequences $(x(1), x(2), \ldots, x(L))$ sampled mn times are generated. The range of each sequence $x(i)$ is (0,1) and these sequences are used in compression and diffusion in our encryption algorithm. In this study, we set N_{pre} empirically to 1000.

Step 5: calculate the measurement matrix and employ the STP-CS for compression and encryption. One of the L sequences, $x(i)$, is selected to produce the chaotic measurement matrix $\Phi_{m_{\mathrm{STP}} \times n_{\mathrm{STP}}}$. Next, perform the transformation on the chaotic sequence $\Phi = \mathrm{reshape}\{1 - 2x(i), m_{\mathrm{STP}} \times n_{\mathrm{STP}}\}$, and a normalized measurement matrix Φ_{STP} can be created

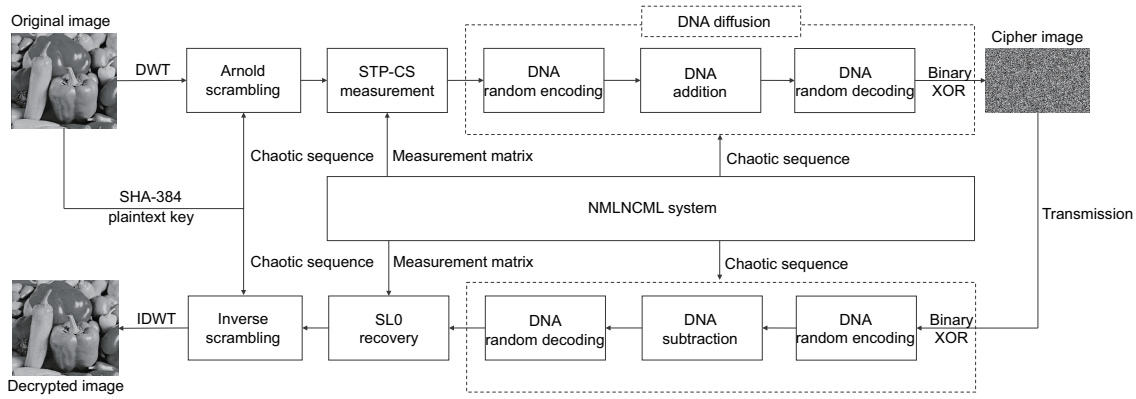

Fig. 4 Schematic diagram of the proposed encryption and decryption algorithm (DWT: discrete wavelet transform; STP-CS: semi-tensor product compressive sensing; NMLNCML: novel mixed linear–nonlinear coupled map lattice; IDWT: inverse discrete wavelet transform; SL0: smooth l_0 norm)

by $\Phi_{\mathrm{STP}} = \sqrt{\frac{2}{m_{\mathrm{STP}}}}\Phi$. Then, apply the STP-CS strategy for the confused sparse matrix P_3 to obtain the compressed and encrypted measurement P_4. Replace x in the STP-CS model with P_3, and Φ_{STP} is the STP measurement matrix. The size of P_4 is $m_{\mathrm{STP}}\frac{m}{n_{\mathrm{STP}}} \times m$.

Step 6: calculate the real diffusion keys and implement diffusion using DNA operations (Chen JX et al., 2018): random encoding (decoding) and DNA addition. Take two groups with four of the chaotic sequences $x(i_1^1)$, $x(i_2^1)$, $x(i_3^1)$, $x(i_4^1)$ and $x(i_1^2)$, $x(i_2^2)$, $x(i_3^2)$, $x(i_4^2)$ in step 4 (e.g., $x(2)$, $x(3)$, $x(4)$, $x(5)$ and $x(6)$, $x(7)$, $x(8)$, $x(9)$) and generate two keys (in the form of column vectors) K_1 and K_2 with size of $m\times 4n$ and one key (in the form of column vectors) K_3 of $m \times 8n$ in the following way:

$$p(i_j^k) = 1 + \mathrm{mod}\left[\mathrm{floor}\left(x(i_j^k) \times 10^{10}\right),\ 8\right],$$
$$j \in \{1,2,3,4\},\ k \in \{1,2\},\ i_j^k \in \{1,2,\ldots,L\}, \quad (5)$$

$$K_1 = \mathrm{vectorized}([p(i_1^1),\ p(i_2^1),\ p(i_3^1),\ p(i_4^1)]^{\mathrm{T}}), \quad (6)$$

$$K_2 = \mathrm{vectorized}([p(i_1^2),\ p(i_2^2),\ p(i_3^2),\ p(i_4^2)]^{\mathrm{T}}), \quad (7)$$

$$q(i_j^k) = \mathrm{mod}\left[\mathrm{floor}\left(x(i_j^k) \times 10^{10}\right),\ 256\right],$$
$$j \in \{1,2,3,4\},\ k \in \{1,2\},\ i_j^k \in \{1,2,\ldots,L\}, \quad (8)$$

$$K_3 = \mathrm{vectorized}([q(i_1^1),\ q(i_2^1),\ q(i_3^1),\ q(i_4^1),\ q(i_1^2),\ q(i_2^2),\ q(i_3^2),\ q(i_4^2)]^{\mathrm{T}}). \quad (9)$$

The keys K_1, K_2, K_3 as well as a DNA initial value d ($d \in$ {"A," "G," "C," "T"}) set by the user are used as the real key values in the diffusion process. Among these keys, K_1 and K_2 are used to control the random encoding and decoding rules of DNA, whose values are 1–8. K_3 controls the binary XOR operation after DNA completion. d is the initial value in DNA addition. First, the compressed matrix P_4 in step 5 is decomposed to a binary sequence with size $m \times 8n$ and converted to the DNA sequence P_5 with size $m\times 4n$ by random DNA encoding. For each two-bit transformation, the random coding rules are determined by the key K_1 in Eq. (6). Then, DNA addition is performed on the encoded DNA sequence P_5 to obtain the diffused DNA sequence P_6. A DNA addition rule is adopted and the addition is presented as in Eq. (10):

$$\begin{cases} P_6(1) = d_0 + P_5(1), \\ P_6(i) = P_6(i-1) + P_5(i), \end{cases} \quad (10)$$

where $i = 2,\ 3,\ \ldots,\ m \times 4n$ and "+" represents the DNA addition operation (Chen JX et al., 2018). Subsequently, the DNA sequence P_6 is randomly decoding to a binary sequence with the key K_2 in Eq. (7) and XORs the bits with the key K_3 in Eq. (9) to obtain the final cipher image P_7. The image decryption process is the inverse of the encryption process.

3.3 Discussion

Our image encryption algorithm has the following merits.

First, a novel image compression–encryption algorithm based on STP-CS and DNA operations is introduced. The architecture of permutation, compression, and diffusion is adopted. The plain image

is first converted into a coefficient matrix by DWT. Arnold scrambling is used to shuffle all elements of the coefficient matrix. Then the confused matrix is compressed by STP-CS, diffused by DNA operations and bit XOR operation, and the final cipher image is created. Because STP is introduced in CS, and the measurement matrix is smaller (in terms of a matrix's dimension and the total number of elements in it) than the traditional CS, the computation overhead is reduced. Additionally, because of the structural properties of STP, the corresponding parallel reconstruction algorithm can further improve the speed of the decryption process.

In STP-CS, every column of the plain image is separately compressed, and thus, energy information is retained in each column. Energy leakage will occur, which reduces the security level of the algorithm. To solve this problem, DNA diffusion is added after the CS, which distributes energy uniformly in the whole cipher image. Therefore, the anti-statistical attack ability of the proposed encryption algorithm is improved and its security level is enhanced.

Second, a plaintext-dependent SHA-384 hash function is introduced to shuffle the sparse coefficient matrix of the plain image. If any pixel in the original image changes, the hash value will be quite different. In permutation, the generation of initial scrambling parameters largely depends on the plain image, and different permutation processes will be obtained. Thus, our scheme can resist the CPAs and NPAs, which can compensate for the CS's disadvantage. Because CS is a linear transform, the encryption schemes based on CS struggle to resist the CPAs and NPAs.

Third, an NMLNCML system is proposed with more stable structure and stronger randomness. Chaotic sequences generated by it are used in compression and diffusion processes of image encryption. The measurement matrix of STP-CS is obtained by the random sequence generated by one of the lattices and used in the compression process, and the keys K_1, K_2, and K_3 are attained by the arrangement and combination of sequences of other lattices and used in the DNA diffusion process. Compared with low-dimensional chaotic systems, high-dimensional spatiotemporal chaotic systems have more complex dynamics and more key parameters. Compared with the MLNCML system, the NMLNCML system is more stable and random. Thus, the corresponding image encryption scheme has a larger key space and a higher security level to resist brute-force attacks.

4 Simulation results

In this section, several simulations are carried out to realize the proposed image encryption algorithm and assess its performance. Three 512×512 gray images (Lena, Peppers, and Baboon images) are chosen as test images. All the simulations are conducted with MATLAB 2020a software on a personal computer with a 3.40 GHz CPU, 8 GB RAM, and 64-bit Microsoft Windows 10. We use a two-level "Haar" wavelet to perform DWT. The initial values of key parameters t_0, a_0, and b_0 in Arnold scrambling are set to positive integers 52, 12, and 7, respectively. The lattice number L of the NMLNCML system is 10. Coupling parameter η is 0.8, and μ in the logistic map is 3.99. Nonlinear neighbor parameters are $p = 7$ and $q = 5$. The initial values of each lattice $x(1), x(2), \ldots, x(10)$ as part of keys in the NMLNCML system are 0.933 993 247 8, 0.678 735 154 9, 0.757 740 130 6, 0.743 132 468 1, 0.392 227 019 5, 0.655 477 890 2, 0.171 186 687 8, 0.706 046 088 0, 0.031 832 846 4, and 0.276 922 985 0. The DNA addition key d_0 is selected as "C." The reconstruction algorithm is smooth l_0 norm (SL0).

4.1 Encryption and decryption results

Fig. 5 represents the simulation results of the Lena, Peppers, and Baboon images when the compression ratio CR = 0.5 (CR is the image volume ratio between the compressed cipher image and plain image). The size of the STP measurement matrix is 128×256. Figs. 5a, 5d, and 5g are three plain images of Lena, Peppers, and Baboon, respectively. Figs. 5b, 5e, and 5h are their corresponding cipher images. Figs. 5c, 5f, and 5i are the decrypted images.

As can be observed from Figs. 5b, 5e, and 5h, the cipher images are similar to noise images. There is no relationship between the original images and the corresponding cipher images, so we cannot obtain any useful information about the original images from the cipher images. Therefore, the proposed encryption algorithm can protect the original images. From Figs. 5c, 5f, 5i, and their plain images, we can see that the decrypted images are similar to the original images.

To quantitatively measure the reconstruction

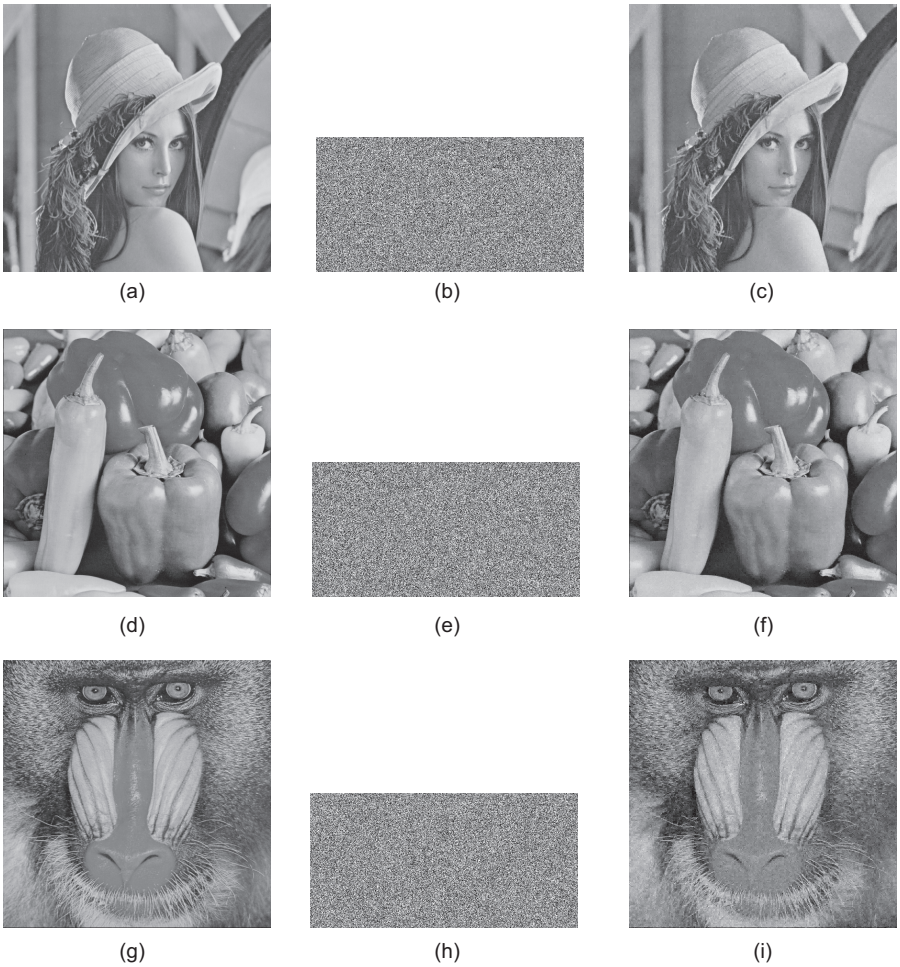

Fig. 5 Results of encryption and decryption: (a) plain image Lena; (b) cipher image of (a); (c) decrypted image of (a); (d) plain image Peppers; (e) cipher image of (d); (f) decrypted image of (d); (g) plain image Baboon; (h) cipher image of (g); (i) decrypted image of (g)

quality of the decrypted image, the peak signal-to-noise ratio (PSNR) (Li LX et al., 2020) is used as an index to describe the similarity between the decrypted image and original image. The greater the value of the PSNR, the higher the quality of the decrypted image.

The PSNRs in Figs. 5c, 5f, and 5i with CR = 0.5 are respectively 33.4462, 33.7960, and 32.1523 dB, which are >30 dB, indicating the effectiveness of decryption. In summary, our algorithm has good encryption and decryption effect, and thus the cipher images could be safely transmitted and saved on public channels and networks.

4.2 Compression performance

To study the influence of CR on the quality of the decrypted image, we also use the PSNR to compute the reconstruction results with different CRs (0.25, 0.50, and 0.75), as shown in Figs. S1 and S2 in the supplementary materials. Fig. S1 shows the encrypted images of Lena, Peppers, and Baboon with different CRs. Fig. S2 illustrates the reconstructed images with different CRs. The original images are shown in Figs. 5a, 5d, and 5g. As the CR decreases, the amount of the cipher image data that needs to be transmitted is reduced, but the quality of the decrypted image is also gradually degrading. However, from the last row in Fig. S2, even if the CR is 0.25, the details of the decrypted images are still clearly recognizable. In addition, Table 1 lists the PSNR values of our algorithm and other methods in Chen TH et al. (2016), Hu GQ et al. (2017), Li LX et al. (2019), and Gan et al. (2020) under the same CR (CR = 0.5), and a 512 × 512 Lena image is chosen

as the test image. From Table 1, we can see that the PSNR value in our cryptosystem is 33.4462 dB, which is greater than the values in Chen TH et al. (2016), Hu GQ et al. (2017), and Gan et al. (2020) and close to that in Li LX et al. (2019), indicating that our compressed encryption method has higher reconstruction quality.

4.3 Robustness to noise and data loss

To test the robustness to noise and data loss, different intensities of Gaussian noise (GN) and salt and pepper noise (SPN) are added to the cipher image of Peppers (256×512 pixels, Fig. 5e) first. Second, 16×16, 32×32, 64×64, and 128×128 pixels are cropped for the cipher image of Peppers, and the corresponding decrypted images are shown in Figs. S3 and S4.

It can be seen from Figs. S3 and S4 that when GN (or SPN) with an intensity of 0.000 07 is added and 1/8 of the data are lost, the decrypted image can still be recognized. This shows that the encryption algorithm is robust to noise and data loss attacks.

4.4 Key space analysis

Generally speaking, an effective image encryption system should have enough key space to resist a brute-force attack. It was recommended in Alvarez and Li (2006) that the qualified keys of an image encryption system should be $> 2^{100} \approx 10^{30}$ to make all kinds of brute-force attacks invalid. For the suggested encryption method, secret keys are: (1) positive integers t, a, b determined by a 384-bit output of hash function and initial values of t_0, a_0, and b_0; (2) the double-precision floating point initial state values of the NMLNCML system $x(1)$, $x(2), \ldots,$ $x(10)$; (3) compressed quantization parameter values $q_{\max}$ and $q_{\min}$; (4) the DNA base symbol of d_0. In this study, we assume that the computational precision of the computer is 10^{-10}, and the key space is $> N \times \left(10^{10}\right)^2 \times \left(10^{10}\right)^{10} \times \left(10^{10}\right)^2 \times 4 \approx 10^{140}$, which is sufficiently large to withstand brute-force attacks. Table 2 gives the key space of different algorithms in Zhang YQ et al. (2016), Li LX et al. (2019), Wen et al. (2020), and Li XH et al. (2022). It can be seen that the key space in our scheme is much larger than that of other algorithms, but smaller than the key space in Li XH et al. (2022).

Table 1 Comparison of PSNR values when CR=0.5

Algorithm	PSNR (dB)
Ours	33.4462
Li LX et al. (2019)	33.6057
Gan et al. (2020)	33.2299
Chen TH et al. (2016)	<33
Hu GQ et al. (2017)	<32

PSNR: peak signal-to-noise ratio; CR: the image volume ratio between the compressed cipher image and plain image

4.5 Key sensitivity analysis

Key sensitivity is an essential indicator to verify the effectiveness of a cryptosystem, and it can be analyzed from two perspectives: (1) from the perspective of the decrypter, completely different cipher images should be obtained as a result of a slight difference in encryption keys; (2) from the perspective of the encrypter, the plain image should not be correctly recovered even if the decryption keys and encryption keys are nuanced.

The plain image Lena is used for demonstration when CR = 0.5. For the first case of key sensitivity assessment, key sensitivity tests are performed during encryption. The correct encryption keys were introduced in Section 4.4 as (1) the 384-bit output of the hash of Lena is "7620c8d5c7eafdab5fc1c0ba1fc09947ce4645de44ba41f9ed222968b9108fe92371a5e26f3130ab893a554380ff1ee9," $t_0 = 388$, $a_0 = 12$, $b_0 = 7$; so, $t = 53$, $a = 41$, and $b = 84$. (2) L ($L = 10$) initial values of lattice $x(1), x(2), \ldots, x(L)$ are respectively set as 0.933 993 247 8, 0.678 735 154 9, 0.757 740 130 6, 0.743 132 468 1, 0.392 227 019 5, 0.655 477 890 2, 0.171 186 687 8, 0.706 046 088 0, 0.031 832 846 4, and 0.276 922 985 0. (3) Compressed quantization parameter values are $q_{\max} = 1.906\,691\,698\,0$, $q_{\min} = -2.295\,009\,277\,4$. (4) $d_0 =$ "C." These keys are used to generate the default cipher image shown in Fig. 5b. Then, after a slight change of 10^{-10} to $x(1)$, $x(2)$, $x(5)$, $x(9)$, and $x(10)$, the comparison of the cipher images is shown in Fig. S5. The pixel difference ratios between the default cipher image

Table 2 Comparison of key space

Algorithm	Key space
Ours	$>10^{140}$
Li XH et al. (2022)	$>10^{1056}$
Li LX et al. (2019)	10^{126}
Wen et al. (2020)	$>10^{80}$
Zhang YQ et al. (2016)	10^{56}

and other cipher images are computed and given in Table S1 in the supplementary materials. It can be seen that there is no similarity between the cipher images, and a small change in the encryption keys will cause >99.55% of pixels to become different in cipher images.

Next, we test the sensitivity of the key from the perspective of the decrypter for the second case. In the decryption process, we use the same key as in the encryption process. Fig. 5c is the recovered image decrypted with the correct key, and Fig. S6 shows the images decrypted with subtly modified keys. The pixel differences between the disordered decipher images and the correct image are 99.8543%, 99.8474%, 99.8558%, 99.8253%, and 99.8405%.

Considering the above two aspects, we can see that even a tiny interference of the keys will result in significant difference in the output of encryption or decryption, so the proposed encryption algorithm is highly sensitive to the secret key, and no valuable information about the key and plaintext will be leaked.

4.6 Statistical attack

Statistical attacks are used to analyze and decipher an encryption system by counting the characteristics of the cipher image in terms of histogram, pixel correlation, and information entropy (Zhang LY et al., 2018). The image histogram reflects the most basic statistical characteristics of the image. Correlation coefficient r_{xy} between adjacent pixels reflects the performance of the scrambling process in a cryptosystem. The lower the correlation between adjacent pixels of cipher images, the better the scrambling effect of the encryption algorithm. Information entropy is a vital indicator used to measure whether the gray value distribution in an image is uniform. The greater the information entropy of the image, the more uniform the gray value distribution of the image, and the greater the possibility of resisting entropy attacks. In theory, if the probability of each pixel value is equal, the maximum value of information entropy is ideally eight.

Fig. S7 shows the histogram information of the three original images and their corresponding cipher images (CR = 0.5). It is obvious that the histograms of the cipher images are distributed uniformly over the interval [0, 255] and are significantly different from those of the plain images.

In our simulation, 3000 pairs of adjacent pixels are randomly selected from the horizontal, vertical, and diagonal directions, separately. Fig. S8 illustrates the correlation distributions of two adjacent pixels in the horizontal, vertical, and diagonal directions of the image Lena. Table S2 shows the results of the correlation coefficient r_{xy} of the plain images and their corresponding cipher images. As can be observed, the correlation between adjacent pixels in the original image before encryption is very strong, but the correlation after encryption is greatly reduced.

Table S3 lists the information entropies of plain images and their corresponding cipher images when CR = 0.5. It can be seen from this table that information entropies of cipher images are all >7.99 and have increased more than that of their plain images. Table S4 presents the comparison with other encryption algorithms, and a 512×512 Lena image is used to test the performance. From Table S4, one may derive that our cryptosystem has good performance compared with Gan et al. (2020), and has better performance than Li LX et al. (2019), Chai et al. (2020a), and Li XH et al. (2022).

The above results prove the strong randomness of different encrypted images, showing the negligibility of information leakage in encryption and further demonstrating that the proposed cryptosystem is secure enough to resist entropy attack.

4.7 Differential attack

In a differential attack, an attacker makes specific changes to the plain image and then compares the corresponding ciphertext to obtain clues about the secret keys. To resist differential attacks, encryption algorithms usually need to have good diffusion performance; that is, a small modification of the original image will bring about significant disturbance in the ciphertext. The number of pixel change rate (NPCR) and unified averaged changed intensity (UACI) (Chai et al., 2022a) are usually used as numerical indicators to evaluate the ability of encryption algorithms.

To test the resistance to a differential attack, the Lena, Peppers, and Baboon images are chosen, the first, last, and a random pixel of each are changed, and different cipher images are obtained with the same keys. Table S5 lists the NPCR and UACI results between different cipher images and their corresponding default cipher images. As can be seen

from Table S5, the NPCR and UACI values under different conditions are close to the expected values 0.996 094 and 0.334 635 (Wu Y et al., 2011), suggesting that the proposed encryption system has good diffusion properties expressly to resist the differential attack.

4.8 Known- and chosen-plaintext attack analyses

Our image encryption algorithm is designed to resist the CPA and NPA, because of the following two aspects:

On one hand, the Arnold scrambling process is related to the plain image. This is because the SHA-384 function and secret keys together determines the parameters of Arnold scrambling. When any bit of the plain image changes, even if the same secret key is used, different output of the SHA-384 function will be generated. Thus, the scrambling process is distinct, making it infeasible to decrypt other cipher images using the key streams retrieved with a well-designed plain image from the attacker's point of view.

On the other hand, because STP-CS is essentially a linear transform, a single STP-CS is unable to resist the CPA and NPA. This is because if an attacker selects an identity matrix as the plaintext, the information of the measurement matrix will be leaked. Therefore, we design the diffusion phase after compression. In the diffusion phase, we adopt chaotic sequence-controlled DNA random coding/decoding, DNA addition, and bit XOR operation, combined with the plaintext-related scrambling stage, to achieve one-time encryption, which is resistant to CPA and NPA.

4.9 Computational and complexity analyses

To evaluate the computational time of our image cryptosystem, tests are performed on 512×512 Lena, Peppers, and Baboon images. Simulations on different images are separately encrypted and decrypted 10 times by our algorithm when CR = 0.5 and STP measurement matrices are with the dimension of 128×256. The total average encryption time is 1.9352 s and decryption time is 14.9216 s. Figs. S9 and S10, respectively, show the proportion of time spent in each phase of the encryption and decryption processes. The comparison results of the encryption time between our scheme and other methods for plain images of 512×512 are listed in Table S6.

For the execution time of our algorithm in Fig. S9, the most time-consuming encryption parts are DNA diffusion and Arnold scrambling. The time complexity of Arnold scrambling is $O(tMN)$, where t ($t \leq N$) represents the number of scramblings, and M and N represent the numbers of rows and columns of an image, respectively. The DNA diffusion, which takes most of the time, includes DNA random encoding, DNA addition, DNA random decoding, and bit XOR operation. The time complexities are as follows: DNA random encoding, $O(MN) + O(4MN)$; DNA addition, $O(4MN)$; DNA random decoding, $O(4MN) + O(MN)$; bit XOR operation, $O(MN)$. Therefore, the time complexity of DNA diffusion is $O(15MN)$.

The iterative process of chaotic systems, although running 263 144 steps, with the time complexity of $O(LMN)$, does not require too much time. One reason is that the chaotic system involves no computationally complex functions, such as the sine map used by Peng et al. (2021), cosine and exponential maps, etc. Another reason is that the number of coupled mapped grids set in our system is 10, which is relatively small. That means when the size of lattices is designed properly, the running speed of our algorithm could increase accordingly. From Table S6, we can see that our encryption algorithm is faster than Chai et al. (2020b), Gan et al. (2020), and Li XH et al. (2022), close to Li LX et al. (2019), and slower than Chai et al. (2020a), indicating the efficiency of the proposed algorithm.

In the decryption process, in addition to confusion and diffusion, the image reconstruction process occupies a larger proportion. This is because the SL0 algorithm takes a long time in the convergence phase. However, STP-CS can improve the signal recovery speed by grouping image coefficients, and each group can run the SL0 algorithm at the same time. By shortening the reconstruction time, the total speed of the proposed decryption algorithm is increased. As shown in Table S7, for a 512×512 Peppers image, when CR = 0.5, we set the measurement matrix of different sizes, and record the time consumed for reconstruction.

As the size of the STP measurement matrix decreases, the time spent on the reconstruction

algorithm also decreases. When the numbers of rows and columns of the measurement matrix are 1/8 of the traditional measurement matrix, the time of the reconstruction algorithm is about 1/4 of the traditional reconstruction algorithm. Therefore, the proposed algorithm is effective.

5 Conclusions

This paper proposed a new scheme for image encryption that took advantages of the NMLNCML system and DNA operations in CS. The proposed NMLNCML system continued the outstanding properties of the MLNCML system and further strengthened the chaotic characteristics (e.g., increased range of the logistic map parameter, more stable randomness in Kolmogorov–Sinai entropy, and reduced number of periodic windows in bifurcation diagrams) of the MLNCML system, which was very suitable for image encryption. We employed the NMLNCML system to generate the measurement matrix in CS and the pseudo-random sequence in DNA operations, which ensured the security of the encryption scheme. The STP-CS model with plaintext-related Arnold scrambling was used to effectively reduce the image redundancy information and measurement matrix storage, which simultaneously implemented a first-level encryption. The entire security was further enhanced by DNA random coding, DNA addition, and bit XOR operation. In the decryption process, the introduction of STP also greatly reduced the decryption time. Simulation results and security analysis indicated that our cryptosystem has significant key space, high sensitivity to secret keys, great resistance to chosen-plaintext, statistical, and differential attacks, and good robustness to noise and data loss. In addition, the outstanding compression and encryption performance can promote secure image compression and transmission on public channels and networks. However, the speed of DNA encryption and STP reconstruction is relatively low in the proposed scheme. In our future research, we will study how to improve the efficiency of these two parts.

Contributors

Yuanyuan LI and Xiaoqing YOU designed the research. Yuanyuan LI, Xiaoqing YOU, Jianquan LU, and Jungang LOU processed the data. Yuanyuan LI, Xiaoqing YOU, and Jungang LOU drafted the paper. Jianquan LU helped organize the paper. Yuanyuan LI, Xiaoqing YOU, Jianquan LU, and Jungang LOU revised and finalized the paper.

Compliance with ethics guidelines

Yuanyuan LI, Xiaoqing YOU, Jianquan LU, and Jungang LOU declare that they have no conflict of interest.

Data availability

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

References

Alvarez G, Li SJ, 2006. Some basic cryptographic requirements for chaos-based cryptosystems. *Int J Bifurc Chaos*, 16(8):2129-2151. https://doi.org/10.1142/S0218127406015970

Chai XL, Chen YR, Broyde L, 2017. A novel chaos-based image encryption algorithm using DNA sequence operations. *Opt Lasers Eng*, 88:197-213. https://doi.org/10.1016/j.optlaseng.2016.08.009

Chai XL, Fu XL, Gan ZH, et al., 2020a. An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata. *Neur Comput Appl*, 32(9):4961-4988. https://doi.org/10.1007/s00521-018-3913-3

Chai XL, Wu HY, Gan ZH, et al., 2020b. An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding. *Opt Lasers Eng*, 124:105837. https://doi.org/10.1016/j.optlaseng.2019.105837

Chai XL, Fu JY, Gan ZH, et al., 2022a. An image encryption scheme based on multi-objective optimization and block compressed sensing. *Nonl Dyn*, 108(3):2671-2704. https://doi.org/10.1007/s11071-022-07328-3

Chai XL, Wang YJ, Chen XH, et al., 2022b. TPE-GAN: thumbnail preserving encryption based on GAN with key. *IEEE Signal Process Lett*, 29:972-976. https://doi.org/10.1109/LSP.2022.3163685

Chen JX, Zhu ZL, Zhang LB, et al., 2018. Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption. *Signal Process*, 142:340-353. https://doi.org/10.1016/j.sigpro.2017.07.034

Chen L, Li CQ, Li C, 2022. Security measurement of a medical communication scheme based on chaos and DNA coding. *J Vis Commun Image Represent*, 83:103424. https://doi.org/10.1016/j.jvcir.2021.103424

Chen TH, Zhang M, Wu JH, et al., 2016. Image encryption and compression based on kronecker compressed sensing and elementary cellular automata scrambling. *Opt Laser Technol*, 84:118-133. https://doi.org/10.1016/j.optlastec.2016.05.012

Donoho DL, 2006. Compressed sensing. *IEEE Trans Inform Theory*, 52(4):1289-1306. https://doi.org/10.1109/TIT.2006.871582

Feng W, He YG, Li HM, et al., 2019. A plain-image-related chaotic image encryption algorithm based on DNA sequence operation and discrete logarithm. *IEEE Access*, 7:181589-181609. https://doi.org/10.1109/ACCESS.2019.2959137

Fira M, 2015. Applications of compressed sensing: compression and encryption. Health and Bioengineering Conf, p.1-4. https://doi.org/10.1109/EHB.2015.7391505

Gan ZH, Chai XL, Zhang JT, et al., 2020. An effective image compression-encryption scheme based on compressive sensing (CS) and game of life (GOL). *Neur Comput Appl*, 32(17):14113-14141. https://doi.org/10.1007/s00521-020-04808-8

Guo SF, Liu Y, Gong LH, et al., 2018. Bit-level image cryptosystem combining 2D hyper-chaos with a modified non-adjacent spatiotemporal chaos. *Multimed Tools Appl*, 77(16):21109-21130. https://doi.org/10.1007/s11042-017-5570-4

Hu GQ, Xiao D, Wang Y, et al., 2017. An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications. *J Vis Commun Image Represent*, 44:116-127. https://doi.org/10.1016/j.jvcir.2017.01.022

Hu HH, Liu JD, Shang K, et al., 2018. Parallel image encryption algorithm based on integer chaos and DNA coding. *Comput Eng Des*, 39(8):2401-2406 (in Chinese). https://doi.org/10.16208/j.issn1000-7024.2018.08.001

Kafedziski V, Stojanovski T, 2011. Compressive sampling with chaotic dynamical systems. 19th Telecommunications Forum, p.695-698. https://doi.org/10.1109/TELFOR.2011.6143641

Kaneko K, 1993. Theory and Applications of Coupled Map Lattices. John Wiley & Sons, Hoboken, USA.

Li LX, Liu LF, Peng HP, et al., 2019. Flexible and secure data transmission system based on semitensor compressive sensing in wireless body area networks. *IEEE Int Things J*, 6:3212-3227. https://doi.org/10.1109/JIOT.2018.2881129

Li LX, Wen GQ, Wang ZM, et al., 2020. Efficient and secure image communication system based on compressed sensing for IoT monitoring applications. *IEEE Trans Multimed*, 22(1):82-95. https://doi.org/10.1109/TMM.2019.2923111

Li XD, Song SJ, Wu JH, 2019. Exponential stability of nonlinear systems with delayed impulses and applications. *IEEE Trans Autom Contr*, 64(10):4024-4034. https://doi.org/10.1109/TAC.2019.2905271

Li XD, Peng DX, Cao JD, 2020. Lyapunov stability for impulsive systems via event-triggered impulsive control. *IEEE Trans Autom Contr*, 65(11):4908-4913. https://doi.org/10.1109/TAC.2020.2964558

Li XH, Zhou LL, Tan F, 2022. An image encryption scheme based on finite-time cluster synchronization of two-layer complex dynamic networks. *Soft Comput*, 26(2):511-525. https://doi.org/10.1007/s00500-021-06500-y

Lu JQ, Sun LJ, Liu Y, et al., 2018. Stabilization of Boolean control networks under aperiodic sampled-data control. *SIAM J Contr Optim*, 56(6):4385-4404. https://doi.org/10.1137/18M1169308

Lu JQ, Li BW, Zhong J, 2021. A novel synthesis method for reliable feedback shift registers via Boolean networks. *Sci China Inform Sci*, 64(5):152207. https://doi.org/10.1007/s11432-020-2981-4

Peng YX, He SB, Sun KH, 2021. A higher dimensional chaotic map with discrete memristor. *Int J Electron Commun*, 129:153539. https://doi.org/10.1016/j.aeue.2020.153539

Rani M, Dhok SB, Deshmukh RB, 2018 A systematic review of compressive sensing: concepts, implementations and applications. *IEEE Access*, 6:4875-4894. https://doi.org/10.1109/ACCESS.2018.2793851

Shao WD, Cheng MF, Luo CK, et al., 2019. An image encryption scheme based on hybrid electro-optic chaotic sources and compressive sensing. *IEEE Access*, 7:156582-156591. https://doi.org/10.1109/ACCESS.2019.2949704

Song CY, Qiao YL, 2015. A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos. *Entropy*, 17(10):6954-6968. https://doi.org/10.3390/e17106954

Sreedhanya AV, Soman KP, 2012. Secrecy of cryptography with compressed sensing. Int Conf on Advances in Computing and Communications, p.207-210. https://doi.org/10.1109/ICACC.2012.48

Testa M, Bianchi T, Magli E, 2020. Secrecy analysis of finite-precision compressive cryptosystems. *IEEE Trans Inform Forens Secur*, 15:1-13. https://doi.org/10.1109/TIFS.2019.2918089

Wang XY, Wang T, 2012. A novel algorithm for image encryption based on couple chaotic systems. *Int J Mod Phys B*, 26(30):1250175. https://doi.org/10.1142/S0217979212501755

Wang XY, Liu PB, 2020. A new image encryption scheme based on a novel one-dimensional chaotic system. *IEEE Access*, 8:174463-174479. https://doi.org/10.1109/ACCESS.2020.3024869

Wang Y, Wong KW, Liao XF, et al., 2011. A new chaos-based fast image encryption algorithm. *Appl Soft Comput*, 11(1):514-522. https://doi.org/10.1016/j.asoc.2009.12.011

Wen WY, Hong YK, Fang YM, et al., 2020. A visually secure image encryption scheme based on semi-tensor product compressed sensing. *Signal Process*, 173:107580. https://doi.org/10.1016/j.sigpro.2020.107580

Wu CW, Wu LG, Liu JX, et al., 2020. Active defense-based resilient sliding mode control under denial-of-service attacks. *IEEE Trans Inform Forens Secur*, 15:237-249. https://doi.org/10.1109/TIFS.2019.2917373

Wu Y, Noonan JP, Agaian S, 2011. NPCR and UACI randomness tests for image encryption. *J Sel Areas Telecommun*, April Edition, p.31-38.

Xie D, Peng HP, Li LX, et al., 2016. Semi-tensor compressed sensing. *Dig Signal Process*, 58:85-92. https://doi.org/10.1016/j.dsp.2016.07.003

Xu H, Tong XJ, Zhang M, et al., 2016. Dynamic video encryption algorithm for H.264/AVC based on a spatiotemporal chaos system. *J Opt Soc Am A*, 33(6):1166-1174. https://doi.org/10.1364/JOSAA.33.001166

Zhang LY, Liu YS, Pareschi F, et al., 2018. On the security of a class of diffusion mechanisms for image encryption. *IEEE Trans Cybern*, 48(4):1163-1175. https://doi.org/10.1109/TCYB.2017.2682561

Zhang YQ, Wang XY, 2014. Spatiotemporal chaos in mixed linear-nonlinear coupled logistic map lattice. *Phys A Stat Mech Appl*, 402:104-118. https://doi.org/10.1016/j.physa.2014.01.051

Zhang YQ, Wang XY, Liu J, et al., 2016. An image encryption scheme based on the MLNCML system using DNA sequences. *Opt Lasers Eng*, 82:95-103. https://doi.org/10.1016/j.optlaseng.2016.02.002

Zhong YS, Xu X, 2015. A novel image encryption method based on couple mapped lattice and two-stage diffusion. *Int J Secur Appl*, 9(11):281-292.

Zhou SW, He Y, Liu YH, et al., 2021. Multi-channel deep networks for block-based image compressive sensing. *IEEE Trans Multimed*, 23:2627-2640. https://doi.org/10.1109/TMM.2020.3014561

List of supplementary materials

Fig. S1 Cipher images under different compression ratios (CRs)

Fig. S2 Decrypted images under different CRs

Fig. S3 Cipher and decrypted images under different intensities of Gaussian noise (GN) and salt and pepper noise (SPN) attacks

Fig. S4 Cipher and decrypted images under different degrees of data loss attacks

Fig. S5 Key sensitivity test in the first case

Fig. S6 Key sensitivity test in the second case

Fig. S7 Histogram information for plain and cipher images

Fig. S8 Correlation distributions of image Lena and its cipher image

Fig. S9 Time proportion of different encryption phases

Fig. S10 Time proportion of different decryption phases

Table S1 Differences between cipher images produced by slightly different keys

Table S2 r_{xy} of adjacent pixels in the plain and cipher images

Table S3 Information entropies of plain and cipher images

Table S4 Information entropy comparison among different methods

Table S5 Differential attack resistance of the proposed scheme

Table S6 Encryption time comparison among different methods

Table S7 Reconstruction time comparison among different semi-tensor product measurements